THÈSE DE DOCTORAT DE L'UNIVERSITÉ PARIS VI

Spécialité

Informatique

Présentée par

Sébastien ORANGE

Pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ PARIS VI

Calcul de corps de décomposition Utilisations fines d'ensembles de permutations en théorie de Galois effective

Soutenue le

Composition du jury

19 janvier 2006

Table des matières

Chapitre 1

Introduction

Dans cette thèse, nous traitons de problèmes intervenant en théorie de Galois effective pour lesquels nous apportons des solutions de nature algorithmique. Plus précisément, notre objectif est de fournir des outils logiciels efficaces fondés sur des algorithmes dont nous maîtrisons la complexité pour permettre le calcul symbolique avec les racines d'un polynôme univarié : étant donné un polynôme univarié f de degré n à coefficients dans un corps K, nous cherchons à calculer une représentation du corps de décomposition de f, c'est-à-dire de l'extension algébrique $K(\alpha_1, \ldots, \alpha_n)$ de K contenant les racines $\alpha_1, \ldots, \alpha_n$ de f. Une représentation du corps de décomposition de f a l'avantage de permettre la détermination de l'action d'une représentation du groupe de Galois de f sur ses racines, abordant ainsi l'un des problèmes centraux de la théorie de Galois effective. Dans cette thèse, nous apportons des algorithmes de calcul d'une représentation du corps de décomposition et de détermination du groupe de Galois de ce polynôme.

Précisons ce que nous entendons par *représenter* le corps de décomposition d'un polynôme. Considérons, par exemple, le polynôme de degré 4 à coefficients rationnels défini par

$$f(x) = x^4 - x^3 - 3x^2 + x + 1\,.$$

Les formules de Cardan ou de Ferrari montrent qu'un 4-uplet $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ de racines de f annule les polynômes :

$$\begin{array}{lcl} f_1(x_1) & = & x_1^4 - x_1^3 - 3x_1^2 + x_1 + 1, \\ f_2(x_1, x_2) & = & x_2 - x_1^3 + x_1^2 + 3x_1 - 1, \\ f_3(x_1, x_2, x_3) & = & x_3^2 + x_3 x_1^3 - x_3 x_1^2 - 2x_3 x_1 - 1, \\ f_4(x_1, x_2, x_3, x_4) & = & x_4 + x_3 + x_1^3 - x_1^2 - 2x_1. \end{array}$$

La donnée de cet ensemble triangulaire de polynômes permet de définir un corps de décomposition de f : il s'agit de l'algèbre quotient de l'anneau des polynômes $K[x_1, x_2, x_3, x_4]$ par l'idéal engendré par l'ensemble triangulaire $\{f_1, f_2, f_3, f_4\}$ qui, nous le verrons plus tard, est maximal.

Notre objectif est d'obtenir pour un polynôme de degré n un tel *ensemble triangulaire* : il peut être vu comme l'ensemble des règles de réécriture dans $K[x_1, \ldots, x_n]$ permettant une représentation symbolique du corps $K(\alpha_1, \ldots, \alpha_n)$.

Les deux questions essentielles qui se posent pour le calcul d'un corps de décomposition sont :

- Quelle représentation de ce corps est la plus utile ?
- Quelle approche algorithmique faut-il privilégier pour aboutir à une telle représentation ?

Dans la suite de ce document, nous dressons un panorama des réponses apportées à la première question et des outils algorithmiques développés pour le calcul des représentations étudiées. Nous déduirons de ces différentes approches qu'une représentation utile et exploitable consiste en la donnée d'un ensemble triangulaire tel que mentionné ci-dessus. Nous verrons que cette représentation est accessible via des algorithmes fondés sur la factorisation de polynômes dans des extensions algébriques ou des algorithmes manipulant des résolvantes de Lagrange. Dans le paragraphe 1.2, nous exposons les résultats principaux de cette thèse. Il s'agit dans un premier temps d'un algorithme mixant les algorithmes de calcul de corps de décomposition fondés sur la factorisation et ceux fondés sur la manipulation de résolvantes de Lagrange. Mixer ces algorithmes n'est possible qu'en ayant accès à des informations de nature groupistique sur des idéaux dits de Galois intervenant dans nos algorithmes. Nous avons alors été amené à nous intéresser au calcul du groupe de décomposition d'un idéal (c'est-à-dire le sous-groupe des permutations dont l'action sur l'idéal laisse invariant cet idéal) ainsi qu'à la caractérisation des parties du groupe symétrique incluses dans l'injecteur d'un idéal de Galois. Dans le paragraphe 1.3, nous résumons chacun des chapitres de cette thèse.

1.1 Représentations du corps de décomposition

Historiquement, le problème du calcul de corps de décomposition fut abordé par la communauté mathématique via la recherche de formules closes pour exprimer les racines d'un polynôme univarié en fonction des valeurs de ses coefficients. Les résultats d'Abel et Galois ont montré que cette voie aboutissait à une impasse pour des degrés supérieurs ou égaux à 5. Des approches relevant de l'algèbre commutative et de la géométrie algébrique effectives pour les degrés $n \geqslant 5$ ont alors été développées pour représenter le corps de décomposition d'un polynôme univarié : il s'agit de définir ce corps comme l'algèbre quotient de l'anneau des polynômes en n variables par l'idéal engendré par les relations algébriques vérifiées par les racines de f. Obtenir un tel idéal peut se faire soit par des calculs de factorisations dans des extensions algébriques soit par des calculs de *résolvantes*. D'autres méthodes exploitent certaines informations sur le groupe de Galois

du polynôme pour faciliter le calcul de son corps de décomposition. Nous détaillons cet historique ci-dessous.

Formules closes. Exprimer les racines d'un polynôme à l'aide des opérations élémentaires $+$, $-$, $\times$, $/$ et de l'extraction de racines est un problème ancien. M. al Khwārizmī fut le premier à se donner explicitement cet objectif ; objectif repris avec succès pour le degré 3 (Cardan, Scipione del Ferro, Tartaglia) et pour le degré 4 (Cardan, Ferrari). La non-résolubilité des équations polynomiales génériques de degré 5 fut prouvée par Abel en 1826. Galois étendit ce résultat au degré $n \geqslant 5$ en donnant la condition nécessaire et suffisante qui, reformulée en termes modernes, s'écrit

> *Un polynôme est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Les possibilités offertes par le calcul formel permirent à D. Lazard d'exprimer les racines d'un polynôme de groupe de Galois résoluble à l'aide de formules closes pour le degré 5 (voir [40]). Cette approche diffère de celle de [21] de par les branchements qui interviennent au cours des calculs des expressions radicales.

Même si de telles formules existent en théorie pour $n \geqslant 6$, leurs calculs seraient particulièrement coûteux (voir [40]) et resteraient limités aux cas des polynômes de groupe de Galois résoluble. C'est pourquoi, dans cette thèse, nous privilégions l'étude de méthodes plus généralistes que nous présentons ci-dessous.

Factorisations successives. En s'appuyant sur la construction de L. Kronecker d'une extension algébrique de corps (voir [34]) mais aussi sur les travaux de F. Mertens (voir [44]), N. Tchebotarev construit un corps de décomposition de $f \in K[X]$ sous forme d'une algèbre quotient (voir [59]) :

$$K \simeq k[x_1, x_2, \ldots, x_n]/\mathcal{M} \ ,$$

où $\mathcal{M}$ est un idéal maximal de l'anneau $K[x_1, \ldots, x_n]$ des polynômes en les variables $x_1, \ldots, x_n$. Un tel idéal $\mathcal{M}$, appelé *idéal des relations de* f, décrit l'ensemble des relations algébriques vérifiées par un n-uplet $(\alpha_1, \ldots, \alpha_n)$ de racines de f. Pour ce faire, on représente d'abord $K(\alpha_1)$ par $K[X]/f$ puis on factorise le polynôme étudié f dans $K(\alpha_1)$ ce qui permet de représenter $K(\alpha_1, \alpha_2)$ par $K(\alpha_1)[X]$ quotienté par un des facteurs calculés et ainsi de suite jusqu'à obtenir $K(\alpha_1, \ldots, \alpha_n)$.

Ce type d'approche répond au problème de la construction de corps de décomposition d'un polynôme de groupe de Galois quelconque par le calcul d'un idéal des relations.

À partir d'algorithmes de factorisation dans des extensions algébriques, X. F. Roblot dans [52] et H. Anai, M. Noro, and K. Yokoyama dans [3] ont réalisé des implantations de cette construction.

En pratique, ces algorithmes peuvent s'avérer très coûteux en temps et en espace car ils n'exploitent pas le fait que la factorisation d'un polynôme sur un corps de rupture dépend fortement du groupe de Galois de ce polynôme. Ceci entraîne, dans certains cas, des factorisations inutiles dans des extensions de degré potentiellement être très élevé. De plus, à l'issue de ces calculs, l'action du groupe de Galois de f sur ses racines reste inconnue et son calcul doit encore être réalisé.

Calculs de résolvantes. Pour caractériser les équations polynomiales résolubles de degré $n \geqslant 5$, Galois utilise des polynômes auxiliaires qui furent ensuite étudiés par Lagrange : ce sont les *résolvantes*. Il s'agit de l'un des outils de base en théorie de Galois effective jusqu'alors principalement utilisé pour le calcul du groupe de Galois d'un polynôme et qui a fait l'objet de nombreuses améliorations (voir [5], [7], [26], [41], [50], [55], [57]). Les résolvantes peuvent permettre d'obtenir deux types d'information : une information galoisienne et une relation algébrique entre les racines du polynôme.

À partir de l'idéal des relations symétriques $\mathcal{S}$ engendrés par l'ensemble triangulaire de polynômes des modules de Cauchy de f (voir [17] ou [59]), il est théoriquement possible de calculer un idéal des relations $\mathcal{M}$ en considérant l'idéal engendré par $\mathcal{S}$ et un polynôme obtenu par un calcul de résolvantes (voir [5]). Cette méthode est similaire à celles fondées sur des calculs d'éléments primitifs. Lorsque le degré de f est trop élevé, cette méthode devient impraticable : le degré des extensions se retrouve en effet dans le degré du polynôme obtenu par ce biais.

L'algorithme `GaloisIdeal` d'A. Valibouze (voir [61]) diminue la difficulté du problème en le décomposant en plusieurs étapes (L. Ducos propose une approche similaire dans [20]). Cet algorithme fait appel à des calculs de résolvantes pour construire une chaîne ascendante d'idéaux appelés *idéaux de Galois* :

$$I_1 \subset I_2 \subset \cdots \subset I_s = \mathcal{M},$$

où I_1 est, par défaut, l'idéal des relations symétriques $\mathcal{S}$. Le calcul de l'idéal I_{i+1} à partir de l'idéal I_i nécessite de connaître un ensemble de polynômes engendrant I_i et un groupe L_i de S_n appelé *injecteur* de I_i.

Dans [62], A. Valibouze propose une généralisation de cet algorithme en traitant le cas où les injecteurs ne sont pas nécessairement des groupes.

Lorsque cet algorithme est appliqué, les premières étapes sont les plus coûteuses de par les calculs de résolvantes qu'elles nécessitent : c'est en effet au début de la chaîne d'idéaux de Galois, que le nombre de sous groupes maximaux contenus dans l'injecteur L et donc de calcul de résolvante est le plus élevé.

Exploitation d'informations sur le groupe de Galois. Les implantations des algorithmes de calcul du groupe de Galois d'un polynôme permettent d'atteindre le degré 23 (voir [11]) alors que le calcul d'un corps de décomposition peut s'avérer difficile, voire infaisable, pour des polynômes de degré inférieur à 10 (par exemple, les algorithmes actuels ne permettent pas, dans des temps raisonnables, de calculer l'idéal des relations d'un polynôme admettant pour groupe de Galois le groupe alterné de degré $n \geqslant 7$). Il est donc naturel de chercher à tirer profit d'informations sur le groupe de Galois du polynôme, pour faciliter le calcul de son corps de décomposition.

La première des informations sur le groupe de Galois que l'on peut tenter d'exploiter est sa résolubilité. Celle-ci est utilisée dans les articles [35], [37] [38], [4], [30]. Ces différents travaux permettent d'obtenir une expression radicale de chacune des racines d'un polynôme résoluble par radicaux mais les coûts en place de ces expressions sont tels qu'ils s'avèrent inexploitables (voir [40]).

Lorsque le centre du groupe de Galois d'un polynôme est non trivial, M. A. Gómez Molleda propose d'exploiter cette propriété pour obtenir une représentation des racines de f (voir [28]).

Le calcul d'un corps de décomposition d'un idéal de Galois d'un polynôme de groupe de Galois diédral D_5 fait l'objet d'un travail de B. K. Spearman et de K. S. Williams (voir [56]). Le cas du groupe diédral D_n a été traité par G. Renault (voir [29]).

De manière plus générale, lorsque le groupe de Galois G d'un polynôme est connu, la théorie de Galois classique ou les résultats de [7] assurent que tout idéal des relations est engendré par un ensemble triangulaire de polynômes $f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)$ et permet de connaître le degré du polynôme f_i en la variable x_i uniquement à partir de G. Déterminer un idéal de relations se ramène alors au calcul des coefficients des polynômes $f_1, \ldots, f_n$.

À partir d'approximations des racines et en supposant connue l'action d'une représentation symétrique du groupe de Galois sur celles-ci, K. Yokoyama calcule ces coefficients (voir [65]). Cette approche s'avère rapidement inapplicable lorsque le nombre de coefficients devant être calculé est trop élevé.

Récemment, G. Renault et K. Yokoyama ont amélioré cette technique en diminuant le nombre de coefficients devant être calculé (voir [29]). Cette amélioration est basée en partie sur une généralisation des techniques utilisées dans le chapitre 5 et aboutit à un algorithme efficace de calcul de corps de décomposition.

Conclusions partielles. Que ce soit par des calculs de factorisation dans des extensions algébriques ou via des calculs de résolvantes, la représentation du corps de décomposition d'un polynôme univarié par un *ensemble triangulaire* engendrant l'idéal des relations algébriques satisfaites par les racines du polynôme considéré est la plus utile.

En effet, celle-ci permet de calculer *modulo* l'idéal des relations ainsi encodé et son calcul peut être atteint et optimisé dès que des informations de nature galoisienne sont connues. Nos principales contributions portent donc sur le calcul d'une telle représentation triangulaire du corps de décomposition en mixant les approches à base de factorisation avec celles fondées sur la manipulation algébrique de résolvantes. Pour mener à bien cette approche, il est nécessaire de savoir extraire des informations de nature groupistique à partir des idéaux de Galois. C'est ce qui motive un deuxième aspect des contributions que nous exposons ci-dessous.

1.2 Contributions

L'approche que nous avons adoptée pour le calcul d'un idéal des relations de f utilise la notion d'idéal de Galois, idéaux qui définissent des ensembles de relations algébriques entre les racines de f, ainsi que les techniques à base de factorisation dans des extensions algébriques. Comme nous le verrons ci-après, ceci ne peut se faire qu'en extrayant des informations de nature galoisienne (groupe de décomposition, notion d'injecteur généralisant la notion de fixateur, etc.) à partir d'un idéal de Galois.

En collaboration avec G. Renault et A. Valibouze, nous avons été amenés à définir la notion d'injecteur d'un idéal de Galois ; un injecteur d'un idéal de Galois est un ensemble de permutations permettant de décrire toute la variété de cette idéal à partir d'un point de celle-ci. Cette notion prolonge celle de fixateur définie dans [61]*. Cette notion joue un rôle fondamental dans nos travaux en fournissant un cadre naturel pour décrire le treillis des idéaux de Galois d'un polynôme, pour établir des précalculs ainsi que pour exprimer la complexité de nos algorithmes. Déterminer et faire appel à ces ensembles de permutations afin de limiter les coûts des calculs algébriques constitue l'un des principaux axes des résultats que nous présentons. Dans [47], nous avons étendu aux idéaux de Galois, à l'aide de la notion d'injecteur, un théorème établi par A. Colin dans [18] pour les idéaux de relations. Ce résultat permet d'obtenir un idéal de Galois d'un polynôme réductible et séparable ainsi qu'un injecteur de cet idéal à partir d'idéaux de Galois et d'injecteurs de ces facteurs irréductibles. Ceci permet d'utiliser récursivement la notion d'injecteur dans les algorithmes de calcul d'un corps de décomposition procédant par factorisation successives mais aussi d'utiliser l'algorithme `FEGI` de [46] au cours de ces factorisations.

Avec G. Renault et A. Valibouze, nous avons étudié les relations entre les groupes de Galois d'un polynôme et ceux de ses facteurs sur un corps de rupture. Ici encore, l'un de nos objectifs est de mixer les techniques à base de résolvantes et celles fondées sur la factorisation dans les extensions algébriques. Cette étude complète celle de L. Soicher

*Dans le cas des idéaux utilisés dans [61], les notions d'injecteur et de groupe de décomposition coïncident ; on parle alors du fixateur d'un idéal et d'*idéaux de Galois purs.*

et J. McKay (voir [55]) en précisant non seulement les degrés des facteurs de rupture d'un polynôme mais aussi leurs groupes de Galois. Cette étude se présente sous forme de table appelée *tables de rupture*. Ces tables sont utiles en théorie de Galois directe : elle permettent d'obtenir des informations sur le groupe de Galois d'un polynôme à partir de ses facteurs de rupture, de connaître les degrés possibles des facteurs de rupture d'un polynôme de degré donné et fournit des informations sur les degrés pour le calcul de corps de décomposition. En théorie de Galois inverse, ces tables donne un moyen simple pour produire des polynômes de groupe de Galois donné à coefficients dans une extension simple d'un corps K à partir de polynômes à coefficients dans K de groupe de Galois connu.

Le groupe de décomposition d'un idéal I de $k[x_1, \ldots, x_n]$ est l'ensemble des permutations qui laissent globalement invariant cet idéal :

$$\mathrm{Dec}(I) = \{\sigma \in S_n \mid \forall f \in I,\, \sigma.f \in I\}\,.$$

Les algorithmes de calcul du groupe de décomposition d'un idéal triangulaire que nous avons élaborés, interviennent naturellement en théorie de Galois mais ne sont pas spécifiques à ce cadre. Le calcul de ce groupe intervient après le calcul d'un corps de décomposition dans le cas des algorithmes procédant par factorisations successives (il s'agit alors de déterminer la représentation du groupe de Galois associé à ce corps) mais aussi dans la détermination d'un injecteur d'un idéal de Galois (voir [46]). Ces algorithmes font appel à la notion d'ensemble fort de générateurs d'un groupe (voir, par exemple, [54], [53], [15]). L'étude de la complexité de ces algorithmes appliqués aux idéaux de Galois passe par une généralisation d'un théorème de prolongement dû à H. Anai, N. Noro et K. Yokoyama (voir [3]) qui permet d'interpréter les parcours d'arbre effectués par nos algorithmes. Le premier de ces algorithmes, nommé `Generateurs` a été réalisé en collaboration avec I. Adeljaoued, G. Renault et A. Valibouze et améliore l'algorithme `Strong_Generators` de [3] en terme de complexité et de temps de calcul. Le second algorithme, appelé `EFG` et issu d'un travail personnel, améliore les deux algorithmes précédents. Le tableau comparatif ci-dessous recense les complexités de ces trois algorithmes en terme de tests d'appartenance à l'idéal I (dans ce tableau, $\phi(L)$ désigne un entier pouvant être calculé à partir de tout injecteur L de I).

Algorithme	`Strong_Generators`	`Generateurs`	`EFG`
Idéaux de relations	$O(n^4)$	$O(n^3)$	$O(n^2)$
Idéaux de Galois purs	Non applicable	$O(n^3)$	$O(n^2)$
Idéaux de Galois	Non applicable	Factorielle	$O\left(n^2\phi(L)\right)$

À l'aide des contributions ci-dessus, il est possible de compenser les faiblesses des algorithmes de calcul d'un corps de décomposition par factorisations successives et l'algorithme `GaloisIdeal` (voir [61]) dont certaines étapes peuvent s'avérer particulièrement

coûteuses. En collaboration avec G. Renault et A. Valibouze, nous avons élaboré un algorithme mixte de calcul de corps de décomposition. La première étape de cet algorithme consiste à factoriser le polynôme sur l'un de ces corps de rupture et la seconde à utiliser l'algorithme `GaloisIdeal` pour obtenir un idéal des relations. Nous évitons ainsi les premières étapes de l'algorithme `GaloisIdeal`. La principale difficulté est de fournir à ce dernier algorithme la deuxième entrée qui lui est nécessaire, c'est à dire un injecteur de cet idéal. D'un point de vue expérimental, l'implantation de cet algorithme en degré 8 montre qu'il améliore de beaucoup les algorithmes procédant par factorisations successives car nous tenons compte et exploitons les informations galoisiennes fournies par les factorisations.

La caractérisation, issue d'un travail personnel, des parties d'un injecteur d'un idéal de Galois montre qu'il est toujours possible de déterminer l'un des injecteurs d'un tel idéal. Nous montrons comment, dans certaines situations, la donnée d'un injecteur d'un idéal de Galois I permet d'obtenir sans calcul une base de Gröbner d'un idéal de Galois contenant strictement I. Ceci généralise et simplifie une technique obtenue en collaboration avec G. Renault et A. Valibouze (voir [46]). Ce type de résultat est prometteur en théorie de Galois effective même s'il reste encore des optimisations à effectuer lorsque les calculs de base de Gröbner ne peuvent être évités.

1.3 Description des chapitres

Une description plus détaillée du contenu et des contributions de chacun des chapitres figure dans les introductions de chacun d'entre eux. Les polynômes utilisés à titre d'illustration tout au long de cette thèse sont extraits de la base de données de G. Malle et J. Klüners (voir [33] et [32]), disponible sur internet à l'adresse
`http ://www.iwr.uni-heidelberg.de/groups/compalg/minimum/`.

Les implantations de nos différents algorithmes ont été réalisées en Magma (voir [11]). Le choix de ce logiciel de calcul symbolique a été motivé, d'une part, parcequ'il réunit l'ensemble des algorithmes nécessaires à toutes nos implantations (bases de Gröbner, bases de données et algorithmes groupistiques, polynômes de groupe de Galois donné...) et, d'autre part, parceque ce logiciel est actuellement le seul qui permette le calcul de groupes de Galois sur des extensions algébriques.

Le chapitre 2 est une synthèse de résultats théoriques qui seront utilisés dans les chapitres 4, 5, 6 et 7. Ces résultats proviennent de différents articles (voir [2], [7], [17], [59], [61]) mais aussi de travaux collaboratifs réalisés avec G. Renault et A. Valibouze (voir [46]). La première partie de ce chapitre rassemble des résultats d'algèbre classiques portant sur les idéaux d'un anneau de polynômes (bases de Gröbner et idéaux triangulaires). Nous nous intéressons ensuite à deux types d'idéaux de Galois particuliers, les idéaux des relations symétriques et les idéaux des relations, avant de porter notre

attention sur les idéaux de Galois généraux. Parallèlement aux idéaux de Galois, nous abordons la notion d'injecteur d'un idéal de Galois afin de décrire la variété d'un idéal de Galois et le treillis des idéaux de Galois d'un polynôme. Cette notion permet d'établir des précalculs aux chapitres 5 et 6 mais aussi d'exprimer la complexité des algorithmes du chapitre 4.

Le chapitre 3 est consacré aux tables de rupture permettant l'étude du lien existant entre le groupe de Galois d'un polynôme irréductible et ceux de ses facteurs irréductibles sur un corps de rupture. Les tables de rupture jusqu'au degré 10 sont jointes en annexe (voir Annexe A). L'information galoisienne obtenue par l'intermédiaire des facteurs de rupture d'un polynôme ainsi que les informations portant sur les bases de Gröbner d'idéaux de relations seront exploitées au chapitre 5. Différentes applications possibles de ces tables sont abordées dans ce chapitre.

Au chapitre 4, nous présentons les algorithmes `Generateurs` et `EFG` pour le calcul du groupe de décomposition d'un idéal triangulaire ainsi que leurs études de complexité. Ces algorithmes ne sont pas spécifiques à la théorie de Galois effective et peuvent être appliqués à tout idéal triangulaire contrairement à leur étude de complexité qui nécessite l'emploi de la notion d'injecteur. Ces algorithmes nous seront utiles au chapitre 5 pour des calculs d'injecteurs d'idéaux de Galois. Ce chapitre s'achève sur des comparaisons en temps entre eux mais aussi avec l'algorithme `Strong_Generators` de [3]. Une implantation de cet algorithme est jointe en annexe (voir Annexe B).

Le chapitre 5 porte sur un algorithme mixte de calcul d'un corps de décomposition. Nous y exploitons les informations galoisiennes et polynomiales obtenues au chapitre 3 pour fournir à l'algorithme `GaloisIdeal` les deux entrées qui lui sont nécessaires : un idéal de Galois et l'un de ses injecteurs. Au premier paragraphe de ce chapitre, nous construisons un idéal de Galois à partir des facteurs de rupture de ce polynôme. Pour des raisons de lisibilité et afin de permettre une généralisation, nous nous restreignons au cas de factorisation d'un polynôme irréductible sur l'un de ses corps de rupture tout en veillant à ce que nos résultats soient suffisamment généraux pour être étendus à d'autres extensions de corps. La principale difficulté est alors d'obtenir l'un des injecteurs de cet idéal ce qui fait l'objet des paragraphes 5.2 et 5.3. Dans certaines situations, seule une liste d'ensembles de permutations dont l'un est un injecteur de l'idéal est obtenue. La détermination de cet injecteur se fait alors par élimination en utilisant, en particulier, les algorithmes du chapitre 4. Le paragraphe 5.4 utilise l'action des groupes de Galois possibles pour obtenir, sans calcul, de nouvelles relations algébriques. La principale difficulté sera là aussi d'obtenir un injecteur de l'idéal obtenu. Nous décrivons ensuite les différents outils dégagés pour élaborer un algorithme de calcul de corps de décomposition pour un degré donné. Ces outils sont alors mis en œuvre dans le dernier paragraphe pour le degré 8. Les temps de calcul de l'algorithme obtenu sont ensuite comparés avec ceux

de l'algorithme procédant par factorisations successives exposé dans [3]

Au chapitre 6, nous caractérisons les parties de S_n incluses dans un injecteur L de I. Cette caractérisation assure, en particulier, qu'il est toujours possible de déterminer l'un des injecteurs d'un idéal de Galois obtenu au chapitre 5. Lorsque L est un groupe, à partir de L et de I, nous montrons comment définir un idéal de Galois I' contenant strictement I d'injecteur connu. Dans certaines situations, une base de Gröbner de l'idéal I' peut être obtenu sans calcul uniquement à partir de L et d'une base de Gröbner de I. Ceci complète et simplifie l'étude faite au paragraphe 5.4.

Le chapitre 7 porte sur le calcul d'un idéal des relations d'un polynôme réductible séparable f. À partir d'idéaux de Galois de ces facteurs irréductibles et d'injecteurs de ces idéaux, nous montrons comment obtenir un idéal de Galois de f et un injecteur de cet idéal. Le dernier paragraphe de ce chapitre présente des exemples d'applications de ce résultat pour le calcul d'un corps de décomposition d'un polynôme.

Chapitre 2

Idéaux de Galois

Dans ce chapitre, sont décrits les principaux objets mathématiques que nous sommes amenés à considérer dans nos algorithmes. La notion d'idéal de Galois, qui est la notion centrale de ce chapitre, est due à A. Valibouze (voir [61]). Elle fournit un cadre théorique en théorie de Galois effective.

Un idéal de Galois d'un polynôme décrit un ensemble de relations algébriques vérifiées par les racines de ce polynôme. Un premier exemple d'idéal de Galois est l'idéal des relations symétriques entre les racines d'un polynôme (voir [17]). Un deuxième exemple est fourni par les idéaux des relations entre les racines d'un polynôme, lesquels permettent d'obtenir des corps de décomposition. Dans [59], Tchebotarev décrit une construction théorique d'un corps de décomposition d'un polynôme par factorisations successives en utilisant des résultats de Kronecker (voir [34]). Une telle construction est mathématiquement équivalente à celle d'une suite croissante d'idéaux de Galois dont le dernier terme est un idéal des relations.

A. Valibouze, dans [61], rattache à la notion d'idéal de Galois la notion géométrique de fixateur de cet idéal : il s'agit de décrire la variété d'un idéal de Galois à l'aide d'un ensemble de permutations. Dans ce chapitre, nous allons prolonger cette notion en définissant celle, plus algébrique, d'injecteur d'un idéal de Galois. Dans les chapitres 4, 5, 6 et 7 ainsi que dans celui-ci, nous utiliserons cette notion pour décrire le treillis des idéaux de Galois d'un polynôme, pour établir des précalculs ainsi que pour exprimer la complexité de certains algorithmes.

Les définitions et les résultats indépendants de la théorie de Galois effective, auxquels nous ferons appel, sont introduits dans le premier paragraphe de ce chapitre.
Le paragraphe 2.2 est consacré aux idéaux des relations symétriques ; il s'agit du cas le plus simple d'idéaux de Galois.
Au paragraphe 2.3, est définie la notion d'idéal des relations entre les racines d'un polynôme. Nous ferons le lien entre ce type d'idéal et la théorie de Galois classique (corps

de décomposition et groupe de Galois). Nous nous intéresserons ensuite à l'action du groupe symétrique sur l'ensemble des idéaux des relations d'un polynôme afin d'éclairer le rapport entre ces idéaux.
Le paragraphe 2.4 de ce chapitre porte sur les idéaux de Galois. Nous y définissons la notion d'injecteurs d'un idéal de Galois pour ensuite faire le lien entre injecteur, variété et groupe de décomposition. Nous établirons pour finir une correspondance entre idéaux de Galois et parties de S_n qui regroupe différents résultats de ce chapitre.

Cette synthèse provient de différents articles (voir [2], [7], [17], [59], [61]) auxquels ont été adjoints de nouveaux résultats obtenus en collaboration avec G. Renault et A. Valibouze (voir [46]).

Dans tout ce chapitre, nous utiliserons les notations suivantes :
- K désigne un corps parfait et $\bar{K}$ une clôture algébrique de K ;
- $K[x_1, \ldots, x_n]$ est l'anneau des polynômes en les n variables algébriquement indépendantes $x_1, \ldots, x_n$;
- $\underline{X}$ désigne le n-uplet $(x_1, \ldots, x_n)$;
- le groupe symétrique de degré n est noté S_n.

Toutes les extensions algébriques que nous serons amenés à considérer seront supposées être contenues dans $\bar{K}$.

2.1 Anneaux de polynômes - idéaux

Dans ce paragraphe, nous abordons les bases de Gröbner d'idéaux polynômiaux. Ces ensembles de polynômes interviennent naturellement en théorie de Galois effective (par exemple, dans le calcul d'un corps de décomposition d'un polynôme).

2.1.1 Base de Gröbner

Définition 2.1.1. Un *monôme* en les n variables (ou indéterminées) $x_1, \ldots, x_n$ est un produit $x_1^{d_1} \ldots x_n^{d_n}$ où $(d_1 \ldots, d_n) \in \mathbb{N}^n$. Le monôme $x_1^{d_1} \ldots x_n^{d_n}$ est aussi noté $\underline{X}^d$.
L'ensemble des monômes muni de la multiplication est un monoide d'élément neutre $1 = x_1^0 \ldots x_n^0$.

Un *terme* est le produit d'un monôme par un élément non nul de K.
Tout *polynôme* est une somme finie de termes.

Définitions 2.1.2. Un *ordre admissible* $\prec$ est un ordre total sur l'ensemble des monômes qui satisfait les axiomes :
- $1 \prec m_1$;
- si m_1, m_2 et m_3 sont trois monômes alors

$$m_1 \prec m_2 \Rightarrow m_1 m_3 \prec m_2 m_3 \,.$$

Soit f un polynôme non nul et $\prec$ un ordre admissible sur l'ensemble des monômes. Le *monôme initial* de f, noté $init(f)$, est le plus grand monôme qui apparaît dans f.

Pour $n > 1$, il existe plusieurs manières d'ordonner les monômes en $x_1, \ldots, x_n$. Pour nos implantations d'algorithme, deux ordres admissibles particuliers vont nous être utiles. Le premier est l'ordre lexicographique : cet ordre interviendra naturellement lors de la détermination de bases de Gröbner d'idéaux de Galois. Le second, plus adapté aux calculs, est l'ordre grevlex.

Définitions 2.1.3. L'*ordre lexicographique induit par* $x_1 < x_2 < \cdots < x_n$ est défini par :

$$x_1^{d_1} \dots x_n^{d_n} \prec x_1^{d'_1} \dots x_n^{d'_n} \text{ ssi il existe } s \in [\![1, n]\!] \text{ tel que } \begin{cases} d_j = d'_j \text{ pour } j < s \\ \text{ et} \\ d_s < d'_s \,. \end{cases}$$

L'*ordre grevlex* (graded lexicographic order) est défini par :

$$x_1^{d_1} \dots x_n^{d_n} \prec x_1^{d'_1} \dots x_n^{d'_n} \text{ ssi } \begin{cases} \sum_{i=1}^n d_j < \sum_{i=1}^n d'_j \\ \text{ ou, en cas d'égalité,} \\ \exists s \in [\![1, n]\!],\ d_j = d'_j \text{ pour } j < s \text{ et } d_s < d'_s \,. \end{cases}$$

Donnons nous un ordre admissible $\prec$ sur $K[x_1, \dots, x_n]$. Un tel ordre permet de généraliser l'algorithme de division euclidienne des polynômes en une variable aux cas des polynômes en plusieurs variables. Des polynômes $f_1, \dots, f_s$ et g de $K[x_1, \dots, x_n]$ étant donnés, il s'agit de calculer des polynômes $q_1, \dots, q_s$ et h tels que $g = q_1 f_1 + \cdots + q_s f_s + h$. Cette généralisation de l'algorithme de division euclidienne peut s'écrire :

Algorithme 2.1.4.
Fonction `NF` $(f_1, \dots, f_s, g)$;
/* Entrées : . Les polynômes $f_1, \dots, f_s$ et g ;
Sortie : . des polynômes $q_1, \dots, q_s$ et h tels que $g = q_1 f_1 + \cdots + q_s f_s + h$. */
Pour $i \in [\![1, n]\!]$ **Faire**
. $q_i = 0$;
Fin Pour ;
$h = 0$;
Tant Que $g \neq 0$ **Faire**
. $E := \{i \in [\![1, n]\!] \mid init(f_i) \text{ divise } init(g)\}$;
. **Si** $E \neq \emptyset$ **Alors**
. . $i := Min(E)$;
. . $q_i := q_i + \frac{init(g)}{init(f_i)}$;
. . $g := g - \frac{init(g)}{init(f_i)} f_i$;
. **Sinon**
. . $g := g - init(g)$;
. . $h := h + init(g)$;
. **Fin Si** ;
Fin Tant Que ;
Retourner $q_1, \dots, q_n, h$;
Fin Fonction

La suite des monômes initiaux de la variable g est strictement décroissante dans la boucle **Tant Que**. Lorsque le nombre de monômes inférieurs à un monôme donné et supérieurs à tous les monômes initiaux $init(f_1), \ldots, init(f_s)$ est fini, la boucle **Tant Que** est exécutée un nombre fini de fois et la terminaison de l'algorithme est assurée.

Le problème fondamental de cet algorithme est la non-unicité du reste obtenu : ce reste dépend de l'ordre des polynômes $f_1, \ldots, f_s$ fournis en arguments. En effet, considérons les polynômes $g(x_1, x_2) = x_1^2 x_2 + 1$, $f_1(x_1, x_2) = x_1\, x_2 - x_1$ et $f_2(x_1, x_2) = x_1^2 - 1$ de $K[x_1, x_2]$ et munissons l'anneau $K[x_1, x_2]$ de l'ordre lexicographique ; l'appel $\texttt{NF}(f_1, f_2, g)$ retourne le reste nul alors que l'appel $\texttt{NF}(f_2, f_1, g)$ retourne le reste $-x_2 + 1$. En particulier, si aucune autre contrainte n'est imposée aux polynômes $f_1, \ldots, f_s$, l'algorithme ne permet pas de tester l'appartennance d'un polynôme g à l'idéal engendré par $f_1, \ldots, f_s$. Les bases de Gröbner, définies ci-après, apportent une solution à ce problème d'unicité.

Définition 2.1.5. Soient I un idéal non nul de l'anneau $K[x_1, \ldots, x_n]$ et $\mathcal{B} = \{f_1, \ldots, f_s\}$ un ensemble de s polynômes non nuls de I.

On appelle *idéal initial de* I l'idéal engendré par l'ensemble des monômes $\{init(f) \mid f \in I\}$.

L'ensemble $\mathcal{B}$ est une *base de Gröbner* de l'idéal I si l'idéal initial de I est engendré par l'ensemble $\{init(f_1), \ldots, init(f_n)\}$.

Le théorème suivant, reformulé en termes de base de Gröbner, est dû à D. Hilbert.

Théorème 2.1.6. *(voir [8] ou [19]) Tout idéal I non nul de $K[x_1, \ldots, x_n]$ admet une base de Gröbner et est engendré par cette base.*

Le premier algorithme permettant le calcul d'une base de Gröbner d'un idéal à partir d'un système de générateurs de cet idéal est dû à B. Buchberger (voir [13]). De nombreuses améliorations de cet algorithme ont été réalisées (par exemple, voir [14] et [23]). Actuellement, la plus efficace est l'algorithme `F5` de Jean-Charles Faugère (voir [24]).

Théorème 2.1.7. *(voir [8] ou [19]) Soient I un idéal de $K[\underline{X}]$ et $\mathcal{B} = \{f_1, \ldots, f_s\}$ un ensemble de s polynômes de I.*
L'ensemble $\mathcal{B}$ est une base de Gröbner de I si et seulement si pour tout polynôme g de $K[\underline{X}]$, il existe un unique polynôme h de $K[\underline{X}]$ tel que

$$\begin{cases} g - h \in I \\ et \\ \forall i \in [\![1, n]\!],\ init(h) < init(f_i). \end{cases}$$

Le théorème 2.1.7 permet d'assurer l'unicité du reste h retourné par l'algorithme 2.1.4 et permet, en particulier, de tester l'appartenance d'un polynôme à un idéal. Ce résultat justifie la définition suivante.

Définition 2.1.8. Le polynôme h de la proposition précédente s'appelle la *forme normale de f modulo* $\{f_1, \ldots, f_s\}$ et se note $NF(f)$.

Définition 2.1.9. Une base de Gröbner $\{f_1, \ldots, f_s\}$ d'un idéal I est dite *réduite* si, pour tout $i \in [\![1, n]\!]$, f_i est égal à sa forme normale modulo $\{f_1, \ldots, f_s\} \setminus \{f_i\}$.

Proposition 2.1.10. *(voir [8] ou [19]) Pour un ordre admissible donné, un idéal de $K[x_1, \ldots, x_n]$ admet une unique base de Gröbner réduite.*

2.1.2 Idéaux triangulaires

Idéaux triangulaires et bases de Gröbner

Les ensembles triangulaires de polynômes constituent un domaine de recherche important de par les applications qu'ils offrent (par exemple, voir [1], [7], [6], [48] et [64]). Dans le cadre particulier des idéaux de Galois, une définition moins générale des idéaux triangulaires nous sera utile. Nous utiliserons les définitions suivantes qui sont dues à D. Lazard.

Définition 2.1.11. (voir [39]) Un idéal de $K[\underline{X}]$ est dit *triangulaire* s'il est engendré par un ensemble triangulaire de polynômes

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

tel que, pour tout $i \in [\![1, n]\!]$, il existe $d_i \in \mathbb{N}^*$ tel que $init(f_i) = x_i^{d_i}$.

Un ensemble triangulaire est dit *séparable* si l'idéal qu'il engendre est radical.

Proposition 2.1.12. *Soit I un idéal triangulaire de $K[\underline{X}]$ engendré par un ensemble triangulaire séparable de polynômes*

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

L'ensemble $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ est une base de Gröbner de l'idéal I relativement à l'ordre lexicographique.

Démonstration. Soit $f \in I$. Il existe n polynômes $q_1, \ldots, q_n$ de $K[\underline{X}]$ tels que $f = \sum_{i=1}^{n} q_i f_i$. Le monôme $init(f)$ est donc égal à $init(q_i f_i) = init(q_i)\, init(f_i)$. Ainsi, tout monôme de l'ensemble $\{init(f) \mid f \in I\}$ appartient à l'idéal engendré par l'ensemble $\{f_1, \ldots, f_n\}$. La proposition découle alors de la définition d'une base de Gröbner. □

Le calcul d'une forme normale modulo un ensemble triangulaire

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

relativement à l'ordre lexicographique peut se réaliser à l'aide de pseudo-divisions euclidiennes. Un polynôme P de $K[x_1, \ldots, x_n]$ étant donnés, la pseudo-division euclidienne de P par f_i relativement à la variable x_i consiste à effectuer la division euclidienne de P par f_i considérés comme polynômes à coefficients dans $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ en la variable x_i. La forme normale de P modulo $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ s'obtient alors en effectuant les pseudo-divisions euclidiennes

Proposition 2.1.13. *Soit $P \in K[x_1, \ldots, x_n]$. Notons $(r_i)_{i\in\{1,\ldots,n\}}$ la suite de $K[x_1, \ldots, x_n]$ définie inductivement comme suit : $r_n = P$ et , pour tout $i \in \{1, \ldots, n-1\}$, r_{i-1} est le reste de la pseudo-division euclidienne de r_i par f_i relativement à la variable x_i.*

Le polynôme r_1 est la forme normale de P modulo I.

En particulier, nous avons l'équivalence :

$$(P \in I) \text{ ssi } (r_1 = 0).$$

L'algorithme 2.1.4, appliqué à l'ensemble triangulaire $\{f_1, f_2, \ldots, f_n\}$ et dans lequel la fonction auxiliaire *init* retourne le monôme initial d'un polynôme pour l'ordre lexicographique, correspond à une implantation de cette proposition.

Variété d'un idéal triangulaire

Notations 2.1.14. Soit I un idéal de $K[\underline{X}]$. La K-variété associée à l'idéal I est notée $V(I)$:

$$V(I) = \{\underline{\alpha} \in \bar{K}^n \mid \forall g \in I,\ g(\underline{\alpha}) = 0\}\ .$$

Définition 2.1.15. Un idéal I de $K[\underline{X}]$ est dit de dimension nulle si $V(I)$ est un ensemble fini.

Un idéal de dimension nulle n'est pas nécessairement triangulaire mais peut toujours s'écrire comme intersection d'idéaux triangulaires (voir [48] et [39]).

Définition 2.1.16. Soit V une partie de $\bar{K}^n$. Notons π_i la projection de $\bar{K}^n$ sur $\bar{K}^i$ qui a tout n-uplet associe ses i premières coordonnées et V_i la projection $\pi_i(V)$.

La partie V est dite *équiprojectable* si, pour tout $i \in [\![1, n]\!]$ et tout $\underline{\beta} \in V_i$, le cardinal $c_i = \mathrm{Card}(\pi_i^{-1}(\underline{\beta}))$ ne dépend que de i. Ceci revient à dire que le nombre c_i de prolongements d'un i-uplet $\underline{\beta} \in V_i$ en un élément de V ne dépend que de i.

Pour tout $i \in [\![1, n]\!]$, nous noterons d_i l'entier $c_{i+1}\,/c_i$. l'entier d_i correspond au nombre de prolongements de tout élément de V_i en un élément de V_{i+1}.

Le théorème suivant, dû à P. Aubry et A. Valibouze, caractérise les idéaux triangulaires de dimension nulle. Il montre que la liste des degrés $(\deg_{x_1}(f_1), \ldots, \deg_{x_n}(f_n))$ d'une base de Gröbner d'un idéal triangulaire I ne dépend que de la variété de cet idéal. Ce théorème justifie la définition 2.1.18.

Théorème 2.1.17. *(voir [7]) Soit V une K-variété de dimension nulle de $\bar{K}^n$. Les conditions suivantes sont équivalentes :*

1. *il existe un ensemble triangulaire séparable $\{f_1, f_2, \ldots, f_n\}$ de $K[\underline{X}]$ tel que $V = V(\langle f_1, f_2, \ldots, f_n\rangle)$;*
2. *V est équiprojectable.*

De plus, lorsque ces conditions sont réalisées, nous avons, avec les notations précédentes, $\forall i \in [\![1, n]\!]$, $d_i = \deg_{x_i}(f_i)$.

Ce théorème permet de poser la définition suivante.

Définition 2.1.18. Soit I un idéal triangulaire de dimension nulle. 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^{e} élément de la liste $\mathcal{L}(I)$.

Le théorème 2.1.17 a pour corollaire immédiat.

Corollaire 2.1.19. *Soit I un idéal triangulaire. Nous avons,*

$$\text{Card}(V(I)) = \prod_{i=1}^{n} \deg_{x_i}(I). \tag{2.1.1}$$

Le cardinal de la variété d'un idéal engendré par un ensemble triangulaire séparable de polynômes s'obtient donc par une simple lecture des degrés des monômes initiaux de ces générateurs.

2.1.3 Action de S_n sur les idéaux

Dans toute la suite, nous allons considérer l'action naturelle du groupe symétrique S_n sur l'algèbre $K[\underline{X}]$:

$$\begin{array}{rcl} S_n \times K[x_1, x_2, \ldots, x_n] & \longrightarrow & K[x_1, x_2, \ldots, x_n] \\ (\sigma, P(x_1, \ldots, x_n)) & \longrightarrow & \sigma.P = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \ . \end{array}$$

Toute permutation $\sigma \in S_n$ définit ainsi un automorphisme d'algèbre de $K[\underline{X}]$. En particulier, nous avons la propriété immédiate suivante.

Proposition 2.1.20. *L'automorphisme induit par $\sigma \in S_n$ sur $K[x_1, \ldots, x_n]$ conserve la radicalité (respectivement, la maximalité) des idéaux de $K[\underline{X}]$.*

Définition 2.1.21. (voir [12, Définition 2, page 36]) Soit I un idéal de $K[\underline{X}]$. Le *groupe de décomposition* de l'idéal I, noté $\mathrm{Dec}(I)$, est le stabilisateur de I sous l'action de S_n ; c'est à dire l'ensemble des permutations de S_n laissant globalement invariant cet idéal :

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

Le groupe de décomposition d'un idéal I peut être calculé à partir d'une base de Gröbner de I (le calcul de ce groupe dans le cas d'un idéal triangulaire est l'objet du chapitre 4). Le théorème 2.3.7 montre que le groupe de décomposition d'un idéal des relations d'un polynôme (voir Définition 2.3.1) est une représentation symétrique de groupe de Galois de ce polynôme.

Notations 2.1.22. Dans toute la suite, les notations suivantes sont utilisées.

- Pour toute permutation $\sigma \in S_n$ et tout sous-groupe G de S_n, le conjugué $\sigma G \sigma^{-1}$ de G est noté G^σ.
- Soit E un ensemble. Le groupe S_n agit sur l'ensemble des n-uplets d'éléments de E en posant, pour tout $\sigma \in S_n$ et tout $(e_1, e_2, \ldots, e_n) \in E^n$,

$$\sigma.(e_1, e_2, \ldots, e_n) = (e_{\sigma(1)}, e_{\sigma(2)}, \ldots, e_{\sigma(n)}) \ .$$

Remarque 2.1.23. L'action de S_n sur les n-uplets d'éléments de E est une action à droite. En effet, si σ_1 et σ_2 deux permutations de S_n et $(e_1, e_2, \ldots, e_n) \in E^n$, nous avons l'égalité

$$\sigma_1.\,(\sigma_2.(e_1, e_2, \ldots, e_n)) = (\sigma_2\sigma_1)(e_1, e_2, \ldots, e_n) \ .$$

L'usage en théorie de Galois effective est de noter cette action à gauche.

Proposition 2.1.24. *Pour tout idéal I de $K[\underline{X}]$ et toute permutation $\sigma \in S_n$, nous avons les égalités :*

1. $\mathrm{Dec}(\sigma.I) = \mathrm{Dec}(I)^\sigma$;
2. $V(\sigma.I) = \sigma^{-1}.V(I) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid (\alpha_1, \alpha_2, \ldots, \alpha_n) \in V(I)\}$.

Démonstration. La première assertion provient de la suite d'égalité

$$\mathrm{Dec}(\sigma.I) = \{\tau \in S_n \mid (\tau\sigma).I = \sigma.I\} = \{\tau \in S_n \mid \sigma^{-1}\tau\sigma \in \mathrm{Dec}(I)\} = \mathrm{Dec}(I)^\sigma \ .$$

La seconde assertion provient des égalités successives :

$$\begin{aligned} V(\sigma.I) &= \{\underline{\beta} \in \bar{K}^n \mid \forall h \in I,\ (\sigma h)(\underline{\beta}) = 0\} \\ &= \{\underline{\beta} \in \bar{K}^n \mid \forall h \in I,\ h(\sigma.\underline{\beta}) = 0\} \\ &= \{\sigma.\underline{\alpha} \in \bar{K}^n \mid \forall h \in I,\ h(\underline{\alpha}) = 0\} \\ &= \sigma.V(I). \end{aligned}$$

□

La définition ci-dessous, de l'injecteur d'un idéal dans un autre, prolonge celle du fixateur d'un idéal définie dans [61]. Dans le paragraphe 2.4 et les chapitres 4, 5, 6 et 7, nous verrons que cette notion fournit un cadre théorique adapté aux idéaux de Galois : elle permet d'interpréter des calculs, de déterminer la complexité de certains algorithmes mais aussi d'effectuer des précalculs.

Définition 2.1.25. Soient I et J deux idéaux de $K[\underline{X}]$. L'*injecteur de I dans J* est l'ensemble des permutations de S_n défini par :

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

Proposition 2.1.26. *(Voir [61]) Si I est un idéal de $K[\underline{X}]$ alors*

$$\mathrm{Dec}(I) = \mathrm{Inj}(I, I) .$$

Démonstration. Par définition de $\mathrm{Dec}(I)$ et de $\mathrm{Inj}(I, I)$, nous avons l'inclusion $\mathrm{Dec}(I) \subset \mathrm{Inj}(I, I)$.
Montrons l'inclusion réciproque. L'ensemble $\mathrm{Inj}(I, I)$ est un groupe puisque ce sous-ensemble de S_n est stable pour le produit. Soit $\sigma \in \mathrm{Inj}(I, I)$. Nous avons $\sigma^{-1} \in \mathrm{Inj}(I, I)$ et donc simultanément les inclusions $\sigma.I \subset I$ et $\sigma^{-1}.I \subset I$, d'où l'égalité $\sigma.I = I$. Ainsi, nous avons $\mathrm{Inj}(I, I) \subset \mathrm{Dec}(I)$. □

Le groupe de décomposition d'un idéal I est donc le stabilisateur de cet idéal pour l'action naturelle de S_n sur $K[\underline{X}]$. Dans [61], les groupes de décomposition des idéaux intervenants dans les calculs de corps de décomposition sont suffisants pour décrire la variété d'un idéal de Galois ; d'où le terme de fixateur défini dans cet article.

2.2 Idéal des relations symétriques d'un polynôme

Dans toute la suite de ce chapitre, f désigne un polynôme de degré n à coefficients dans K. Quitte à diviser f par le coefficient de son monôme en x^n, nous supposerons le polynôme f unitaire :

$$f(x) = x^n + \sum_{i=1}^{n} (-1)^i a_i \, x^{n-i} .$$

Les n racines de f dans la clôture algébrique $\bar{K}$ de K seront notées $\alpha_1, \ldots, \alpha_n$.

Définition 2.2.1. Pour tout $j \in [\![1, n]\!]$, la $j^{ème}$ *fonction symétrique élémentaire s_j en les n indéterminées $x_1, \ldots, x_n$* est le polynôme de $K[\underline{X}]$ défini par :

$$s_j(\underline{X}) = \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} x_{i_1} \cdots x_{i_j} .$$

Les racines de f vérifient les relations de Newton :

$$\forall j \in [\![1, n]\!], \qquad s_j(\alpha_1, \ldots, \alpha_n) = a_j \ . \tag{2.2.1}$$

Nous sommes alors amenés à poser la définition suivante :

Définition 2.2.2. L'idéal de $K[\underline{X}]$ engendré par les n polynômes

$$s_1(\underline{X}) - a_1,\ s_2(\underline{X}) - a_2,\ \ldots\ ,\ s_n(\underline{X}) - a_n$$

est appelé l'*idéal des relations symétriques de* f.

L'idéal de relations symétriques de f est stable sous l'action de S_n.

Exemple 2.2.3. Considérons le polynôme f de $\mathbb{Q}[X]$ défini par :

$$f(x) = x^6 - 3x^5 - 2x^4 + 9x^3 - x^2 - 4x + 1 \ .$$

L'idéal des relations symétriques de f est engendré par les 6 polynômes :

$$s_1 + 3,\ s_2 - 2,\ s_3 - 9,\ s_4 - 1,\ s_5 + 4,\ s_6 + 1$$

Définitions 2.2.4. (voir [2]) Les *fonctions interpolaires d'Ampère de* f sont les polynômes de $K[\underline{X}]$ définis inductivement par $f_1(x) = f(x)$ et, pour tout $i \in [\![1, n]\!]$,

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

Pour tout $i \in [\![1, n]\!]$, le $i^{ème}$ *module de Cauchy de* f est le polynôme $f_i(x_1,\ \ldots\ , x_{i-1},\ x_i)$.

La proposition suivante est une reformulation modernisée d'un résultat dû à Cauchy.

Proposition 2.2.5. *(voir [17] et [59]) L'idéal des relations symétriques de* f *est engendré par les* n *modules de Cauchy de* f.

Remarquons que, d'après la proposition 2.1.12, l'ensemble triangulaire des n modules de Cauchy de f forme une base de Gröbner de l'idéal des relations symétriques relativement à l'ordre lexicographique.

Exemple 2.2.6. Reprenons l'exemple 2.2.3. D'après la proposition précédente, l'idéal des relations symétriques du polynôme f est engendré par l'ensemble triangulaire de poly-

nômes :

$$\begin{aligned}
f_1(x_1) &= x_1^6 - 3x_1^5 - 2x_1^4 + 9x_1^3 - x_1^2 - 4x_1 + 1\,,\\
f_2(x_1,x_2) &= x_2^5 + x_2^4x_1 - 3x_2^4 + x_2^3x_1^2 - 3x_2^3x_1 - 2x_2^3 + x_2^2x_1^3 - 3x_2^2x_1^2 - 2x_2^2x_1 + 9x_2^2\\
&\quad + x_2x_1^4 - 3x_2x_1^3 - 2x_2x_1^2 + 9x_2x_1 - x_2 + x_1^5 - 3x_1^4 - 2x_1^3 + 9x_1^2 - x_1 - 4\,,\\
f_3(x_1,x_2,x_3) &= x_3^4 + x_3^3x_2 + x_3^3x_1 - 3x_3^3 + x_3^2x_2^2 + x_3^2x_2x_1 - 3x_3^2x_2 + x_3^2x_1^2 - 3x_3^2x_1 - 2x_3^2\\
&\quad + x_3x_2^3 + x_3x_2^2x_1 - 3x_3x_2^2 + x_3x_2x_1^2 - 3x_3x_2x_1 - 2x_3x_2 + x_3x_1^3 - 3x_3x_1^2\\
&\quad - 2x_3x_1 + 9x_3 + x_2^4 + x_2^3x_1 - 3x_2^3 + x_2^2x_1^2 - 3x_2^2x_1 - 2x_2^2 + x_2x_1^3 - 3x_2x_1^2\\
&\quad - 2x_2x_1 + 9x_2 + x_1^4 - 3x_1^3 - 2x_1^2 + 9x_1 - 1\,,\\
f_4(x_1,\ \ldots\ ,x_4) &= x_4^3 + x_4^2x_3 + x_4^2x_2 + x_4^2x_1 - 3x_4^2 + x_4x_3^2 + x_4x_3x_2 + x_4x_3x_1 - 3x_4x_3\\
&\quad + x_4x_2^2 + x_4x_2x_1 - 3x_4x_2 + x_4x_1^2 - 3x_4x_1 - 2x_4 + x_3^3 + x_3^2x_2 + x_3^2x_1\\
&\quad - 3x_3^2 + x_3x_2^2 + x_3x_2x_1 - 3x_3x_2 + x_3x_1^2 - 3x_3x_1 - 2x_3 + x_2^3 + x_2^2x_1\\
&\quad - 3x_2^2 + x_2x_1^2 - 3x_2x_1 - 2x_2 + x_1^3 - 3x_1^2 - 2x_1 + 9\,,\\
f_5(x_1,\ \ldots\ ,x_5) &= x_5^2 + x_5x_4 + x_5x_3 + x_5x_2 + x_5x_1 - 3x_5 + x_4^2 + x_4x_3 + x_4x_2 + x_4x_1\\
&\quad - 3x_4 + x_3^2 + x_3x_2 + x_3x_1 - 3x_3 + x_2^2 + x_2x_1 - 3x_2 + x_1^2 - 3x_1 - 2\,,\\
f_6(x_1,\ \ldots\ ,x_6) &= x_6 + x_5 + x_4 + x_3 + x_2 + x_1 - 3\,.
\end{aligned}$$

Définition 2.2.7. Soient $r \in \mathbb{N}$ et $s \in [\![1,n]\!]$. La $r^{ième}$ *fonction symétrique complète*, notée $h_r(x_1,\ \ldots\ ,x_r)$, est la somme des monômes de degré total r en $x_1,\ \ldots\ ,x_r$. Pour $r=0$, nous posons $h_0(x_1,\ \ldots\ ,x_r)=1$.

La définition 2.2.4 permet de calculer récursivement les modules de Cauchy de f. Le théorème 2.2.8 donne une formule close qui permet de les obtenir sans calcul.

Théorème 2.2.8. *(Machì-Valibouze)(voir [7]) Posons $a_0 = 1$. Pour tout $i \in [\![1,n]\!]$, le module de Cauchy $f_i(x_i)$ de f s'écrit :*

$$f_i(x_i) = \sum_{r=1}^{i} h_r(x_i,\ \ldots\ ,x_n)a_{i-r}\ .$$

2.3 Idéaux des relations entre les racines d'un polynôme

2.3.1 Idéaux des relations et groupe de Galois

Nous supposerons désormais le polynôme f séparable (i.e. sans racine multiple).

Définition 2.3.1. Un idéal I est un *idéal des relations entre les racines de f*, ou plus simplement un *idéal des relations de f*, si I est un idéal maximal de $K[\underline{X}]$ contenant l'idéal des relations symétriques de f.

Exemple 2.3.2. Considérons le polynôme $f(x) = x^6 - 3x^5 - 2x^4 + 9x^3 - x^2 - 4x + 1$ des exemples 2.2.3 et 2.2.6. Les résultats du chapitre 5 permettent d'obtenir une base de Gröbner réduite pour l'ordre lexicographique de l'un des idéaux des relations I de f. Cette base de Gröbner est constituée des polynômes de $\mathbb{Q}[x_1, \ldots, x_6]$:

$$
\begin{aligned}
&x_1^6 - 3x_1^5 - 2x_1^4 + 9x_1^3 - x_1^2 - 4x_1 + 1\,,\\
&x_2 + x_1 - 1\,,\\
&x_3^4 - 2x_3^3 + x_3^2x_1^2 - x_3^2x_1 - 4x_3^2 - x_3x_1^2 + x_3x_1 + 5x_3 + x_1^4 - 2x_1^3 - 4x_1^2 + 5x_1 + 4\,,\\
&x_4 + x_3 - 1\,,\\
&x_5^2 - x_5 + x_3^2 - x_3 + x_1^2 - x_1 - 5\,,\\
&x_6 + x_5 - 1\,.
\end{aligned}
$$

Exemple 2.3.3. Soit f le polynôme de $\mathbb{Q}[x]$ défini par $f(x) = x^8 - x^4 - 1$. Les résultats du chapitre 5 permettent d'obtenir une base de Gröbner de l'un des idéaux des relations de f. Celle-ci est formée des 8 polynômes de $\mathbb{Q}[x_1, \ldots, x_8]$:

$$
\begin{aligned}
&x_1^8 - x_1^4 - 1\,,\\
&x_2 + x_1\,,\\
&x_3^2 + x_1^2\,,\\
&x_4 + x_3\,,\\
&x_5^2 - x_3x_1^5 + x_3x_1\,,\\
&x_6 + x_5\,,\\
&x_7 + x_5x_3x_1^7 - x_5x_3x_1^3\,,\\
&x_8 - x_5x_3x_1^7 + x_5x_3x_1^3\,.
\end{aligned}
$$

Proposition 2.3.4. *Soit I un idéal de $K[\underline{X}]$. Les assertions suivantes sont équivalentes :*

1. *I est un idéal des relations de f ;*
2. *il existe un n-uplet $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \bar{K}^n$ des racines de f tel que I soit le noyau de l'homomorphisme d'évaluation :*

$$
\begin{aligned}
K[x_1, x_2, \ldots, x_n] &\longrightarrow K(\alpha_1, \ldots, \alpha_n)\\
P(x_1, \ldots, x_n) &\longrightarrow P(\alpha_1, \ldots, \alpha_n)\,.
\end{aligned}
$$

Démonstration. Montrons (1) $\Longrightarrow$ (2). Le quotient $K[\underline{X}]/I$ est un corps puisque I est maximal. Par ailleurs, puisque I contient l'idéal des relations symétriques de f, les classes $\alpha_1, \ldots, \alpha_n$ de $x_1, \ldots, x_n$ modulo I vérifient les relations de Newton (Égalités (2.2.1)) et sont donc n racines de f.

Montrons (2) $\Longrightarrow$ (1). Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \bar{K}^n$ un n-uplet des racines de f. L'homomorphisme de l'assertion (2) est surjectif. Le noyau de cet épimorphisme est donc un idéal maximal de $K[x_1, x_2, \ldots, x_n]$. Par ailleurs, les relations de Newton étant vérifiées par $\underline{\alpha}$, l'idéal des relations symétriques appartient au noyau de cet épimorphisme. □

Nous sommes alors amenés à poser la définition suivante.

Définition 2.3.5. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \bar{K}^n$ un n-uplet des racines de f. L'*idéal des $\underline{\alpha}$-relations*, noté $M_{\underline{\alpha}}$, est défini par :

$$M_{\underline{\alpha}} = \{R \in K[\underline{X}] \mid R(\underline{\alpha}) = 0\}.$$

L'idéal $M_{\underline{\alpha}}$ dépend de la numérotation $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ des racines de f : si les racines de f sont réordonnées en un autre n-uplet $\underline{\alpha}'$, l'idéal $M_{\underline{\alpha}'}$ peut être distinct de $M_{\underline{\alpha}}$ (Voir Exemple 2.3.11).

Définition 2.3.6. Le groupe de Galois de $\underline{\alpha}$ sur K, noté $\mathrm{Gal}_K(\underline{\alpha})$, est le groupe de décomposition de l'idéal des $\underline{\alpha}$-relations :

$$\mathrm{Gal}_K(\underline{\alpha}) = \mathrm{Dec}(M_{\underline{\alpha}}) \ (= \{\sigma \in S_n \mid \sigma.M_{\underline{\alpha}} \subset M_{\underline{\alpha}}\}) \ .$$

Cette terminologie se justifie par le fait que le groupe $\mathrm{Dec}(M_{\underline{\alpha}})$ est l'une des représentations dans S_n du groupe de Galois de f sur K comme le montre le théorème suivant.

Théorème 2.3.7. *Soit I un idéal des relations d'un polynôme séparable f. Alors,*

1. *le quotient $K[\underline{X}]/I$ est un corps de décomposition de f ;*
2. *le groupe de décomposition de I est un groupe de Galois de f sur K.*

Démonstration. L'assertion (1) provient de la proposition 2.3.4 (rappelons que les racines $\alpha_1, \ldots, \alpha_n$ de f dans $K[\underline{X}]/I$ sont les classes des monômes $x_1, \ldots, x_n$ modulo I).

Montrons (2). Notons ϕ l'application qui, par passage au quotient, associe à toute permutation σ du groupe de décomposition, identifiée à l'automorphisme quelle induit, associe l'automorphisme $\bar{\sigma}$ de $\mathrm{Gal}_K(K[\underline{X}]/I)$.

Montrons que cette application est injective. Soient σ_1 et σ_2 deux permutations de $\mathrm{Dec}(I)$ telles que $\bar{\sigma_1} = \bar{\sigma_2}$. Pour tout $i \in [\![1, n]\!]$, il vient alors $\bar{\sigma_1}(\underline{\alpha}_i) - \bar{\sigma_2}(\underline{\alpha}_i) = 0$, ce qui s'écrit, compte-tenu de la définition de l'application ϕ, $\sigma_1(x_i) - \sigma_2(x_i) \in I$. Ainsi, nous avons, pour tout $i \in [\![1, n]\!]$, $x_{\sigma_1(i)} - x_{\sigma_2(i)} \in I$. Les monômes $x_1, \ldots, x_n$ étant tous distincts modulo I, les permutations σ_1 et σ_2 sont égales.

Montrons la surjectivité de ϕ. Soit $g \in \mathrm{Gal}_K(K[\underline{X}]/I)$, l'automorphisme g induit une permutation $\tau \in S_n$ sur les $\alpha_1, \ldots, \alpha_n$. Puisque I est un idéal maximal, il en est de même de l'idéal $\tau(I)$. Pour conclure, il suffit de montrer que nous avons l'inclusion $\tau(I) \subseteq I$, car, d'après la proposition 2.1.26, nous aurons alors $\tau.I = I$.

Raisonnons par l'absurde en supposant que nous ayons $\tau(I) \nsubseteq I$. Par maximalité, nous avons alors $I + \tau(I) = K[\underline{X}]$. Il existerait alors deux polynômes P et Q de I tels que $P + \tau.Q = 1$. Cette dernière égalité évaluée en $(\alpha_1, \ldots, \alpha_n)$ donne alors successivement :

$$\begin{aligned}
1 &= P(\alpha_1, \ldots, \alpha_n) + \tau.Q(\alpha_1, \ldots, \alpha_n) \\
&= 0 + Q(\bar{\tau}(\alpha_1), \ldots, \bar{\tau}(\alpha_n)), \text{ par définition de } \bar{\tau}, \\
&= \bar{\tau}(Q(\alpha_1, \ldots, \alpha_n)), \text{ car } \bar{\tau} \text{ définit un automorphisme d'algèbre,} \\
&= \bar{\tau}(0), \text{ car } Q \in I, \\
&= 0, \text{ car } \tau \in \mathrm{Gal}_K(K[\underline{X}]/I), .
\end{aligned}$$

Ce qui est absurde. L'application ϕ est donc surjective. □

Exemple 2.3.8. Poursuivons l'exemple 2.3.2. Le groupe de décomposition de l'idéal des relations I est le sous-groupe de S_6 engendré par les permutations

$$(6,5),\ (4,3),\ (6,4)(5,3),\ (2,1) \text{ et } (4,2)(3,1).$$

D'après le théorème 2.3.7, ce groupe est l'une des représentations symétriques dans S_6 du groupe de Galois du polynôme $f(x) = x^6 - 3x^5 - 2x^4 + 9x^3 - x^2 - 4x + 1$.

Remarque 2.3.9. Dans [34], L. Kronecker construit un corps de décomposition d'un polynôme par factorisations successives (voir [22] pour reformulation modernisée de la démarche de Kronecker). Cette construction aboutit à un idéal des relations du polynôme.

2.3.2 Action de S_n sur les idéaux de relations

D'après le théorème précédent, la donnée d'un idéal des relations de f permet de définir un corps de décomposition de f. Pour déterminer l'ensemble des idéaux de relations de f, il est suffisant de préciser l'action de S_n sur l'ensemble des idéaux de relations de f. En effet, cet ensemble d'idéaux ne forme qu'une seule orbite sous l'action de S_n comme le montre la proposition suivante.

Proposition 2.3.10. *Le groupe S_n agit transitivement sur l'ensemble des idéaux de relations de f. De plus, en notant $M_{\underline{\alpha}}$ un idéal des relations de f, nous avons, pour tout $\sigma \in S_n$:*

$$\sigma.M_{\underline{\alpha}} = M_{\sigma^{-1}.\underline{\alpha}}\,; \tag{2.3.1}$$

$$\mathrm{Dec}(\sigma.M_{\underline{\alpha}}) = \mathrm{Gal}_K(\underline{\alpha})^{\sigma}\ (= \mathrm{Gal}_K(\sigma.\underline{\alpha}))\ . \tag{2.3.2}$$

Démonstration. Soient I et I' deux idéaux de relations de f. Montrons qu'il existe une permutation $\tau \in S_n$ telle que $\tau.I = I'$. Notons $\bar{\tau}$ le K-isomorphisme de $K[\underline{X}]/I = K(\alpha_1, \ldots, \alpha_n)$ sur $K[\underline{X}]/I' = K(\alpha'_1, \ldots, \alpha'_n)$:

$$\begin{array}{ccc} K[x_1, \ldots, x_n] & \longrightarrow & K[\underline{X}]/I = K(\alpha_1, \ldots, \alpha_n) \\ \downarrow \tau & & \downarrow \bar{\tau} \\ K[x_1, \ldots, x_n] & \longrightarrow & K[\underline{X}]/I' = K(\alpha'_1, \ldots, \alpha'_n)\ . \end{array}$$

L'application $\bar{\tau}$ étant un K-isomorphisme, les images $\bar{\tau}(\alpha_1), \ldots, \bar{\tau}(\alpha_n)$ sont les n racines distinctes de f dans $K[\underline{X}]/I' = K(\alpha'_1, \ldots, \alpha'_n)$. Il existe donc une unique permutation $\tau \in S_n$ tel que

$$\forall i \in [\![1, n]\!],\ \bar{\tau}(\alpha_{\tau(i)}) = \alpha'_i\ .$$

Soit $P \in I'$. Par définition de I', nous avons $P(\alpha'_1, \ldots, \alpha'_n) = 0$; ce qui s'écrit encore

$$P(\bar{\tau}(\alpha_{\tau(1)}), \ldots, \bar{\tau}(\alpha_{\tau(n)})) = 0 \ .$$

L'application $\bar{\tau}$ étant un K-isomorphisme, nous obtenons,

$$\begin{aligned} \bar{\tau}(P(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})) &= 0 \text{ , puis,} \\ P(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) &= 0 \ . \end{aligned}$$

Cette dernière égalité montre que $\tau.P(\alpha_1, \ldots, \alpha_n) = 0$. Il vient alors $\tau.P \in I$, puis l'inclusion $\tau.I' \subset I$. L'idéal I' étant maximal, il s'en suit l'égalité $\tau.I = I'$.

L'égalité (2.3.1) provient directement de la définition de $M_{\underline{\alpha}}$ et l'égalité (2.3.2) est une conséquence de la proposition 2.1.24. □

Exemple 2.3.11. Poursuivons l'exemple 2.3.2. Notons σ la transposition $(2,3)$ du groupe symétrique S_6. La base de Gröbner réduite pour l'ordre lexicographique de l'idéal $\sigma.I$ est :

$$\begin{array}{l} x_1^6 - 3x_1^5 - 2x_1^4 + 9x_1^3 - x_1^2 - 4x_1 + 1, \\ x_2^4 - 2x_2^3 + x_2^2x_1^2 - x_2^2x_1 - 4x_2^2 - x_2x_1^2 + x_2x_1 + 5x_2 + x_1^4 - 2x_1^3 - 4x_1^2 + 5x_1 + 4, \\ x_3 + x_1 - 1, \\ x_4 + x_2 - 1, \\ x_5^2 - x_5 + x_2^2 - x_2 + x_1^2 - x_1 - 5, \\ x_6 + x_5 - 1 \ . \end{array}$$

Les bases de Gröbner réduites des idéaux I et $\sigma.I$ étant différentes, ces idéaux sont donc deux idéaux de relations distincts du polynôme

$$f(x) = x^6 - 3x^5 - 2x^4 + 9x^3 - x^2 - 4x + 1 \ .$$

Une conséquence immédiate de la proposition 2.3.10 est le résultat suivant.

Proposition 2.3.12. *Il existe* $n!/\operatorname{Card}(\operatorname{Gal}_K(f))$ *idéaux de relations de* f.

Démonstration. Reprenons les notations de la proposition précédente. Le stabilisateur pour l'action de S_n sur l'ensemble des idéaux des relations de l'idéal $M_{\underline{\alpha}}$ est le groupe $\operatorname{Gal}_K(\underline{\alpha})$. Le groupe S_n agissant transitivement sur l'ensemble des idéaux des relations de f, la formule de Lagrange montre que le nombre de ces idéaux est égal à $n!/\operatorname{Card}(\operatorname{Gal}_K(\underline{\alpha}))$. Le théorème 2.3.7 prouve alors le résultat. □

Il existe donc $n!/\operatorname{Card}(\operatorname{Gal}_K(f))$ représentations du corps de décomposition de f sous forme d'algèbre quotient de $K[\underline{X}]$ par un idéal des relations de ce polynôme.

2.4 Idéaux de Galois d'un polynôme

2.4.1 Définition et premières propriétés

Définition 2.4.1. Un *idéal de Galois de f* est un idéal propre de $K[\underline{X}]$ contenant l'idéal des relations symétriques de f.

Exemple 2.4.2. Un des idéaux de Galois du polynôme $f(x) = x^8 - x^4 - 1$ de l'exemple 2.3.3 est engendré par les polynômes :

$$\begin{aligned}
&x_1^8 - x_1^4 - 1\,,\\
&x_2 + x_1\,,\\
&x_3^2 + x_1^2\,,\\
&x_4 + x_3\,,\\
&x_5^4 + x_1^4 - 1\,,\\
&x_6^3 + x_6^2 x_5 + x_6 x_5^2 + x_5^3\,,\\
&x_7^2 + x_7 x_6 + x_7 x_5 + x_6^2 + x_6 x_5 + x_5^2\,,\\
&x_8 + x_7 + x_6 + x_5\,.
\end{aligned}$$

(Il s'agit de l'idéal induit de l'idéal de rupture du polynôme f ; ce type d'idéal de Galois est défini au chapitre 5.)

Tout idéal de Galois vérifie le critère de radicalité de Seidenberg ci-dessous.

Théorème 2.4.3. *(voir [8]) Soit I un idéal de $K[\underline{X}]$ de dimension nulle. Supposons que, pour tout $i \in [\![1, n]\!]$, il existe un polynôme séparable $g_i \in K[x_i]$ tel que $g_i(x_i) \in I$. Alors, l'idéal I s'écrit comme intersection d'un nombre fini d'idéaux premiers et est, en particulier, radical.*

Corollaire 2.4.4. *Soient K_1, K_2 deux extensions algébriques de K telles que $K_1 \subset K_2$. Si I (resp. J) est un idéal de Galois de $K_1[x_1, \ldots, x_n]$ (resp. $K_2[x_1, \ldots, x_n]$) alors les deux idéaux suivants sont des idéaux de Galois :*

1. *L'idéal de $K_2[x_1, \ldots, x_n]$ engendré par I. Cet idéal est obtenu par extension des scalaires et s'exprime sous la forme du produit tensoriel $K_2 \otimes_{K_1} I$.*
2. *L'idéal $K_1[x_1, \ldots, x_n] \cap J$ trace de J dans $K_1[x_1, \ldots, x_n]$.*

Injecteurs et variété d'un idéal de Galois

La proposition suivante éclaire le lien entre variété correspondante à un idéal de Galois et la notion d'injecteur (voir Définition 2.1.25).

Proposition 2.4.5. *(voir [61]) Si I est un idéal de Galois de f et $M_{\underline{\alpha}}$ l'idéal des $\underline{\alpha}$-relations de f, alors*

$$V(I) = \mathrm{Inj}(I, M_{\underline{\alpha}}).\underline{\alpha} \tag{2.4.1}$$

et, comme le polynôme f est séparable,

$$\mathrm{Card}(\mathrm{Inj}(I, M_{\underline{\alpha}})) = \mathrm{Card}(V(I)). \tag{2.4.2}$$

Reprenons les notations de la proposition précédente. Dans [61], A. Valibouze s'intéresse à l'ensemble des parties $\mathcal{P}$ de S_n telles que

$$I = \{R \in K[\underline{X}] \mid \forall \sigma \in \mathcal{P},\ (\sigma.R)(\underline{\alpha}) = 0\}\,.$$

Cet ensemble admet un plus grand élément L et la variété de l'idéal I est alors donnée par l'égalité $V(I) = L.\underline{\alpha}$ (voir Définition 1.13 et Proposition 3.17 de [61]). La notion d'injecteur est plus adaptée à l'étude du treillis des idéaux de Galois et aux résultats qui s'y rattachent.

Remarque 2.4.6. L'identité (2.4.1) fait apparaître que l'idéal I est entièrement déterminé par un n-uplet de $\overline{K}$ sur lequel il s'annule et par son injecteur relatif à ce n-uplet. Ainsi, l'injecteur $\mathrm{Inj}(I, M_{\underline{\alpha}})$ est de nature géométrique. En effet, pour toute extension algébrique K' de K, nous avons :

$$\mathrm{Inj}(I, \underline{\alpha}) = \mathrm{Inj}(K' \otimes_K I, M_{\underline{\alpha}})\,. \tag{2.4.3}$$

Notations 2.4.7. Pour tout $P_1 \subset S_n$ et tout $P_2 \subset S_n$, nous notons $P_1\ P_2$ la partie de S_n définie par :

$$P_1\ P_2 = \{\, \pi_1 \pi_2 \mid \pi_1 \in P_1,\ \pi_2 \in P_2 \,\}\,.$$

Définition 2.4.8. Nous appellerons *injecteur de I* tout injecteur de I dans l'un des idéaux maximaux qui le contient.

Proposition 2.4.9. *Si I est un idéal de Galois de f et $L = \mathrm{Inj}(I, M_{\underline{\alpha}})$ l'injecteur de I dans l'idéal $M_{\underline{\alpha}}$ des $\underline{\alpha}$-relations de f alors*

1. *L'ensemble des idéaux de relations de f contenant I est $\{M_{\sigma.\underline{\alpha}} \mid \sigma \in L\}$;*
2. *Si $\sigma \in S_n$ alors l'injecteur $\mathrm{Inj}(I, M_{\sigma.\underline{\alpha}})$ s'écrit*

$$\mathrm{Inj}(I, M_{\sigma.\underline{\alpha}}) \ = \ \sigma^{-1}L. \tag{2.4.4}$$

En particulier, l'ensemble des injecteurs de I est $\{\sigma^{-1}L \mid \sigma \in L\}$.

Démonstration. Assertion 1. D'après le théorème 2.3.7, tout idéal des relations de f s'écrit $M_{\underline{\beta}}$ où $\underline{\beta} \in S_n.\underline{\alpha}$. De plus, si $I \subset M_{\underline{\beta}}$ alors $V(I) \subset M_{\underline{\beta}}$. D'après la proposition 2.4.5, il existe $\ell \in L$ tel que $\underline{\beta} = \ell.\underline{\alpha}$. Ainsi, tout idéal des relations contenant I appartient à $\{M_{\sigma.\underline{\alpha}} \mid \sigma \in L\}$. Réciproquement, si $\sigma \in L$, nous avons $\sigma.\underline{\alpha} \in V(I)$ puis $I \subset M_{\underline{\alpha}}$.

Assertion 2. Par définition de l'injecteur, il vient :

$$\begin{aligned}\mathrm{Inj}(I, M_{\sigma.\underline{\alpha}}) &= \mathrm{Inj}(I, \sigma.M_{\underline{\alpha}}) \\ &= \{\tau \in S_n \,|\, \tau.I \subset \sigma.M_{\underline{\alpha}}\} \\ &= \{\tau \in S_n \,|\, \sigma^{-1}\tau.I \subset M_{\underline{\alpha}}\} \\ &= \sigma\{\rho \in S_n \,|\, \rho.I \subset M_{\underline{\alpha}}\} = \sigma\,\mathrm{Inj}(I, M_{\underline{\alpha}})\ .\end{aligned}$$

□

Action de S_n sur les idéaux de Galois

La proposition suivante précise l'action du groupe symétrique S_n sur l'ensemble des idéaux de Galois de f.

Proposition 2.4.10. *L'ensemble des idéaux de Galois de f est stable sous l'action du groupe symétrique S_n. De plus, si σ désigne une permutation de S_n, nous avons :*

$$\mathrm{Inj}(\sigma.I, M_{\underline{\alpha}}) = \mathrm{Inj}(I, M_{\underline{\alpha}})\sigma^{-1}; \tag{2.4.5}$$

$$V(\sigma.I) = \mathrm{Inj}(I, M_{\underline{\alpha}})\sigma^{-1}.\,\underline{\alpha}\,. \tag{2.4.6}$$

Démonstration. L'égalité (2.4.5) est une conséquence immédiate de la définition d'un injecteur. L'égalité (2.4.6) se déduit de l'expression de la variété donnée par l'égalité (2.4.1). □

Une conséquence immédiate de la définition du groupe de décomposition et des injecteurs d'un idéal de Galois est la proposition suivante :

Proposition 2.4.11. *Si I est un idéal de Galois de f et $M_{\underline{\alpha}}$ l'idéal des $\underline{\alpha}$-relations de f, alors*

$$\mathrm{Inj}(I, M_{\underline{\alpha}})\ \mathrm{Dec}(I) = \mathrm{Inj}(I, M_{\underline{\alpha}})\ .$$

Idéaux de Galois purs

La proposition suivante éclaire le cas des idéaux de Galois d'unique injecteur le groupe de décomposition.

Proposition 2.4.12. *(voir [61]) Si I est un idéal de Galois de f et $M_{\underline{\alpha}}$ l'idéal des $\underline{\alpha}$-relations de f alors les conditions suivantes sont équivalentes :*

1. $\mathrm{Inj}(I, M_{\underline{\alpha}})$ *est un groupe ;*
2. $\mathrm{Inj}(I, M_{\underline{\alpha}}) = \mathrm{Dec}(I)$ *;*
3. $\mathrm{Card}(\mathrm{Dec}(I)) = \prod_{i=1}^{n} \deg_{x_i}(I)$ *;*
4. $\mathrm{Gal}_K(\underline{\alpha}) \subseteq \mathrm{Dec}(I)$.

Si l'une de ces assertions est vérifiée, l'idéal I n'admet qu'un seul injecteur : le groupe $\mathrm{Dec}(I)$. *Nous parlerons alors de l'injecteur de I.*

Définition 2.4.13. Un *idéal de Galois pur* est un idéal de Galois vérifiant l'une des conditions équivalentes de la proposition 2.4.12.

Tout idéal des relations symétriques d'un polynôme ainsi que tout idéal des relations entre les racines d'un polynôme admet pour unique injecteur son groupe de décomposition : ce sont des idéaux de Galois purs.

2.4.2 Correspondance entre idéaux de Galois et parties de S_n

Triangularité des idéaux de Galois

L'égalité (2.4.1) met en bijection variété d'un idéal de Galois et permutations de l'un de ces injecteurs. Ceci permet de transposer aux idéaux de Galois le théorème 2.1.17 de P. Aubry et A. Valibouze (voir Corollaire 2.4.17).

Notations 2.4.14. Pour tout groupe $H \subset S_n$, dans [7] il est montré comment calculer, à partir de H, une liste identique à $\mathcal{L}(J)$ pour tout idéal de Galois J ayant H comme injecteur. Cette liste est notée $\mathcal{L}(H)$.

Proposition 2.4.15. *Soit I un idéal de Galois triangulaire et L l'un des injecteurs de I. Nous avons*

$$\mathrm{Card}(V(I)) = \prod_{i=1}^{n} \deg_{x_i}(I) = \mathrm{Card}(L). \tag{2.4.7}$$

Définition 2.4.16. Soient $\sigma \in S_n$ et $k \in [\![1, n]\!]$. Le *préfixe de longueur k* de σ est le k-uplet $[\sigma(1), \ldots, \sigma(k)]$.

Une partie L de S_n est dite *équiprojectable* si, pour tout $k \in [\![1, n]\!]$ et toute permutation $\sigma \in L$, le cardinal c de l'ensemble des permutations de L admettant $[\sigma(1), \ldots, \sigma(k)]$ pour préfixe de longueur k ne dépend que de k :

$$\#\left(\{\tau \in L \mid \forall i \in [\![1, k]\!],\ \sigma^{-1}\tau(i) = i\}\right) = c\,.$$

Le corollaire ci-dessous, du à P. Aubry et A. Valibouze, est une conséquence immédiate du théorème 2.1.17 appliqué aux idéaux de Galois.

Corollaire 2.4.17. *(voir [7]) Soit L l'un des injecteurs d'un idéal de Galois I. Les assertions suivantes sont équivalentes :*

- *il existe un ensemble triangulaire $T = \{f_1, f_2, \ldots, f_n\}$ engendrant I ;*
- *L est équiprojectable ;*

De plus, si l'une de ces deux conditions équivalentes est vérifiée, le degré de chacun des polynômes f_i en x_i est donné par :

$$\deg_{x_i}(f_i) = \mathrm{Card}(L_{i-1})/\,\mathrm{Card}(L_i).$$

Les conditions équivalentes ci-dessus sont en particulier vérifiées lorsque L est un sous-groupe de S_n (i.e. lorsque la Proposition 2.4.12 est vérifiée) comme, par exemple, dans le cas des idéaux de relations (voir Théorème 2.3.7).

Proposition 2.4.18. *(Voir [7]) Si le groupe* $\mathrm{Dec}(I)$ *est l'injecteur de I alors I est un idéal triangulaire.*

Décomposition d'un idéal de Galois

Proposition 2.4.19. *Soient I et $M_1, \ldots, M_m$ des idéaux de Galois de f. Supposons que l'idéal I admette pour décomposition*

$$I = \bigcap_{i=1}^{m} M_i \,; \tag{2.4.8}$$

Les conditions suivantes sont alors équivalentes.

1. *Les idéaux $M_1, \ldots, M_m$ sont deux à deux comaximaux ;*
2. *L'injecteur* $\mathrm{Inj}(I, M_{\underline{\alpha}})$ *est égal à l'union disjointe :*

$$\mathrm{Inj}(I, M_{\underline{\alpha}}) = \mathrm{Inj}(M_1, M_{\underline{\alpha}}) \cup \cdots \cup \mathrm{Inj}(M_m, M_{\underline{\alpha}})\,. \tag{2.4.9}$$

Démonstration. Les idéaux $M_1, \ldots, M_m$ sont comaximaux si et seulement si la variété $V(I)$ est l'union disjointe des variétés des idéaux $M_1, \ldots, M_m$. D'après l'égalité (2.4.1), ceci équivaut à la seconde assertion. □

Correspondance entre idéaux de Galois et injecteurs

Les deux propositions suivantes, dues à A. Valibouze, caractérisent les parties de S_n qui sont les injecteurs d'idéaux de Galois de f.

Notations 2.4.20. Pour toute partie non vide L de S_n, l'idéal de $K[\underline{X}]$ s'annulant sur l'ensemble $L.\underline{\alpha}$ est noté $Id(L.\underline{\alpha})$:

$$Id(L.\underline{\alpha}) = \{P \in K[\underline{X}] \mid \forall \underline{\beta} \in L.\underline{\alpha},\ P(\underline{\beta}) = 0\}\,.$$

Proposition 2.4.21. *(voir [61]) L'idéal $Id(L.\underline{\alpha})$ est un idéal de Galois de f d'injecteur* $\mathrm{Inj}(I, M_{\underline{\alpha}}) = \mathrm{Gal}_K(\underline{\alpha})L$.

Proposition 2.4.22. *(voir [61]) Soit L une partie non vide de S_n. Les assertions suivantes sont équivalentes :*

1. $L = \mathrm{Gal}_K(\underline{\alpha})L$;
2. *il existe un idéal de Galois d'injecteur L.*

Le Nullstelensatz et les deux propositions précédentes permettent d'établir le dictionnaire suivant entre idéaux de Galois d'un polynôme séparable f et parties de S_n stable par translation à gauche par toute permutation du groupe $\mathrm{Gal}_K(\underline{\alpha})$ (i.e. les parties $L \subseteq S_n$ telles que $L = \mathrm{Gal}_K(\underline{\alpha})L$).

Théorème 2.4.23. *Notons $\mathcal{I}$ l'ensemble des idéaux de Galois de f et $\mathcal{P}(S_n)^{\mathrm{Gal}_K(\underline{\alpha})}$ l'ensemble des parties L stable par translation à gauche par les permutations du groupe $\mathrm{Gal}_K(\underline{\alpha})$.*

L'application qui associe à $I \in \mathcal{I}$ l'injecteur $\mathrm{Inj}(I, M_\alpha) \in \mathcal{P}(S_n)^{\mathrm{Gal}_K(\underline{\alpha})}$ et l'application qui a $L \in \mathcal{P}(S_n)^{\mathrm{Gal}_K(\underline{\alpha})}$ associe l'idéal de Galois $Id(L.\underline{\alpha})$ définissent des bijections réciproques décroissantes pour l'inclusion.

De plus, nous avons la correspondance suivante :

$\mathcal{I}$	$\longleftrightarrow$	$\mathcal{P}(S_n)^{\mathrm{Gal}_K(\underline{\alpha})}$
$Id(L.\underline{\alpha})$	$\longleftarrow$	L
I	$\longrightarrow$	$\mathrm{Inj}(I, M_\alpha)$
$\sigma.I$	$\longrightarrow$	$\mathrm{Inj}(I, M_\alpha)\sigma^{-1}$
$I_1 \cap I_2$	$\longrightarrow$	$\mathrm{Inj}(I_1, M_\alpha) \cup \mathrm{Inj}(I_2, M_\alpha)$
$I_1 + I_2$	$\longrightarrow$	$\mathrm{Inj}(I_1, M_\alpha) \cap \mathrm{Inj}(I_2, M_\alpha)$
I_1 *et* I_2 *comaximaux*	$\longrightarrow$	$\mathrm{Inj}(I_1, M_\alpha)$ *et* $\mathrm{Inj}(I_2, M_\alpha)$ *disjoints*
I *triangulaire*	$\longrightarrow$	$\mathrm{Inj}(I, M_\alpha)$ *équiprojectable*

où σ désigne une permutation de S_n.

Un premier exemple d'idéal de Galois non triangulaire est présenté dans la thèse de G. Renault (voir [29]). Cet idéal est l'intersection de deux idéaux de Galois ; ceci traduit le fait que l'ensemble des parties équiprojectables de S_n n'est pas stable pour l'union ensembliste.

Chapitre 3

Corps de rupture et groupes de Galois

Dans ce chapitre, nous étudions le lien entre factorisation d'un polynôme sur l'un de ses corps de rupture et groupe de Galois de ce polynôme.

Soit f un polynôme irréductible à coefficients dans un corps parfait K. Dans [9], [45] ou [60], les auteurs présentent des algorithmes permettant de factoriser f sur l'un de ses corps de rupture K. Dans [55], J. McKay et L. Soicher utilisent des calculs de résolvantes linéaires pour déterminer le groupe de Galois de f sur K. Les tables présentées dans ce chapitre, appelées *tables de rupture*, utilisent les degrés et les facteurs irréductibles de f sur K. Elles complètent celles de J. McKay et L. Soicher,

- en précisant les groupes de Galois des facteurs irréductibles de f sur le corps de rupture K ;
- en permettant de déterminer certains polynômes apparaissant dans une base de Gröbner d'un idéal des relations de f.

La construction des tables est l'objet du paragraphe 3.1. Cette construction repose uniquement sur les listes des sous-groupes transitifs de S_n (voir [16] et [31]).
Dans le paragraphe 3.2, la proposition 3.2.4 montre que les degrés et les groupes de Galois des facteurs irréductibles de f sur K dépendent uniquement de $\mathrm{Gal}_K(f)$. Nous ferons alors le lien entre tables de rupture et groupes de Galois.
Le paragraphe 3.3 est consacré aux applications de ces tables :

- détermination de groupes de Galois ;
- factorisation d'un polynôme sur l'un de ses corps de rupture ;
- calcul de corps de décomposition ;
- recherche d'un polynôme de groupe de Galois donné.

Les tables de ruptures en degré n pour $n \in \{3, \ldots, 10\}$ sont jointes en annexe (Annexe A). Les tables en degré n pour $n \in \{11, \ldots, 23\}$ sont disponibles à l'adresse `ftp ://ftp.lip6.fr/lip6/reports/2005/`.

Ce travail a été réalisé en collaboration avec G. Renault et A. Valibouze et est l'objet de l'article préliminaire [].

3.1 Les tables de rupture

Dans ce paragraphe, est défini l'objet central de ce chapitre : *les tables de rupture*.

3.1.1 Notations

Dans la suite de ce chapitre, nous allons utiliser les notations suivantes.

- Conformément à la nomenclature de Butler et McKay (voir [16]), nT_i désigne le i-ème groupe de la liste $\mathcal{T}(n)$ des sous-groupes transitifs de S_n (cette liste fournit un représentant par classe de S_n-conjugaison). La notation nT_i est complétée en y adjoignant un exposant $+$ (resp. $*$) lorsque le groupe G est pair (resp. résoluble).
- L'ensemble des groupes des listes $\mathcal{T}(n)$ est muni de la relation d'ordre $\ll$ définie par :

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

- 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 $\mathcal{O}$.
- Pour tout sous-groupe G de S_n et toute partie $\mathcal{P} \subset \{1, \ldots, n\}$, le fixateur de $\mathcal{P}$ dans G est noté $\mathrm{Fix}_{\mathcal{P}}(G)$:

$$\mathrm{Fix}_{\mathcal{P}}(G) = \{g \in G \mid \forall i \in \mathcal{P},\ g(i) = i\} \ .$$

Pour simplifier les notations, nous utilisons la notation exponentielle. Par exemple :

- la suite d'entiers $1, 1, 1, 1, 2, 3, 3, 3, 4, 4$ est représentée par $1^4, 2, 3^3, 4^2$;
- la suite de groupes $1T_1$, $2T_1$, $2T_1$, $4T_2$, $4T_3$, $4T_3$, $4T_3$ est représentée par $1T_1$, $2T_1^2$, $4T_2$, $4T_3^3$.

3.1.2 Définition des tables de rupture

Dans tout ce paragraphe, G désigne un sous-groupe fixé de S_n et nous considérons l'ensemble des orbites $\mathcal{O}(G)$ de $\{1, \ldots, n\}$ sous l'action du groupe $\mathrm{Fix}_{\{1\}}(G)$.

Pour chaque orbite $\mathcal{O} \in \mathcal{O}(G)$, l'action transitive de $\mathrm{Fix}_{\{1\}}(G)$ sur $\mathcal{O}$ est identifiée à celle du sous-groupe $G_{\mathcal{O}} \in \mathcal{T}(\mathrm{Card}(\mathcal{O}))$ de $S_{\mathcal{O}}$.

Notons :

- $S(G)$ la suite croissante (pour l'ordre $\ll$) des groupes $G_{\mathcal{O}}$ où $\mathcal{O}$ parcourt $\mathcal{O}(G)$.
- $D(G)$ la suite des degrés des groupes de la liste $S(G)$ (i.e. la suite croissante des cardinaux des orbites de $\mathcal{O}(G)$).

Choisissons un groupe G' dans la classe de S_n-conjugaison de G tel que $\mathrm{Fix}_{\{1\}}(G')$ soit égal au produit direct des groupes de la suite croissante $S(G)$.

Nous noterons $\mathcal{L}(G)$ la liste $[d_1 = n, \ldots, d_n = 1]$ définie par :

- $d_1 = \mathrm{Card}(G')/\mathrm{Card}(\mathrm{Fix}_{\{1\}}(G')\})$ et,
- pour tout $i \in [\![2, n]\!]$, $d_i = \mathrm{Card}(\mathrm{Fix}_{\{1,\ \ldots,i-1\}}(G'))/\mathrm{Card}(\mathrm{Fix}_{\{1,\ \ldots,i\}}(G')\})$.

Remarque 3.1.1. Soit G' l'un des S_n-conjugué de G. Nous avons les égalités $S(G) = S(G')$ et $D(G) = D(G')$. Toutefois, la liste $\mathcal{L}(G')$ n'est pas nécessairement égale à $\mathcal{L}(G)$. Pour chaque groupe G de la table de rupture, nous avons choisi l'une des listes $\mathcal{L}(G)$ définies ci-dessus.

La table contenant les suites $S(G)$, où G parcourt $\mathcal{T}(n)$, est appelée la *table de rupture en degré* n. Pour tout groupe G de la table de rupture, sont adjointes la suite $D(G)$ et l'une des suites $\mathcal{L}(G)$ décrites ci-dessus.

3.1.3 Construction des tables de rupture

Les tables ont été produites à l'aide du logiciel de calcul formel Magma (voir [11]) dans lequel ont étés implantées les fonctions calculant les listes $\mathcal{L}(G)$ et les suites $S(G)$ et $D(G)$. La base de données des groupes de $\mathcal{T}(m)$ pour $m \leq 23$ est disponible dans ce logiciel.

Chaque ligne de la table de rupture en degré n correspond à un groupe G de $\mathcal{T}(n)$. Les lignes des tables sont ordonnées en respectant les règles suivantes.
Pour tout groupe G et H de $\mathcal{T}(n)$,

- si $S(G) \neq S(H)$ et si $S(G)$ est inférieur à $S(H)$ pour l'ordre lexicographique induit par $\ll$, la ligne correspondante à G est placée avant celle de H ;
- si $S(G) = S(H)$ et si $G \ll H$, la ligne correspondante à G est placée avant celle de H.

Exemple 3.1.2. Décrivons la construction de la table en degré 3. Pour ce degré, il y a deux groupes transitifs : $3T_1 = A_3$ et $3T_2 = S_3$.

Dans le cas de $3T_1$, le groupe $\mathrm{Fix}_{\{1\}}(3T_1)$ étant réduit à la permutation identité, les orbites de $\{1, 2, 3\}$ sous l'action du groupe $\mathrm{Fix}_{\{1\}}(3T_1)$ sont $\{1\}, \{2\}$ et $\{3\}$ et l'action de $\mathrm{Fix}_{\{1\}}(3T_1)$ sur chacune de ces orbites est triviale. Nous avons donc $D(3T_1) = 1^3$ et $S(3T_1) = 1T_1, 1T_1, 1T_1$.

Dans le cas de $3T_2$, les orbites de $\{1, 2, 3\}$ sous l'action de $\mathrm{Fix}_{\{1\}}(3T_2)$ sont $\{1\}$ et $\{2, 3\}$. L'action de ce groupe sur la seconde orbite s'identifie à celle du groupe $2T_1$. Nous obtenons donc $D(3T_2) = 1, 2$ et $S(3T_2) = 1T_1, 2T_2$.

3.2 Tables de rupture et groupes de Galois

Dans ce paragraphe, nous établissons le lien entre tables de rupture et groupes de Galois. Un polynôme irréductible f de degré n à coefficients dans un corps parfait K étant donné, nous notons $\mathrm{Gal}_K(f)$ le groupe de Galois de f sur K. Le polynôme f étant irréductible, son groupe de Galois s'identifie un sous groupe transitif G_f de S_n. Nous noterons α_1 l'une des racines de f dans une clôture algébrique de K.

3.2.1 Degrés et groupes de Galois des facteurs de rupture

Définition 3.2.1. Les $s > 1$ facteurs irréductibles

$$g_1(\alpha_1, X) = X - \alpha_1,\ g_2(\alpha_1, X),\ \ldots,\ g_s(\alpha_1, X)$$

de f sur $K' = k(\alpha_1)$ sont appelés les *facteurs de rupture de* f, et seront rangés dans l'ordre croissant de leur degrés.

Pour tout $i \in [\![1, s]\!]$, le groupe de Galois g_i sur k est isomorphe à l'un des groupes G_i de $\mathcal{T}(\deg_X(g_i))$. Quitte à ré-indexer les polynômes g_i, nous supposerons la suite $G_1, \ldots, G_n$ croissante pour l'ordre $\ll$.

Définition 3.2.2. La suite $D(f) = \deg_X(g_1), \ldots, \deg_X(g_s)$ est appelée la *suite des degrés de rupture* de f et la suite $S(f) = G_1, \ldots, G_s$ est appelée la *suite des groupes de rupture* de f.

Proposition 3.2.3. *Soit K' une extension algébrique de K. Considérons $g \in K'[x]$ un polynôme séparable de degré d. Notons $\mathrm{Gal}'_K(g)$ le groupe de Galois de g sur K' et O une orbite de $\{1, \ldots, d\}$ sous l'action de $\mathrm{Gal}'_K(g)$. L'application*

$$\varphi :\ \mathrm{Gal}'_K(g) \ \longrightarrow\ S_O,$$

induite par l'action de $\mathrm{Gal}'_K(g)$ sur O, a pour image le groupe de Galois du facteur irréductible g_1 de g sur K' donné par :

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

où les β_i sont des racines de g dans $\overline{K}$.
En particulier, nous avons l'égalité $\mathrm{Card}(O) = deg(g_1)$.

Proposition 3.2.4. *Nous avons :*

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

et, par conséquent, $D(f) = D(G_f)$. Autrement dit, les groupes de Galois sur K' des facteurs de rupture de f sont les groupes de la suite $S(G_f)$ et ne dépendent que du groupe de Galois de f sur K.

Démonstration. Soit M une extension 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. g) dans une clôture algébrique de K contenant M. Comme g est irréductible sur M, la théorie de Galois classique assure que l'ensemble $\mathcal{O}_g$ est l'orbite de toute racine de g sous l'action du groupe $Aut_M(M(\mathcal{O}_f))$. Puisque tout automorphisme de $Aut_M(M(\mathcal{O}_g))$ peut être prolongé en un automorphisme de $Aut_M(M(\mathcal{O}_f))$, la restriction de l'homomorphisme

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

est surjective. Par conséquent, l'action de $Aut_M(M(\mathcal{O}_f))$ sur $\mathcal{O}_g$ s'identifie à celle de $Aut_M(M(\mathcal{O}_g))$ sur $\mathcal{O}_g$ et donc à la représentation symétrique G_g de son groupe de Galois.

Dans le cas de $M = K' = K(\alpha_1)$, ce résultat prouve que G_g est l'un des groupes de $S(G)$. Par conséquent, un groupe de $S(G)$ correspond à une unique $\mathrm{Fix}_G(1)$-orbite de $\{1, \ldots, n\}$ qui correspond à un sous-ensemble $\mathcal{O}$ de $\mathcal{O}_f$. La théorie de Galois assure que $\mathcal{O}$ est l'ensemble de tous les conjugués de l'un de ses éléments. Le polynôme minimal sur K' de l'un des éléments de $\mathcal{O}$ est un facteur de f sur K'. L'égalité $S(f) = S(G_f)$ en découle. □

3.2.2 Factorisation sur un corps de rupture et calcul de résolvante

Dans ce paragraphe, le corps K est supposé infini.

Soit $H = S_{\{1\}} \times S_{\{2\}} \times S_{\{3,\ldots,n\}}$ et $t \in K \setminus \{1\}$. Considérons le H-invariant S_n-relatif $X_1 + t\,X_2$ et notons $[S_n|H]_d$ l'ensemble des classes à droite de S_n modulo H.

Le corps K étant infini, la résolvante absolue $\mathcal{L}_{X_1+t\,X_2,\,f}$ de f sur $K(\alpha_1)$ est séparable pour un élément $t \in K \setminus \{1\}$. Nous avons alors

$$\begin{aligned} \mathcal{L}_{X_1+t\,X_2,\,f}(X) &= \prod_{\sigma\in[S_n|H]_d} (X - \sigma.(\alpha_1 + t\,\alpha_2)) \\ &= \prod_{i=1}^{n} \prod_{j\neq i} (X - (\alpha_j + t\,\alpha_i)) \\ &= \prod_{i=1}^{n} \frac{\prod_{j=1}^{n} (X - (\alpha_j + t\,\alpha_i))}{X - (\alpha_i + t\,\alpha_i)} \\ &= \prod_{i=1}^{n} \frac{f(X - t\,\alpha_i)}{(X - t\,\alpha_i) - \alpha_i}\,. \end{aligned}$$

La résolvante absolue $\mathcal{L}_{X_1+t\,X_2,\,f}$ est donc la norme du polynôme

$$\frac{f(X - t\,\alpha_1)}{(X - t\,\alpha_1) - \alpha_1}\,.$$

L'algorithme `Split_field` de B. Trager (voir [60]) factorise cette norme pour déterminer les s facteurs irréductibles $g_2, \ldots, g_s$ de f dans $K(\alpha_1)[X]$ (déplaçant ainsi dans $K[X]$ le problème de la factorisation dans $K(\alpha_1)[X]$). Calculer la résolvante absolue $\mathcal{L}_{X_1+t\,X_2,\,f}$ revient donc à factoriser f sur $K(\alpha_1)[X]$ par l'algorithme `Split_field` de B. Trager.

Plus précisement, en notant $N_1, N_2, \ldots, N_r$ les facteurs irréductibles de $\mathcal{L}_{X_1+t\,X_2}(X)$ dans $K(\alpha_1)[X]$, le théorème 2.2 de [60] montre que nous avons :

. $r = s - 1$;
. pour tout $i \in [\![2, n]\!]$, $g_i(X - t\,\alpha_1) = \mathrm{PGCD}(N_{i-1}, f(X - t\,\alpha_1))$ sur $K(\alpha_1)[X]$;
. $n \deg(g_i) = \deg(N_i)$.

Cette dernière égalité lie les degrés des facteurs de rupture de f et ceux des facteurs irréductibles de la résolvante linéaire $\mathcal{L}_{X_1+t\,X_2,\,f}$.

L. Soicher et J. Mckay, dans [55], sont les premiers à utiliser les degrés des résolvantes linéaires pour déterminer une représentation symétrique du groupe de Galois de f. Nous complèterons l'étude des degrés des facteurs de rupture de f en précisant les groupes de Galois de ces facteurs. De plus, nous utiliserons les facteurs de rupture pour construire un idéal des relations de f (voir Paragraphe 3.3.3 et Chapitre 5).

3.2.3 Degrés initiaux d'un idéal des relations

Définition 3.2.5. Soit I un idéal de Galois de f engendré par un ensemble triangulaire de polynômes

$$\{f_1(x_1) = f(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}\ .$$

La *liste des degrés initiaux de* I est définie par :

$$\mathcal{L}(I) = [\deg_{x_1}(f_1), \deg_{x_2}(f_2), \ldots, \deg_{x_n}(f_n)].$$

Remarque 3.2.6. La liste des degrés initiaux $\mathcal{L}(I)$ dépend de I mais pas de l'ensemble triangulaire $\{f_1,\ f_2,\ \ldots,\ f_n\}$ l'engendrant (voir Théorème 2.4.17).

Soit $\underline{\alpha}$ un n-uplet des racines de f. D'après le théorème 2.4.17 appliqué à l'idéal des relations $M_{\underline{\alpha}}$ (voir Définition 2.3.1), nous avons :

Proposition 3.2.7. *(Voir [7] ou Théorème 2.4.17) L'idéal $M_{\underline{\alpha}}$ est engendré par un ensemble triangulaire de polynômes et la liste $\mathcal{L}(M_{\underline{\alpha}})$ est égale à la liste $\mathcal{L}(G_{\underline{\alpha}})$ (voir Définition 2.3.6).*

3.3 Applications

Dans ce paragraphe, sont présentés des applications des tables de rupture.

3.3.1 Détermination du groupe de Galois

D'après la proposition 3.2.4, le groupe de Galois est l'un des groupes H de l'ensemble $\mathcal{T}(n)$ satisfaisant $S(H) = S(f)$. Nous appellerons *groupes candidats* tout groupe vérifiant $D(H) = D(f)$.

La liste $D(f)$ est connue à partir de la factorisation de f sur K'. S'il n'y a qu'un groupe candidat H, ou si les groupes candidats H satisfont $S(f) = S(H)$, nous savons alors que $H = G_f$. Pour connaître les groupes candidats H vérifiant $S(f) = S(H)$, il n'est pas nécessaire de déterminer la totalité de la suite $S(f)$. La détermination de certains groupes de Galois des facteurs de rupture de f peut être suffisante (voir Exemple 3.3.2). D'autres méthodes effectives peuvent être appliquées afin de compléter cette recherche. Par exemple, nous pouvons factoriser f modulo un nombre premier ne divisant pas son discriminant (voir [16] et [42]), exploiter la parité du groupe de Galois de f ou effectuer des calculs de résolvantes linéaires (voir [55]).

Les exemples suivants se réfèrent aux tables de rupture.

Exemple 3.3.1. Lorsque le groupe de Galois G_f est l'un des groupes $6T_5$, $7T_4$, $10T_6$, $13T_5^+$, $14T_8$, $14T_{16}$, $15T_2$, $15T_6^+$, $15T_7$, le calcul de $D(f)$ est suffisant pour sa détermination.

Exemple 3.3.2. Si un polynôme irréductible f de degré 15 vérifie $D(f) = 1, 2, 4, 8$ alors, d'après la table de rupture en degré 15, nous savons que son groupe de Galois est l'un des groupes $15T_{10}^+$, $15T_{11}$, $15T_{22}^+$, $15T_{23}$ ou $15T_{29}$. La détermination du groupe de Galois sur $K(\alpha_1)$ de son facteur de rupture de degré 4 est suffisante pour connaître le groupe de Galois de f.

Exemple 3.3.3. Si un polynôme irréductible f de degré 15 vérifie $D(f) = 1, 4, 5^2$, et si le discriminant de son facteur de rupture est un carré de $K(\alpha_1)$, alors le groupe de Galois de f est $15T_{92}^+$.

Exemple 3.3.4. Si un polynôme irréductible de degré 9 vérifie $D(f) = 1, 2, 3^2$, la liste des groupes candidats est $9T_{13}$, $9T_{22}$, $9T_{25}^+$ and $9T_{28}$.

Exemple 3.3.5. Si un polynôme irréductible de degré 16 et si $D(f) = 1^8, 8$, il y a trois groupes candidats. Si, de plus, le discriminant de f prouve que son groupe de Galois est pair alors la table de rupture en degré 16 montre qu'alors $G_f = 16T_{289}$.

Exemple 3.3.6. Si f, de degré 15, est tel que $D(f) = 1, 2, 3^4$ alors le groupe de Galois f est l'un des groupes suivants : $15T_{33}$, $15T_{44}$, $15T_{71}^+$ ou $15T_{81}$. Déterminer $S(f)$ ne suffit pas pour le distinguer. Si f est pair, il reste trois groupes. Les tables de rupture ne sont, dans ce cas, pas suffisantes pour déterminer le groupe de Galois.

Exemple 3.3.7. Supposons que f se scinde en n facteurs linéaires sur K' (i.e. $D(f) = 1^n$). Si, comme dans le cas du degré 4, plusieurs groupes sont candidats, il est malgré tout possible de les distinguer. En fait, pour $\underline{\alpha}$ tel que $g_i(\alpha_1, \alpha_i) = 0$, l'idéal $M_{\underline{\alpha}}$ des α-relations est engendré par l'ensemble triangulaire :

$$f(x_1),\ g_2(x_1, x_2),\ \ldots,\ g_n(x_1, x_n)$$

et le groupe de Galois de $G_{\underline{\alpha}}$ sur K est le groupe de décomposition de cet idéal (le calcul de ce groupe est l'objet du chapitre 4).

3.3.2 Factorisation de polynômes sur un corps de rupture

Les tables de rupture de degré n donnent l'ensemble $\mathcal{D}(n)$ des listes des degrés de rupture possibles d'un polynôme irréductible f de degré n. Ainsi, pour factoriser f sur l'un de ses corps de rupture, il est possible de restreindre la recherche des facteurs possibles à celle dont la liste des degrés de rupture appartient à $\mathcal{D}(n)$. Par ce biais, les algorithmes classiques de factorisation peuvent éviter des calculs inutiles (e.g. voir [41]).

Exemple 3.3.8. Le nombre d'éléments de l'ensemble $\mathcal{D}(7)$ est a priori majoré par le nombre de partitions de 6, c'est à dire 11. La table en degré 7 donne la valeur exacte : $|\mathcal{D}(7)| = 4$. Par ce biais, un grand nombre de combinaisons des facteurs possibles dans des algorithmes de factorisation peuvent être évitées. Si des informations sur le groupe de Galois sont disponibles, la liste des degrés de rupture peut être restreinte à un sous-ensemble de $\mathcal{D}(n)$.

3.3.3 Détermination du corps de décomposition d'un polynôme

La détermination d'un corps de décomposition de f équivaut à celle d'un idéal des relations $M_{\underline{\alpha}}$ de f, où $\underline{\alpha}$ est un n-uplet de racines de f.

Une méthode classique consiste à factoriser successivement f sur des corps de rupture (voir [34], [59] ou [3]). Cette méthode peut être améliorée en utilisant les tables de rupture en guidant la factorisation à l'aide des informations sur le groupe de Galois de f.

Une autre méthode pour déterminer $M_{\underline{\alpha}}$ consiste en la construction d'une chaîne croissante d'idéaux de premier terme l'idéal des relations symétriques des racines de f et de dernier terme un idéal des relations $M_{\underline{\alpha}}$.

Soit I un idéal de Galois de f contenu dans $M_{\underline{\alpha}}$ et engendré par un système triangulaire

$$S_I = \{f_1(x_1) = f(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}\ .$$

Posons $m_i = \deg_{x_i}(f_i)$, pour tout $i \in [\![1, n]\!]$. Supposons les polynômes S_I connus ; nous souhaitons connaître ceux d'un ensemble triangulaire de générateurs $S_{M_{\underline{\alpha}}}$ de $M_{\underline{\alpha}}$.

La liste $\mathcal{L}(M_{\underline{\alpha}}) = [d_1, d_2, \ldots, d_n]$ est égale à $\mathcal{L}(G_{\underline{\alpha}})$ (voir Proposition 3.2.7). Supposons que la liste $\mathcal{L}(G_{\underline{\alpha}})$ est connue grâce à des informations sur le groupe de Galois de f. Ceci

est par exemple le cas lorsque le groupe de Galois $G_{\underline{\alpha}}$ appartient à l'une des listes connues de groupe H ayant des listes $\mathcal{L}(H)$ identiques. Montrons maintenant comment simplifier la recherche de $\mathcal{S}_{M_{\underline{\alpha}}}$.

Nous avons,

$$d_i \leq m_i,\ i = 1, 2, \ldots, n.$$

La comparaison des listes $\mathcal{L}(I)$ et $\mathcal{L}(G_{\underline{\alpha}})$ induit le résultat suivant :

1- $d_i = m_i$ si et seulement s'il est possible de choisir, pour i-ème polynôme de l'ensemble $\mathcal{S}_{M_{\underline{\alpha}}}$, le i-ème polynôme de l'ensemble $\mathcal{S}_I$;

2- si $d_i < m_i$, alors le i-ème polynôme de l'ensemble $\mathcal{S}_{M_{\underline{\alpha}}}$ est un facteur du i-ème polynôme de la liste $\mathcal{S}_I$ considéré comme polynôme de l'anneau $K(\alpha_1, \ldots, \alpha_{i-1})$.

Les méthodes citées ci-dessus (factorisations sur des corps de rupture, algorithme `GaloisIdeal`), utilisées conjointement avec cette information supplémentaire, peuvent être appliquées pour déterminer un polynôme manquant de $\mathcal{S}_{M_{\underline{\alpha}}}$.

Remarque 3.3.9. Un ensemble de générateurs d'un idéal I contenu dans l'idéal $M_{\underline{\alpha}}$ peut être obtenu à partir de la suite $f_1(x_1), g_2(x_1, x), \ldots, g_s(x_1, x)$ dans laquelle le polynôme $g_1(x_1, x) = x - x_1$ est absent. La procédure consiste à remplacer inductivement chaque polynôme g_i de la suite à l'aide ses modules de Cauchy, en s'assurant que les variables introduites ne figurent pas déjà dans les polynômes de la nouvelle suite en construction. L'idéal ainsi obtenu est appelé l'*idéal de rupture du polynôme* f (voir Chapitre 5).

Remarque 3.3.10. La méthode de McKay et Stauduhar (voir [43]) peut être appliquée pour trouver des relations linéaires de l'idéal $M_{\underline{\alpha}}$.

Exemple 3.3.11. Considérons l'exemple 3.3.1. La liste des degrés de l'ensemble de générateurs de l'idéal de rupture de f est $[16, 8, 7, 6, 5, 4, 3, 2, 1^8]$. Les tables de rupture en degré 16 montrent que $\mathcal{L}_M = [16, 8, 1^{14}]$ (dans ce cas particulier, les degrés initiaux de l'idéal des relations de f sont égaux ; i.e. la liste $\mathcal{L}$ est indépendante du représentant de la classe de S_n-conjugaison de tout groupe candidat). Si nous comparons ces deux listes, nous saurons qu'un idéal des relations s'obtient en substituant, dans l'idéal de rupture de f, les modules de Cauchy du facteur g_8 de degré 8 (à l'exception du polynôme g_8 lui-même) par des relations linéaires de la forme $x_i + g_i(x_1, x_8)$, pour $i \in [\![10, 16]\!]$.

Remarque 3.3.12. Pour pouvoir utiliser récursivement des tables de rupture en factorisant f dans des extensions de corps, il est nécessaire d'établir des tables de rupture pour les sous-groupes non transitifs de S_n. En fait, le groupe de Galois d'un polynôme réductible sans racine multiple est un sous-groupe du produit direct des groupes de Galois de ces facteurs (voir Chapitre 7).

3.3.4 Calculer des polynômes de groupe de Galois donné dans des extensions algébriques

Soit H un sous-groupe transitif de S_r. Les tables de rupture permettent de rechercher des polynômes à coefficients dans une extension algébrique de groupe de Galois H.

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

Supposons, de plus, que nous connaissons un polynôme $f \in K[x]$ de groupe de Galois sur K isomorphe à G. Pour $n \leq 15$, nous disposons des polynômes de la base de données GALPOLS de MAGMA (voir [11]).

Soit α l'une des racines de f. Nous savons que le groupe de Galois sur $K' = K(\alpha)$ de l'un des facteurs de rupture de f est isomorphe à H.

Remarque 3.3.13. Si l'un des sous-groupes de S_r de la suite $S(G)$ est différent de H, il faut alors déterminer lequel des facteurs de rupture de f admet H pour groupe de Galois. Dans ce cas, une méthode adaptée pour le calcul du groupe de Galois est le calcul algébrique de résolvantes (voir, par exemple, [10], [25], [26], [55] ou [5]). Il est clairement préférable, si possible, de choisir un polynôme f afin d'éviter cette situation.

Exemple 3.3.14. Un polynôme de groupe de Galois $10T_{39}$ sur une extension monogène de K peut être obtenu à partir d'un polynôme de groupe de Galois $12T_{293}$. Sur l'un de ses corps de rupture K', tout polynôme de groupe de Galois $12T_{293}$ se factorise en deux facteurs linéaires et un facteur de degré 10 dont le groupe de Galois sur K' est $10T_{39}$.

Le polynôme suivant est celui de groupe de Galois $12T_{293}$ sur $\mathbb{Q}$ de la base de données GALPOLS de MAGMA :

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

La factorisation de f sur $K' = \mathbb{Q}(\alpha)$ retourne deux facteurs linéaires et un facteur de rupture de degré 10 :

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

D'après la table de rupture en degré 16, le groupe de Galois de h sur $\mathbb{Q}(\alpha)$ est donc $10T_{39}$.

Chapitre 4

Groupe de décomposition d'un idéal triangulaire

Dans ce chapitre, nous présentons deux algorithmes de calcul du groupe de décomposition d'un idéal triangulaire. Ces algorithmes reposent sur des algorithmes classiques de théorie des groupes (voir [54], [15] ou [53]).

La première partie de ce chapitre est extrait d'un article réalisé en collaboration avec Inès Abdeljaouad, Guénaël Renault et Annick Valibouze (voir [1]). Nous y présentons un premier algorithme, i.e. l'algorithme 4.2.12, de calcul du groupe de décomposition d'un idéal triangulaire quelconque.

Dans [3], Anai, Noro et Yokoyama transposent aux idéaux de relations le théorème de prolongement des automorphismes de corps. Le théorème 4.2.21 de ce chapitre généralise ce résultat à tout idéal de Galois et fournit une interprétation du parcours d'arbre effectué par l'algorithme 4.2.12.

Ce premier algorithme améliore l'algorithme `StrongGenerators` de [3] :

- de par son champ d'application (`StrongGenerators` ne s'applique qu'aux idéaux de relations) ;
- de par sa complexité ($O(n^3)$ formes normales sont nécessaires pour calculer le groupe de décomposition d'un idéal de Galois pur alors que `StrongGenerators` effectue $O(n^4)$ formes normales dans le cas d'un idéal des relations.

La seconde partie de ce chapitre est constituée de résultats personnels. Un second algorithme, nommé `EFG` de calcul du groupe de décomposition d'un idéal triangulaire y est présenté. L'algorithme `EFG` améliore le premier de par sa complexité :

- appliqué aux idéaux de Galois purs, $O(n^2)$ formes normales sont nécessaires pour ce calcul ;
- appliqué aux idéaux de Galois quelconques, $O(n^2 \frac{(Dim(I))^2}{\text{Card}(S)\ \text{Card}(\text{Dec}(I))})$, où S désigne un sous groupe de S_n et $Dim(I)$ la dimension de I, formes normales sont nécessaires

pour ce calcul (alors que ce nombre peut être égal à $(n-2)!$ avec le premier algorithme).

4.1 Nature du problème

4.1.1 Notations

Dans toute la suite, les notations suivantes seront utilisées :
- pour toute partie $\mathcal{A}$ de l'ensemble $\{1,\ldots,n\}$ et tout sous-groupe G de S_n, nous noterons $Fix_G(\mathcal{A})$ le fixateur dans G de $\mathcal{A}$, c'est à dire le sous-groupe constitué des permutations σ de G vérifiant $\forall i \in \mathcal{A},\ \sigma(i) = i$;
- $\langle \mathcal{E} \rangle$ désignera le sous-groupe engendré par toute partie non vide $\mathcal{E}$ de S_n ;
- $K[X_1,\ldots,X_n]$ désigne l'anneau des polynômes à coefficients dans un corps parfait K en les n indéterminées $X_1,\ldots,X_n$;
- I est un idéal de $K[X_1,\ldots,X_n]$ engendré par un ensemble triangulaire S de n polynômes de $K[X_1,\ldots,X_n]$:

$$S = \{f_1(X_1), f_2(X_1,X_2),\ldots,f_n(X_1,X_2,\ldots,X_n)\}\,.$$

Conformément à la définition donnée au chapitre 2, le *groupe de décomposition de l'idéal* I, noté $Dec(I)$, est le stabilisateur de l'idéal I pour l'action naturelle du groupe symétrique S_n sur l'anneau $K[X_1,\ldots,X_n]$:

$$Dec(I) = \{\sigma \in S_n \mid \forall P \in I, \sigma.P \in I\}.$$

4.1.2 Nature et contraintes des algorithmes

Les deux algorithmes présentés ci-après calculent le groupe de décomposition de l'idéal triangulaire I. Cet idéal étant engendré par les polynômes $\{f_1, f_2, \ldots, f_n\}$, le groupe de décomposition de I s'écrit :

$$Dec(I) = \{\sigma \in S_n \mid \forall i \in \{1,\ldots,n\},\ \sigma.f_i \in I\}.$$

Ainsi, nous avons l'équivalence :

$$\sigma \in Dec(I) \text{ ssi } \begin{cases} f_1(X_{\sigma(1)}) \in I \\ f_2(X_{\sigma(1)}, X_{\sigma(2)}) \in I \\ \quad\vdots \\ f_n(X_{\sigma(1)},\ldots,X_{\sigma(n)}) \in I\,. \end{cases} \qquad \{*\}$$

Pour tout $r \in [\![1,n]\!]$, définissons le prédicat logique P_r en posant :

$$P_r(a_1,\ldots,a_r) \text{ est vrai ssi } f_r(X_{a_1}, X_{a_2},\ldots,X_{a_r}) \in I$$

et notons $\mathcal{P}$ l'ensemble de ces n conditions :

$$\mathcal{P} = \{P_1,\ldots,P_n\}\,.$$

Une permutation $\sigma \in S_n$ appartient donc au groupe $\mathrm{Dec}(I)$ ssi la conjonction logique

$$p_1(\sigma(1)) \wedge p_2(\sigma(1), \sigma(2)) \wedge \cdots \wedge p_n(\sigma(1), \ldots, \sigma(n))$$

est vérifiée. Le groupe $\mathrm{Dec}(I)$ est alors défini comme l'ensemble des permutations de S_n vérifiant l'ensemble des conditions $\mathcal{P}$.

Les algorithmes de "backtrack search" utilisés en théorie algorithmique des groupes (voir [54], [15] ou [53]) permettent de déterminer un groupe D défini comme l'ensemble des permutations de S_n vérifiant un ensemble de propriétés $\mathcal{P}$. Une n-liste $(a_1, \ldots, a_n)$ d'entiers de $[\![1, n]\!]$ étant donnée, ce type d'algorithme calcule un ensemble de générateurs de chaque groupe de la suite croissante de fixateurs de D :

$$\{Id_{S_n}\} = Fix_D(\{a_1, \ldots, a_n\}) \subseteq Fix_D(\{a_1, \ldots, a_{n-1}\}) \subseteq \cdots \subseteq Fix_D(\{a_1\}) \subseteq D,$$

chaque ensemble de générateurs de l'un des fixateurs servant au calcul de l'ensemble de générateurs suivant.

L'ensemble de générateurs du groupe D obtenu est un ensemble fort de générateurs de D : il s'agit d'un ensemble E de générateurs de D tel que, pour tout $i \in [\![1, n]\!]$, $Fix_D(\{a_1, \ldots, a_i\}) \cap E$ engendre $Fix_D(\{a_1, \ldots, a_i\})$.

Les algorithmes 4.2.12 et `EFG` du paragraphe 4.3.2 ci-après sont des algorithmes utilisant des techniques de "backtrack search". Les coûts des calculs groupistiques étant négligeables par rapport au coût des formes normales modulo S, il est naturel de chercher à diminuer le nombre de formes normales, i.e. de calcul de prédicats $P_1, \ldots, P_n$, nécessaires au calcul de $\mathrm{Dec}(I)$ à l'aide de ce type d'algorithme.

4.2 Algorithme `Generateurs` - Application aux idéaux de Galois purs

L'algorithme du paragraphe 4.2.1 retourne toutes les permutations d'un groupe D défini comme ensemble des permutations de S_n vérifiant tous les prédicats de l'ensemble $\mathcal{P} = \{P_1, \ldots, P_n\}$. Cet algorithme est qualifié de "naïf" car il n'exploite pas la structure de groupe de D et retourne toutes les permutations de D. Modifié pour ne retourner qu'une seule permutation, il sera appelé par l'algorithme 4.2.12 (nous verrons alors que, sous la condition $\mathcal{H}$ du paragraphe 4.2.4, une permutation de D est retournée en au plus n^2 calculs de prédicats).

4.2.1 Algorithme naïf

Cet algorithme, nommé `ToutesLesPermutations`, repose sur l'équivalence $\{*\}$ et peut être décrit comme suit :

- À la première étape, cet algorithme détermine les valeurs possibles $a_1 \in \{1, \ldots, n\}$ telles que $P_1(a_1)$ soit vrai. La seconde étape est alors appliquée à chacune de ces valeurs.
- À la $r^{\text{ème}}$ étape ($2 \leq r \leq n$), l'algorithme a déterminé $r-1$ valeurs distinctes $a_1, \ldots, a_{r-1}$ telles que $\forall i \in \{1, \ldots, r-1\}, P_i(a_1, \ldots, a_i)$.
  Les entiers $a_r \in \{1, \ldots, n\} \backslash \{a_1, \ldots, a_{r-1}\}$ pour lesquels les prédicats $P_r(a_1, \ldots, a_r)$ sont vrais sont alors recherchés. Pour chacun de ces entiers a_r, l'algorithme passe à l'étape suivante.
- Lorsque $r = n+1$, l'algorithme a déterminé une permutation $\sigma = \left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$ du groupe D.

Algorithme 4.2.1.

Fonction `ToutesLesPermutations` $(\mathcal{P})$
/*
Entrée : L'ensemble des prédicats $\mathcal{P} = \{P_1, \ldots, P_n\}$.

Sortie : Le groupe D.
*/
Retourner `ConstructionDesPermutations` $(1, [\,], \{Id\}, \mathcal{P})$;
Fin Fonction

Fonction `ConstructionDesPermutations` $(r, [a_1, \ldots, a_{r-1}], \mathcal{G}, \mathcal{P})$
/*
Entrées : . Un entier r de $\{1, \ldots, n+1\}$.
. Une liste $[a_1, \ldots, a_{r-1}]$ d'entiers de $\{1, \ldots, n\}$, distincts deux à deux, pour laquelle est recherché des suffixes $[a_r, \ldots, a_n]$ tels que $\left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right) \in D$.
. L'ensemble $\mathcal{G}$ des permutations de D déterminées aux étapes précédentes.
. L'ensemble des prédicats $\mathcal{P} = \{P_1, \ldots, P_n\}$.

Sortie : . L'ensemble $\mathcal{G}$ auquel a été éventuellement rajouté une permutation de D.
*/
Si $r = n+1$ **Alors**
. /* $\left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$ appartient à D */
. $\mathcal{G} := \mathcal{G} \cup \{\left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)\}$;
Sinon
. **Pour Tout** $a \in \{1, \ldots, n\} \backslash \{a_1, \ldots, a_{r-1}\}$ **Faire**
. . /* Les images possibles a de r sont recherchées */
. . **Si** $P_r(a_1, \cdots, a_{r-1})$ **Alors**
. . $\mathcal{G} :=$ `ConstructionDesPermutations` $(r+1, [a_1, \ldots, a_{r-1}, a], \mathcal{G}, \mathcal{P})$;
. . **Fin Si** ;
. **Fin Pour** ;
Fin Si ;
Retourner $\mathcal{G}$;
Fin Fonction

A la $k^{\text{ème}}$ étape ($k \in [\![1, n]\!]$), la fonction `ConstructionDesPermutations` ne réalise qu'au plus $n + 1 - k$ appels récursifs ce qui assure la terminaison de l'algorithme. Pour qu'une permutation σ soit stockée dans $\mathcal{G}$, il faut qu'elle vérifie les n conditions $P_1, \ldots, P_n$; ainsi l'ensemble retourné par la fonction `ToutesLesPermutations` est bien le groupe D.

Parcours d'arbre effectué

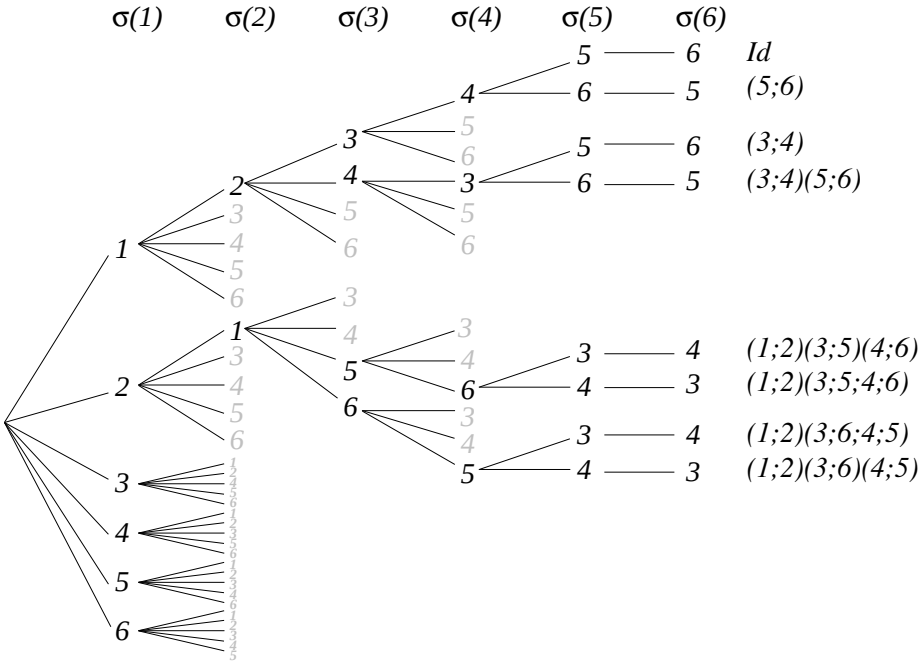
Exemple 4.2.2. Considérons l'idéal de Galois I (voir Définition 6.1.1) de $\mathbb{Q}[x_1, \ldots, x_6]$ engendré par les polynômes :

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

Rappelons qu'ici le groupe D est le groupe de décomposition de I, $\mathrm{Dec}(I)$, et que l'ensemble des prédicats $\mathcal{P} = \{P_1, \ldots, P_n\}$ est défini, au paragraphe 4.1.2, par :

$$\forall r \in [\![1, n]\!],\ (P_r(a_1, \ldots, a_r) \text{ est vrai}) \text{ ssi } (f_r(X_{a_1}, X_{a_2}, \ldots, X_{a_r}) \in I)\ .$$

L'algorithme 4.2.1 parcourt l'arbre suivant, dans lequel à chaque entier correspond un test d'appartenance à l'idéal :



Remarquons qu'en cours de calcul l'algorithme détermine la suite ascendante des fixateurs :

$$Fix_{Dec(I)}(\{1,\dots,n\}) < \cdots < Fix_{Dec(I)}(\{1,2\}) < Fix_{Dec(I)}(\{1\}),$$

qui sera exploitée lors de la conception des algorithmes `Generateurs` et `EFG` des paragraphes 4.3.2 et 4.2.12.

Dans cet exemple, un certain nombre de calculs sont inutiles. En effet, la permutation $(3;4)(5;6)$ appartient au groupe $\langle(3;4),(5;6)\rangle$ et les permutations $(1;2)(3;5;4;6)$, $(1;2)(3;6;4;5)$, $(1;2)(3;6)(4;5)$ appartiennent au groupe $\langle(3;4),(5;6),(1;2)(3;5)(4;6)\rangle$. La recherche d'un algorithme ne retournant qu'un système de générateurs de $Dec(I)$, qui apparaît ici comme naturelle, fera l'objet du paragraphe suivant.

4.2.2 Système fort de générateurs

Dans le cas où $D = S_n$, l'algorithme 4.2.1 présente l'inconvénient d'effectuer $n!$ calculs de prédicats et de stocker les $n!$ permutations de son groupe de décomposition.

Dans cette partie, nous allons reprendre cet algorithme en nous limitant à la détermination d'un système de générateurs du groupe D. Ceci aura pour conséquence, dans le cas où $D = S_n$, de n'avoir à effectuer que $n(n+1)/2-1$ tests d'appartenance à l'idéal pour déterminer un système de générateurs composé de $n-1$ transpositions.

Dans toute la suite, k désigne un entier quelconque de $\{1, \ldots, n\}$.

Notons G_k le groupe $Fix_D(\{1, \ldots, k\})$ et posons $G_0 = D$. Pour tout sous-groupe G de S_n, notons $Orb_G(k)$ la G-orbite de k.

L'algorithme 4.2.1 détermine, en cours de calcul, tous les termes de la suite croissante pour l'inclusion :

$$\{Id\} = G_n < G_{n-1} < \cdots < G_2 < G_1 < G_0 = D.$$

Pour ce faire, cet algorithme construit le groupe G_{k-1}, pour tout $k \in [\![1, n]\!]$, en ajoutant au groupe G_k les éléments de $G_{k-1} \backslash G_k$. Afin d'éviter d'avoir à calculer toutes les permutations de $G_{k-1} \backslash G_k$, les propositions du paragraphe suivant nous permettrons de construire un système de générateurs du groupe G_{k-1} à partir de tout ensemble de générateurs du groupe G_k. Nous obtiendrons ainsi un système fort de générateurs de D.

Construction d'un système de générateurs

A partir d'un ensemble de générateurs d'un sous-groupe H de G_{k-1} contenant G_k et d'une permutation de G_{k-1} déterminée par l'algorithme 4.2.1, l'idée est de construire un ensemble de générateurs d'un groupe H' contenant strictement H en utilisant la proposition 4.2.3. En réitérant ce processus, nous déterminerons alors, par l'algorithme 4.2.11, une chaîne croissante de groupes de premier terme G_k et de dernier terme G_{k-1}. Ces groupes seront représentés par des systèmes de générateurs.

Proposition 4.2.3. *Soit H un sous-groupe de S_n tel que $G_k \subseteq H \subseteq G_{k-1}$. Soient $\mathcal{G}$ un système de générateurs de H et O une H-orbite de $\{1, \ldots, n\}$ incluse dans $\{k+1, \ldots, n\}$.*

Supposons l'ensemble $\mathcal{E} = \{\sigma \in G_{k-1} \mid \sigma(k) \in O\}$ non vide et notons $H' = \langle H \cup \mathcal{E} \rangle$.

Alors le groupe H' contient strictement H et il est engendré par $\mathcal{G} \cup \{\sigma\}$ quelque soit σ choisit dans $\mathcal{E}$.

Démonstration. Soit $\sigma \in \mathcal{E}$. Puisque $\mathcal{G} \cup \{\sigma\}$ engendre $\langle H \cup \{\sigma\} \rangle$ et que $\langle H \cup \mathcal{E} \rangle$ engendre H', il suffit de montrer que tout élément de l'ensemble $H \cup \mathcal{E}$ appartient au groupe $\langle H \cup \{\sigma\} \rangle$. Soit $\sigma' \in H \cup \mathcal{E}$.

Si $\sigma' \in H$, le résultat est immédiat.

Si $\sigma' \in \mathcal{E}$ alors les entiers $\sigma'(k)$ et $\sigma(k)$ appartiennent à l'orbite O. Donc il existe $\tau \in H$ tel que $\tau(\sigma(k)) = \sigma'(k)$ et nous avons alors $\sigma^{-1}(\tau^{-1}(\sigma'(k))) = k$. Puisque les permutations σ, τ et σ' appartiennent à

$$G_{k-1} = Fix_D(\{1, \ldots, k-1\}),$$

l'égalité précédente montre que $\rho = \sigma^{-1}\tau^{-1}\sigma' \in G_k \subset H$. Nous avons alors $\sigma' = \tau\sigma\rho$, ce qui prouve que la permutation σ' s'écrit comme produit d'éléments de H et de la permutation σ. □

Le résultat suivant permet de limiter la recherche des permutations de $\mathcal{E}$ en se limitant à celles qui transforment k en $a = Min(O)$. Ce sont ces permutations qui sont testées en premier par l'algorithme 4.2.1.

Proposition 4.2.4. *Reprenons les hypothèses et les notations de la proposition* 4.2.3 *et posons* $a = Min(O)$. *Si* $\mathcal{E}$ *est non vide alors il existe* $\sigma \in \mathcal{E}$ *tel que* $\sigma(k) = a$.

Démonstration. Si $\mathcal{E}$ n'est pas vide alors il existe $\sigma' \in G_{k-1}$ tel que $\sigma'(k) \in O$. Or $\sigma'(k)$ et a appartiennent à l'orbite O, donc il existe $\tau \in H$ tel que $\tau\sigma'(k) = a$. Puisque τ et σ' sont deux permutations de G_{k-1}, nous obtenons $\tau\sigma' \in \mathcal{E}$. □

Les propositions 4.2.6 et 4.2.7 permettent de tester l'égalité $H = G_{k-1}$ et constituent les conditions d'arrêt de l'algorithme 4.2.12.

Lemme 4.2.5. *Soit* H *un sous-groupe de* S_n *tel que* $G_k \subseteq H \subseteq G_{k-1}$. *Nous avons l'égalité :*

$$Card(H) = Card(G_k) \,.\, Card(Orb_H(k)) \,.$$

Démonstration. Posons $Orb_H(k) = \{a_1, \ldots, a_r\}$ et considérons, pour tout $i \in \{1, \ldots, r\}$, une permutation σ_i de H telle que $\sigma_i(k) = a_i$. Nous avons :

$$H = \sigma_1 G_{k-1} + \cdots + \sigma_r G_{k-1},$$

d'où le résultat. □

Proposition 4.2.6. *Soit* H *un sous-groupe de* S_n *tel que* $G_k \subseteq H \subseteq G_{k-1}$. *S'il n'existe pas de* H*-orbite de* $\{1, \ldots, n\}$ *incluse dans* $\{k+1, \ldots, n\}$ *alors* $H = G_{k-1}$.

Démonstration. La H-orbite contenant n est incluse dans $\{k, \ldots, n\}$ (puisque $H \subseteq G_{k-1} = Fix_D(\{1, \ldots, k-1\})$). Si cette orbite n'est pas incluse dans $\{k+1, \ldots, n\}$ alors elle s'identifie à $\{k, \ldots, n\}$ et est donc égale à $Orb_H(k)$.

L'inclusion $H \subseteq G_{k-1}$ impose alors $Orb_{G_{k-1}}(k) = \{k, \ldots, n\}$. D'après le lemme 4.2.5 appliqué à H et à G_{k-1}, il vient $Card(H) = Card(G_{k-1})$, d'où le résultat. □

Proposition 4.2.7. *Soit* H *un sous-groupe de* S_n *tel que* $G_k \subseteq H \subseteq G_{k-1}$. *Supposons non vide l'ensemble* $\mathcal{O}$ *des* H*-orbites de* $\{1, \ldots, n\}$ *incluses dans* $\{k+1, \ldots, n\}$ *et notons* $\mathcal{O} = \{O_1, \ldots, O_r\}$. *Pour tout* $i \in \{1, \ldots, r\}$, *posons* $\mathcal{E}_i = \{\sigma \in G_{k-1} \mid \sigma(k) \in O_i\}$.
Si, pour tout $i \in \{1, \ldots, r\}$, $\mathcal{E}_i = \emptyset$ *alors* $H = G_{k-1}$.

Démonstration. Raisonnons par l'absurde en supposant que $H \neq G_{k-1}$. Le lemme 4.2.5 montre que nous avons l'inégalité $Orb_H(k) \neq Orb_{G_{k-1}}(k)$. De plus, l'inclusion $H \subseteq G_{k-1}$ implique $Orb_H(k) \subset Orb_{G_{k-1}}(k)$. Ainsi, il existe $a \in Orb_{G_{k-1}}(k) \backslash Orb_H(k)$ (vérifiant donc $a \neq k$) et , par suite, une permutation $\sigma \in G_{k-1} \backslash H$ telle que $\sigma(k) = a$. Nous avons donc $a \in \{k+1, \ldots, n\}$ et, quelque soit $h \in H$, $h(a) \neq k$ (sinon $h^{-1}(k) = a \in Orb_{G_{k-1}}(k)$). Donc la H-orbite O de $\{1, \ldots, n\}$ contenant a est une orbite O_t appartenant à $\mathcal{O}$. Nous avons alors $\mathcal{E}_t \neq \emptyset$, ce qui est absurde. □

Remarque 4.2.8. Les propositions 4.2.6 et 4.2.7 suffisent pour tester l'égalité $H = G_{k-1}$.

Pour appliquer les propositions 4.2.3 et 4.2.4, nous avons besoin de déterminer les orbites de $\{1, \ldots, n\}$ sous l'action du sous-groupe $H' = \langle \{\sigma\} \cup H \rangle$. La proposition 4.2.9 permet de déterminer ces orbites en fonction de celles de H et de σ.

Proposition 4.2.9. *Soit $\mathcal{O}$ l'ensemble des orbites de $\{1, \ldots, n\}$ sous l'action d'un sous-groupe H de S_n et $O \in \mathcal{O}$. Soit σ une permutation de S_n et notons H' le sous-groupe engendré par $\{\sigma\} \cup H$.*

Notons $(E_r)_{r\in\mathbb{N}}$ et $(F_r)_{r\in\mathbb{N}}$ les suites définies par récurrence par :

– $E_1 = O$ et $F_1 = (\sigma.E_1) \cup E_1$;

– Pour tout $k \in \mathbb{N}^*$, $E_{k+1} = \cup_{\{O' \in \mathcal{O} \mid O' \cap F_k \neq \emptyset\}} O'$ et $F_{k+1} = (\sigma.E_{k+1}) \cup E_{k+1}$.

Alors, la suite $(E_k)_{k\in\mathbb{N}^*}$ est une suite stationnaire à partir d'un certain rang k_0 et l'ensemble E_{k_0} est l'orbite de $\{1, \ldots, n\}$ sous l'action de H' contenant O.

Démonstration. Soit $k \in \mathbb{N}^*$, nous avons $E_k \subseteq F_k$. Posons $\mathcal{O} = \{O_1, \ldots, O_s\}$. Puisque $O_1, \ldots, O_s$ est une partition de $\{1, \ldots, n\}$, $\{F_k \cap O_i\}_{i\in\{1,\ldots,s\}}$ est une partition de F_k. Par suite $F_k \subseteq \cup_{\{O' \in \mathcal{O} \mid O' \cap F_k \neq \emptyset\}} O' = E_{k+1}$ et il vient : $E_k \subset E_{k+1}$. La suite $(E_k)_{k\in\mathbb{N}^*}$, croissante pour l'inclusion et majorée par $\{1, \ldots, n\}$, est donc stationnaire à partir d'un certain rang k_0.

Notons $O'_1, \ldots, O'_{s'}$ les orbites de $\{1, \ldots, n\}$ sous l'action de H'.

Nous avons l'égalité $E_{k_0} = E_{k_0+1}$. Ceci impose les égalités $E_{k_0} = F_{k_0}$ et $E_{k_0} = \sigma.E_{k_0}$. Par ailleurs, E_{k_0} s'écrivant comme réunion d'orbites prises parmi $O_1, \ldots, O_s$, l'ensemble E_{k_0} est stable sous l'action de H. Ainsi, E_{k_0} est stable sous l'action de $H' = \langle \{\sigma\} \cup H \rangle$ ce qui montre que E_{k_0} s'écrit comme réunion d'orbites prises parmi $\{O'_1, \ldots, O'_{s'}\}$.

Une récurrence immédiate montre que, pour tout $k \in \{1, \ldots, k_0\}$, E_k (et donc, en particulier, E_{k_0}) est inclus dans la H'-orbite contenant O.

Par conséquent, E_{k_0} est la H'-orbite contenant O. □

4.2.3 Algorithme `Generateurs`

Dans ce paragraphe, est présenté l'algorithme 4.2.12, nommé `Generateurs`, de calcul du groupe de décomposition d'un idéal triangulaire ainsi que sa preuve de correction et de terminaison.

Fonction `NouvellesOrbites`

La fonction `NouvellesOrbites` ci-dessous est appelée par la fonction `De_Gk_a_G(k-1)`. A partir de l'ensemble (noté *orbites*) des orbites de $\{1, \ldots, n\}$ sous l'action d'un groupe H et d'une permutation σ appartenant à S_n, la fonction `NouvellesOrbites` détermine les orbites de $\{1, \ldots, n\}$ sous l'action du groupe $H' = \langle H \cup \{\sigma\} \rangle$.

Pour construire ces nouvelles orbites, l'algorithme part d'une H-orbite O et construit la H'-orbite E contenant O sous forme d'une réunion d'orbites associées à H, en générant

les suites $(E_k)_{k\in\mathbb{N}^*}$ et $(F_k)_{k\in\mathbb{N}^*}$ de la proposition 4.2.9 .

Algorithme 4.2.10.

Fonction `NouvellesOrbites` ($orbites$,σ)
/*
Entrées : . L'ensemble, noté *orbites*, formé par les orbites de $\{1,\ldots,n\}$ sous l'action d'un sous-groupe H de S_n.
. Une permutation σ appartenant à S_n. */

Sortie : . *nvorbites* qui est l'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action de $H' = \langle H \cup \{\sigma\}\rangle$.

$nvorbites := \emptyset$;
Pour $O \in orbites$ **Faire**
. $E := O$;
. $P := E \cup \sigma.E$;
. **Tant que** $E \neq P$ **Faire**
. . /* Construction du terme E_{k+1} de la suite $(E_k)_{k\in\mathbb{N}^*}$ */
. . **Pour** $O' \in orbites$ **Faire**
. . . **Si** $P \cap O' \neq \emptyset$ **Alors**
. . . . $E = E \cup \{O'\}$;
. . . . $orbites := orbites \setminus O'$;
. . . **Fin Si** ;
. . **Fin Pour** ;
. . /* Construction du terme F_{k+1} de la suite $(F_k)_{k\in\mathbb{N}^*}$ */
. . $P := E \cup \sigma.E$;
. **Fin Tant que** ;
. $nvorbites := nvorbites \cup \{E\}$;
Fin Pour ;
Retourner $nvorbites$;
Fin Fonction

Fonction `TrouverUnePermutation`

Considérons la fonction `TrouverUnePermutation` obtenue en modifiant la fonction `ConstructionDesPermutations` (Algorithme 4.2.1) pour qu'elle retourne

- une permutation du groupe D dès qu'elle est trouvée, si elle existe ;
- la permutation identité sinon.

Le paramètre formel $\mathcal{G}$ de la fonction `ConstructionDesPermutations`, qui est un ensemble de permutation, est remplacé par un paramètre ne représentant qu'une permutation dans la fonction `TrouverUnePermutation`.

Fonction `De_Gk_a_G(k-1)` - Preuve de correction et de terminaison

La fonction suivante `De_Gk_a_G(k-1)` construit inductivement à partir de G_k une suite croissante finie de groupes :

$$G_k = H_0 < H_1 < \cdots < H_m = G_{k-1}\,,$$

chaque groupe étant représenté par un ensemble de permutations l'engendrant.

Soit H l'un des groupes H_i, pour $i \in [\![0, m]\!]$ et $\mathcal{G}$ un ensemble de permutation l'engendrant. Cette fonction détermine, lorsqu'elle existe, une permutation $G_{k-1}\backslash H$ qui, adjointe à $\mathcal{G}$, formera un ensemble de générateurs d'un nouveau groupe $H_{i+1} = H'$. Ce procédé sera réitéré jusqu'à ce qu'aucune nouvelle permutation ne puisse être trouvée auquel cas nous aurons l'égalité $H = G_{k-1}$.

Explicitons la méthode de calcul du groupe H' à partir de H.

Soit $(O_1, \ldots, O_r)$ une H-orbite de $\{1, \ldots, n\}$. Nous avons alors deux cas :

Cas 1 : Aucune orbite est incluse dans $\{k+1, \ldots, n\}$ et alors $H = G_{k-1}$ (cas 1. Proposition 4.2.6).

Cas 2 : Soient $O'_1, \ldots, O'_s$ les H-orbites incluses dans $\{k+1, \ldots, n\}$; la fonction auxiliaire `De_Gk_a_G(k-1)` recherche un entier i dans $[\![1, s]\!]$ et une permutation $\sigma \in G_{k-1}\backslash G_k$ vérifiant $\sigma(k) = Min(O'_i)$. La détermination d'une orbite O'_i est réalisée par l'appel :

`TrouverUnePermutation`$(k+1, [1, \ldots, k, Min(O'_i)], Id, \mathcal{P})$.

Pour tout $i \in [\![1, s]\!]$, nous posons $\mathcal{E}_i = \{\sigma \in G_{k-1}\backslash G_k \mid \sigma(k) \in O'_i\}$.

L'une des deux situations se présente alors :

Cas 2.1 : pour tout $i \in [\![1, s]\!]$, l'ensemble des permutations de $\sigma \in G_{k-1}\backslash G_k$ vérifiant $\sigma(k) = Min(O'_i)$ est vide ; d'après la remarque 4.3.5, ceci équivaut à $\forall i \in [\![1, s]\!]$, $\mathcal{E}_i = \emptyset$. Nous avons alors $G = G_{k-1}$ (cas 2. Proposition 4.2.6).

Cas 2.2 : Il existe $i_0 \in [\![1, r]\!]$ tel que $\sigma(k) = Min(O_{i_0})$. Dans ce cas, le groupe $H' = \langle H \cup \mathcal{E}_{i_0} \rangle$ est engendré par l'ensemble de permutations $\mathcal{G}' = \mathcal{G} \cup \{\sigma\}$ (voir Proposition 4.2.3).

Si $H = G_{k-1}$, le procédé s'arrête. Dans le cas contraire, la Fonction `De_Gk_a_G(k-1)` est appelée récursivement avec, pour nouveaux arguments, l'ensemble de permutations $\mathcal{G}'$ et la H'-orbite de $\{1, \ldots, n\}$ déterminée à l'aide de la fonction `NouvellesOrbites`.

Algorithme 4.2.11.

Fonction `De_Gk_a_G(k-1)`(k, $\mathcal{G}$, *orbites*, $\mathcal{P}$)

/*

Entrée : . k, l'indice du groupe G_k.
. $\mathcal{G}$, la liste utilisée pour stocker les permutations d'un ensemble de générateur de G_{k-1} et égale, au premier appel, à l'ensemble de générateurs de G_k.
. *orbites*, l'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action de G_k. */
. L'ensemble de conditions $\mathcal{P} = (P_1,\ldots,P_n)$ décrit dans le paragraphe 4.1.2.

Sortie : . $\mathcal{G}$, un ensemble de générateurs de G_{k-1}.
. *orbites*, l'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action de G_{k-1}.

$elts := \{\text{Min}(O) \mid O \in orbites \text{ et } O \subset \{k+1,\ldots,n\}\}$;
Tant que $elts \neq \emptyset$ **Faire**
. $a := \text{Min}\ (elts)$;
. $elts := elts \setminus \{a\}$;
. **Si** $P_k(1,2,\ldots,k-1,a)$ **Alors** (*Condition C*)
. . $\sigma :=$ `TrouverUnePermutation`$(k+1,\ [1,2,\ldots,k-1,a]$,$Id$,$\mathcal{P})$;
. . **Si** $\sigma \neq Id$ **Alors**
. . . $\mathcal{G} := \mathcal{G} \cup \{\sigma\}$;
. . . $orbites :=$ `NouvellesOrbites`$(orbites,\ \sigma)$;
. . . $elts := \{\text{Min}(O) \mid O \in orbites \text{ et } O \subset \{k+1,\ldots,n\}\}$;
. . **Fin Si** ;
. **Fin Si** ;
Fin Tant que ;
Retourner $\mathcal{G}$, *orbites* ;
Fin Fonction ;

Fonction `Generateurs`

La fonction `Generateurs`, définie ci-dessous, construit la suite croissante de groupes :

$$\{Id\} = G_n < G_{n-1} < \cdots < G_2 < G_1 < G_0.$$

Pour chacun de ces groupes, un ensemble de générateurs est calculé par `De_Gk_a_G(k-1)`. Le cardinal du groupe de décomposition est aussi calculé : ceci nous sera utile au paragraphes 4.2.5.

Algorithme 4.2.12. ---
Fonction `Generateurs`$(\mathcal{P})$
/*
Entrée : . L'ensemble de conditions $\mathcal{P} = (P_1,\ldots,P_n)$ décrit dans le paragraphe 4.1.2.

Sortie : . Le cardinal, noté *Cardinal*, du groupe $Dec(I)$;
. Une liste $\mathcal{G}$ de générateurs du groupe $Dec(I)$.
*/
$\mathcal{G} := \{Id_{S_n}\}$;
$orbites := \{\{1\},\ldots,\{n\}\}$;
$k := n-1$;

$Cardinal := 1$;
Tant que $k \neq 0$ **Faire**
. $\mathcal{G}$, $orbites := \texttt{De\_Gk\_a\_G(k-1)}(k, \mathcal{G}, orbites, \mathcal{P})$;
. $Cardinal := Card(Orb_{G_k}(k+1)) * Cardinal$;
. $k := k - 1$;
Fin Tant que ;
Retourner $Cardinal, \mathcal{G}$;
Fin Fonction ;

Remarque 4.2.13. L'égalité suivante, qui est une conséquence directe du lemme 4.2.5, permet le calcul du cardinal du groupe G

$$Card(G) = \prod_{i=0}^{n-1} Card(Orb_{G_i}(i+1)) \ .$$

Remarque 4.2.14. Une récurrence directe montre qu'à chaque étape, nous avons l'égalité

$$Card(\mathcal{G}) + Card(orbites) = n + 1.$$

Par conséquent, le nombre de générateurs retourné par cet algorithme est majoré par n.

Parcours d'arbre effectué par l'algorithme 4.2.12

Poursuivons l'exemple de l'idéal I_{6T3} (voir Exemple 4.2.2).

L'algorithme récursif 4.2.12 parcourt l'arbre de la figure 4.1 et retourne la liste $[Id, (5,6), (3,4), (1,2)(3,5)(4,6)]$. Le nombre de tests nécessaires au calcul du groupe de décomposition de I est alors de 32 alors qu'il est de 64 pour l'algorithme 4.2.1.

4.2.4 Complexité - Cas où l'hypothèse de prolongement des préfixes est vérifiée

Dans ce paragraphe, nous étudions la complexité de l'algorithme 4.2.12. Puisque le coût total de cet algorithme est dominé par le coût des formes normales effectuées, son efficacité est évaluée en terme de formes normales. Nous allons faire ce calcul de complexité lorsque l'hypothèse $\mathcal{H}$ de backtrack ci-dessous est réalisée.

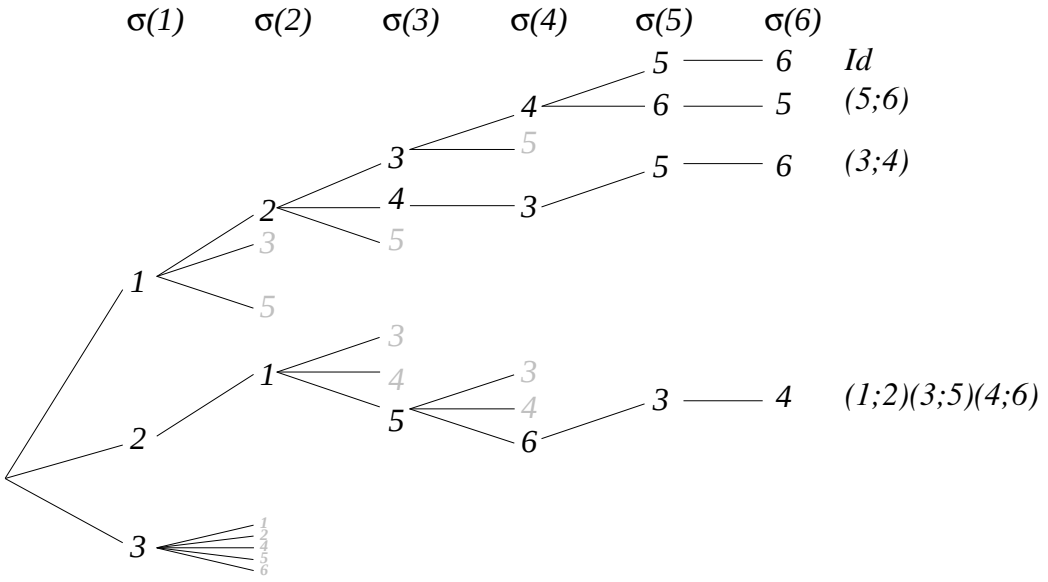


FIG. 4.1 – Parcours d'arbre effectué par l'algorithme `Generateurs`

Définition 4.2.15. Nous dirons que l'algorithme 4.2.11 effectue un *backtrack* lorsqu'un préfixe vérifiant la condition C de cet algorithme ne peut pas être prolongé, c'est à dire quand `TrouverUnePermutation` retourne $\{Id\}$. Rappelons qu'un préfixe vérifie la condition C s'il vérifie le prédicat P_k et que, dans ce cas, l'algorithme cherche à compléter ce préfixe en celui d'une permutation de D.

Nous allons majorer le nombre de formes normales calculées effectué par l'algorithme 4.2.12 lorsque l'hypothèse suivante est réalisée :

$\mathcal{H}$: *aucun backtrack n'apparaît lors du calcul de* D.

Cette hypothèse revient à dire que tout préfixe de longueur t apparaissant dans le calcul de D par l'algorithme 4.2.12 et vérifiant les conditions $P_1, \ldots, P_t$ peut être prolongé en un préfixe de longueur $t+1$ vérifiant les conditions $P_1, \ldots, P_{t+1}$.

Proposition 4.2.16. *Lorsque l'hypothèse* $\mathcal{H}$ *est vérifiée, le nombre de formes normales calculées par la fonction* `Generators` *est majoré par* $O(n^3)$.

Démonstration. Les calculs de formes normales effectués par l'algorithme `Generateurs` le sont lors des appels de la fonction `De_Gk_a_G(k-1)`.

Étudions la complexité de cette dernière fonction.

Lors d'un appel de la fonction `De_Gk_a_G(k-1)`, une forme normale est calculé pour tester la Condition C de l'algorithme 4.2.11. Deux cas apparaissent alors :

- la condition C est fausse et aucun autre calcul n'est effectuée pour le préfixe considéré. Dans ce cas, une seule forme normale est calculée. De plus, pour un appel de la fonction `De_Gk_a_G(k-1)`, ce cas apparaît au plus n fois ;
- la condition C est vraie. La fonction `TrouverUnePermutation` est alors appelée et l'hypothèse $\mathcal{H}$ assure qu'une permutation est retournée et adjointe au paramètre $\mathcal{G}$ de `De_Gk_a_G(k-1)`. Le théorème 4.2.21 permet une analyse immédiate de la complexité de cette fonction : le nombre de formes normales nécessaires au calcul de la permutation que cette fonction retourne est majoré par $O(n^2)$.

La fonction `Generateurs` appelle $n-1$ fois la fonction `De_Gk_a_G(k-1)`. Le nombre de formes normales calculées par lesquelles la condition C est fausse est donc majoré par $O(n^2)$.

Le cardinal du paramètre $\mathcal{G}$ est majoré par n (voir Remarque 4.2.14), donc la condition C est vraie au plus n fois. Par suite, pendant l'exécution de l'algorithme `Generateurs`, le nombre de formes normales pour lesquelles la condition C est vraie est majoré par $n\,O(n^2)$.

La complexité de l'algorithme `Generateurs` évaluée en terme de formes normales est majoré par $O(n^2) + n\,O(n^2) = O(n^3)$. □

4.2.5 Applications aux idéaux de Galois purs

Dans ce paragraphe, la notion d'idéal de Galois du chapitre 2 est étendue afin de définir un champ d'application plus large du résultat principal de ce paragraphe, le théorème 4.2.21. Ce théorème généralise celui d'Anai, Noro et Yokoyama (voir [3]) aux cas des idéaux de Galois de la définition 4.2.18. Le résultat d'Anai, Noro et Yokoyama ne s'applique qu'aux idéaux de relations (Voir Définition 2.2), seul cadre dans lequel il leur est nécéssaire d'effectuer le calcul du groupe de décomposition d'un idéal.

Le théorème 4.2.21 permet d'interpréter le parcours d'arbre effectué par les algorithmes 4.2.12 et `EFG` du paragraphe 4.3.2 et par ce biais d'évaluer leurs compléxités.

Soit I un idéal triangulaire radical. Notons $f_1, \ldots, f_n$ un ensemble triangulaire séparable de générateurs de I (voir Définition 2.1.11) et $V(I)$ sa variété (i.e. l'ensemble de zéros de I dans $\bar{K}$). Le cardinal de $V(I)$, $\Pi(I)$, est donné par la formule :

$$\Pi(I) = \prod_{i=1}^{n} \deg_{X_i}(f_i),$$

(voir [7] ou Corollaire 2.1.19). La proposition 4.2.17 ci-dessous est une conséquence directe de cette égalité.

Proposition 4.2.17. *Soit I un idéal triangulaire. Le groupe de décomposition $Dec(I)$ agit fidèlement sur la variété $V(I)$ et nous avons*

$$Card(Dec(I)) \leq \Pi(I)\,. \tag{4.2.1}$$

Lorsque la majoration (4.2.1) est une égalité, la variété $V(I)$ est déterminée uniquement par un élément $\underline{\alpha} \in \bar{K}$ et par $Dec(I)$ de par l'égalité :

$$V(I) = Dec(I).\underline{\alpha}\,.$$

Dans ce cas, l'idéal I est un *idéal de Galois pur*.

Nous voulons déterminer si I est un idéal de Galois pur et, si tel est le cas, calculer $Dec(I)$. Ci-après, nous montrons comment spécialiser l'algorithme 4.2.12 dans ce cas particulier.

Définition 4.2.18. Soit I un idéal de $K[X_1, \ldots, X_n]$ et $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ dans $V(I)$. L'idéal I est un $\underline{\alpha}$-*idéal de Galois* si les deux conditions suivantes sont réalisées :

1. si $i \neq j$ alors $\alpha_i \neq \alpha_j$;
2. il existe L, un sous ensemble de S_n tel que

$$I = \{f \in K[X_1, \ldots, X_n] \mid \forall \sigma \in L,\, f(\sigma.\underline{\alpha}) = 0\}.$$

Un tel idéal est noté $I^L_{\underline{\alpha}}$ et l'ensemble L est appelé son *injecteur relativement à* $\underline{\alpha}$.

Remarque 4.2.19. Le n-uplet $\underline{\alpha}$ de la définition précédente n'est pas nécéssairement un n-uplet des racines d'un polynôme. Cette définition étend donc celle des idéaux de Galois donnée au chapitre 2.

Définition 4.2.20. Soit σ une permutation de S_n et $t \in [\![1, n]\!]$. Le *préfixe de longueur t de σ* est la suite $(\sigma(1), \ldots, \sigma(t))$.

Théorème 4.2.21. *Soit I un idéal de Galois engendré par un ensemble triangulaire*

$$\mathcal{T} = \{f_1, f_2, \ldots, f_n\} \quad .$$

Soit $\underline{\alpha}$ l'un des zéros de I et L son injecteur relativement à $\underline{\alpha}$. Soit $t \in [\![1, n-1]\!]$ et $(c_1, \ldots, c_t)$ une t-liste de l'ensemble $\{1, \ldots, n\}$. Soit d le produit $\deg_{X_{t+1}}(f_{t+1}) \cdots \deg_{X_n}(f_n)$.

Pour tout $i \in [\![1, t]\!]$, $f_i(\alpha_{c_1}, \ldots, \alpha_{c_i}) = 0$ ssi il existe un élément $\sigma \in L$ admettant $(c_1, \ldots, c_t)$ pour préfixe de longueur t.

Plus précisément, le nombre de permutations de L de préfixe $(c_1, \ldots, c_t)$ est d.

Démonstration. Soit t un entier de $[\![1, n-1]\!]$. Puisque la variété V de I est équiprojectable (voir [7]), tout élément $\underline{\beta}$ de la variété de l'idéal $\langle f_1, f_2, \ldots, f_t \rangle$ est la projection sur les t premières coordonnées de d éléments de V.
La correspondance bijective entre V et L prouve alors le résultat. □

Remarque 4.2.22. Dans le cas particulier où I est un idéal de Galois maximal, le Théorème 5 de [3] est alors un corollaire du théorème précédent.

La proposition suivante joue un rôle central pour l'amélioration de l'algorithme 4.2.12 afin de tester si I est un idéal de Galois pur et, le cas échéant, pour le calcul de son groupe de décomposition.

Proposition 4.2.23. *Soit I un idéal engendré par un ensemble triangulaire S de générateurs. Si un backtrack apparaît lors d'un appel de la fonction* `Generateurs`(S) *par la fonction* `De_Gk_a_G(k-1)` *alors I n'est pas un idéal de Galois pur.*

Démonstration. Un backtrack apparaît dans l'algorithme 4.2.11 lorsqu'un préfixe $(c_1, \ldots, c_t)$, vérifiant $\forall i \in [\![1, t]\!]$ $f_i(\alpha_{c_1}, \ldots, \alpha_{c_i}) = 0$, ne peut pas être complété en un préfixe $(c_1, \ldots, c_{t+1})$ tel que $f_{t+1}(\alpha_{c_1}, \ldots, \alpha_{c_{t+1}}) = 0$. Autrement dit, l'algorithme a trouveé une permutation $\sigma \notin Dec(I)$ dont le préfixe de longueur t vérifie la condition de la proposition précédente. D'après le théorème 4.2.21, ceci ne peut se produire que si I n'est pas un idéal de Galois ou si I est un idéal de Galois tel que $Dec(I)$ ne soit pas l'injecteur de I. La proposition suit. □

Soit I un idéal triangulaire. Pendant le calcul du groupe $Dec(I)$ par l'algorithme 4.2.12, seuls deux cas peuvent se produire :

1. un backtrack apparaît et alors I n'est pas un idéal de Galois pur,
2. aucun backtrack n'apparaît et alors I est un idéal de Galois pur ssi la condition $Card(Dec(I)) = \Pi(I)$ est vérifiée.

Afin de tester si l'idéal triangulaire I est un idéal de Galois pur, l'algorithme 4.2.12 peut être modifié en un algorithme appelé `IsPureGaloisIdeal`. Pour cela, il suffit en cours de calcul de vérifier qu'aucun backtrack n'a lieu et, si tel est le cas, de tester l'égalité $Card(Dec(I)) = \Pi(I)$. Si aucun backtrack n'apparaît alors l'hypothèse $\mathcal{H}$ du paragraphe 4.2.4 est vérifiée et la proposition 4.2.16 admet alors pour corollaire :

Corollaire 4.2.24. *Soit $\langle S \rangle$ un idéal triangulaire de $K[X_1, \ldots, X_n]$. Le nombre de formes normales effectuées par la fonction* `IsPureGaloisIdeal` *est majoré par $O(n^3)$.*

4.3 Algorithme EFG - Application aux idéaux de Galois

Le premier algorithme de ce chapitre, l'algorithme `Generateurs`, n'exploite que partiellement les sous-groupes obtenus en cours de calcul pour déterminer un ensemble de permutations engendrant D.

Les propositions du paragraphe 4.3.1 vont permettre d'optimiser la fonction auxilliaire `TrouverUnePermutation` en imposant des contraintes plus fortes sur la permutation qu'il recherche. Nous remplacerons alors la fonction `TrouverUnePermutation` de l'algorithme `Generateurs` par la fonction `TUP` du paragraphe 4.3.1 pour définir un nouvel algorithme nommé `EFG`.

L'étude de complexité de `EFG` est l'objet du paragraphe 4.3.3. Nous bornons le nombre de formes normales effectuées par l'algorithme dans le cas des idéaux de Galois quelconque. Lorsque l'idéal est un idéal de Galois pur, cette borne est alors en $O(n^2)$.

Au paragraphe 4.3.4, nous nous intéressons au cas où un sous-groupe de $\mathrm{Dec}(I)$ est connu : cette information permet d'éviter de nombreux calculs. Une telle situation se présente lorsqu'apparaissent des modules de Cauchy dans l'ensemble triangulaire de générateur de I. C'est en particulier, le cas des idéaux de rupture.

4.3.1 Branch et cut complet

Reprenons les notations de la proposition 4.2.3.

La fonction `TrouverUnePermutation` de ce paragraphe effectue la recherche d'une permutation de $\mathcal{E}$ en se restreignant à celles qui transforment l'entier k en l'élément minimal d'un orbite O. La proposition 4.3.5 ci-après énonce des propriétés permettant d'imposer des contraintes supplémentaires à la permutation recherchée dans $\mathcal{E}$. Ces contraintes supplémentaires restreignent le nombre de tests d'appartenance à l'idéal I (voir Proposition 4.3.6).

Notations 4.3.1. Soient $r \in \{1, \ldots, n\}$ et G un sous-groupe de S_n.

Pour tout r-liste $[a_1, \ldots, a_r]$ d'entiers de $\{1, \ldots, n\}$, nous noterons $G_{[a_1,\ldots,a_r]}$ le fixateur dans G (des éléments) de l'ensemble $\{a_1, \ldots, a_r\}$:

$$G_{[a_1,\ldots,a_r]} = \{\sigma \in G \mid \forall i \in [\![1, r]\!],\ \sigma(a_i) = a_i\} .$$

Dans le cas particulier du r-uplet $[1, \ldots, r]$, conformément aux notations précédentes, le fixateur $G_{[1,\ldots,r]}$ est noté G_r ; la notation G_0 désignant le groupe G lui-même.

Nous noterons $\mathcal{M}_{G_{[]}} = \{Min(O) \mid O \in Orb(G)\}$ et, pour tout $s \in [\![1, n]\!]$,

$$\mathcal{M}_{G_{[a_1,\ldots,a_r]}} = \{Min(O) \mid O \in Orb(G_{[a_1,\ldots,a_r]})\} .$$

Exemple 4.3.2. Pour illustrer la notation $\mathcal{M}_{G_{[a_1,\ldots,a_r]}}$, considérons la permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{smallmatrix}\right)$ et le sous-groupe G de S_6 défini par

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

Dans le tableau suivant, sont regroupés les groupes $G_{[\sigma(1),\sigma(2),\dots,\sigma(s)]}$, leurs orbites respectives dans $\{1,\dots,6\}$ et les ensembles $\mathcal{M}_{G_{[\sigma(1),\sigma(2),\dots,\sigma(s)]}}$.

s	Groupes $G_{[\sigma(1),\sigma(2),\dots,\sigma(s)]}$	Orbites	Ensembles $\mathcal{M}_{G_{[\sigma(1),\sigma(2),\dots,\sigma(s)]}}$
0	G	$\{1,2,\dots,6\}$	$\mathcal{M}_{G_{[]}} = \{1\}$
1	$G_{[\sigma(1)]} = \langle (1;2),(3;4)\rangle$	$\{1,2\},\{3,4\},\{5\},\{6\}$	$\mathcal{M}_{G_{[\sigma(1)]}} = \{1,3,5,6\}$
2	$G_{[\sigma(1),\sigma(2)]} = \langle (1;2),(3;4)\rangle$	$\{1,2\},\{3,4\},\{5\},\{6\}$	$\mathcal{M}_{G_{[\sigma(1),\sigma(2)]}} = \{1,3,5,6\}$
3	$G_{[\sigma(1),\dots,\sigma(3)]} = \langle (1;2)\rangle$	$\{1,2\},\{3\},\dots,\{6\}$	$\mathcal{M}_{G_{[\sigma(1),\dots,\sigma(3)]}} = \{1,3,4,5,6\}$
4	$G_{[\sigma(1),\dots,\sigma(4)]} = \langle (1;2)\rangle$	$\{1,2\},\{3\},\dots,\{6\}$	$\mathcal{M}_{G_{[\sigma(1),\dots,\sigma(4)]}} = \{1,3,4,5,6\}$
5,6	$G_{[\sigma(1),\dots,\sigma(s)]} = \langle Id\rangle$	$\{1\},\dots,\{6\}$	$\mathcal{M}_{G_{[\sigma(1),\dots,\sigma(s)]}} = \{1,\dots,6\}$

Pour déterminer une permutation de l'ensemble $\mathcal{E}$ de la proposition 4.2.3, nous allons nous ramener à la recherche d'une permutation σ' telle que $\forall s \in [\![1,n]\!]$, $\sigma'(s) \in \mathcal{M}_{G_{[\sigma'(1),\dots,\sigma'(s-1)]}}$.

Lemme 4.3.3. *Soit G un sous-groupe de S_n. Pour toute permutation σ de S_n, il existe une unique permutation σ' de S_n telle que :*

1. $\forall s \in [\![1,n]\!]$, $\sigma'(s) \in \mathcal{M}_{G_{[\sigma'(1),\dots,\sigma'(s-1)]}}$;
2. $\sigma'\sigma^{-1} \in G$.

Démonstration. Raisonnons par récurrence sur k pour montrer l'assertion suivante.
Pour tout $k \in [\![1,n]\!]$, il existe une unique permutation $\sigma'_k \in S_n$ telle que :

1. $\forall s \in [\![1,k]\!]$, $\sigma'_k(s) \in \mathcal{M}_{G_{[\sigma'_{k'}(1),\dots,\sigma'_{k'}(s-1)]}}$;
2. $\sigma'_k\,\sigma^{-1} \in G$.

Au rang $k=1$, notons a le plus petit entier de la G-orbite contenant $\sigma(1)$. Il existe $\rho \in G$ tel que $\rho(\sigma(1)) = a$ car les entiers a et $\sigma(1)$ appartiennent à la même G-orbite. La permutation $\sigma'_1 = \rho.\sigma$ vérifie alors l'hypothèse de récurrence pour $k=1$.

Supposons l'assertion vraie au rang k pour $k \in [\![1,n-1]\!]$. Posons $F_k = G_{[\sigma'_k(1),\sigma'_k(2),\dots,\sigma'_k(k)]}$. Notons a le plus petit entier de l'orbite de $Orb(F_k)$ contenant $\sigma'_k(k+1)$. Il existe une permutation ρ de F_k telle que $\rho(\sigma'_k(k+1)) = a$ car un groupe agit transitivement sur ses orbites.

En posant $\sigma'_{k+1} = \rho.\sigma'_k$, la définition de ρ et la première assertion de l'hypothèse de récurrence montre que nous avons :

$$\forall s \in [\![1,k]\!],\ \sigma'_{k+1}(s) = \sigma'_k(s) \in \mathcal{M}_{G_{[\sigma'(1),\dots,\sigma'(s-1)]}} \subset \mathcal{M}_{G_{[\sigma'_{k+1}(1),\dots,\sigma'_{k+1}(s-1)]}}$$

car toute orbite de $Orb(F_{k+1})$ est incluse dans une orbite de $Orb(F_k)$. De plus, l'égalité $\rho(\sigma'_k(k+1)) = a$ implique $\sigma'_{k+1}(k+1) = \rho(\sigma'_k(k+1)) = a$ et, par suite, $\sigma'_{k+1}(k+1) \in \mathcal{M}_{G_{[\sigma'_{k+1}(1),\dots,\sigma'_{k+1}(s-1)]}}$.

L'égalité $\sigma'_k = \rho^{-1}.\sigma'_{k+1}$, avec $\rho \in G$, et l'assertion $\sigma'_k\sigma^{-1} \in G$ de l'hypothèse de récurrence prouvent l'assertion $\sigma'_{k+1}\sigma^{-1} \in G$. Ceci prouve le lemme. □

Exemple 4.3.4. Poursuivons l'exemple 4.3.2. Le lemme 4.3.3 se vérifie en considérant la permutation $\sigma' = \left(\begin{smallmatrix}1&2&3&4&5&6\\1&2&5&6&3&4\end{smallmatrix}\right)$ de S_6. En effet, en choisissant $\tau = (1;3;5)(2;4;6)(5;6)$ dans G,

- l'égalité $\sigma = \tau\sigma'$ confirme l'assertion 2. ;
- la condition 1. est vérifiée comme le montre le tableau suivant.

s	Groupes $G_{[\sigma'(1),\sigma'(2),\ldots,\sigma'(s)]}$	Ensembles $\mathcal{M}_{G,\sigma',s}$	$\sigma'(s)$
0	$G_{[]} = G$	$\mathcal{M}_{G,\sigma',0} = \{1\}$	$\sigma'(1) = 1 \in \mathcal{M}_{G_{[]}}$
1	$G_{[\sigma'(1)]} = \langle (3;4), (5;6)\rangle$	$\mathcal{M}_{G,\sigma',1} = \{1,2,3,5\}$	$\sigma'(2) = 2 \in \mathcal{M}_{G_{[\sigma'(1)]}}$
2	$G_{[\sigma'(1),\sigma'(2)]} = \langle (3;4), (5;6)\rangle$	$\mathcal{M}_{G,\sigma',2} = \{1,2,3,5\}$	$\sigma'(3) = 5 \in \mathcal{M}_{G_{[\sigma'(1),\sigma'(2)]}}$
3	$G_{[\sigma'(1),\ldots,\sigma'(3)]} = \langle (3;4)\rangle$	$\mathcal{M}_{G,\sigma',3} = \{1,2,3,5,6\}$	$\sigma'(4) = 6 \in \mathcal{M}_{G_{[\sigma'(1),\ldots,\sigma'(3)]}}$
4	$G_{[\sigma'(1),\ldots,\sigma'(4)]} = \langle (3;4)\rangle$	$\mathcal{M}_{G,\sigma',4} = \{1,2,3,5,6\}$	$\sigma'(5) = 3 \in \mathcal{M}_{G_{[\sigma'(1),\ldots,\sigma'(4)]}}$
5	$G_{[\sigma'(1),\ldots,\sigma'(5)]} = \{Id\}$	$\mathcal{M}_{G,\sigma',5} = \{1,\ldots,6\}$	$\sigma'(6) = 4 \in \mathcal{M}_{G_{[\sigma'(1),\ldots,\sigma'(5)]}}$

Proposition 4.3.5. *Soient H un sous-groupe de S_n tel que $G_k \subseteq H \subseteq G_{k-1}$ et O une H-orbite de $\{1,\ldots,n\}$ incluse dans $\{k+1,\ldots,n\}$.*

Si $\mathcal{E} = \{\sigma \in G_{k-1} \mid \sigma(k) \in O\}$ est non vide alors

$$\exists \sigma' \in \mathcal{E},\ \forall s \in [\![1,n]\!],\ \sigma'(s) \in \mathcal{M}_{G_{[\sigma'(1),\sigma'(2),\ldots,\sigma'(s-1)]}}.$$

Démonstration. D'après le lemme 4.3.3 appliqué à une permutation σ appartenant à l'ensemble $\mathcal{E}$, il existe une permutation σ' de S_n telle que

$$\forall s \in [\![1,n]\!],\ \sigma'(s) \in \mathcal{M}_{H_{[\sigma'(1),\ldots,\sigma'(s-1)]}}\ .$$

D'après ce lemme, nous avons, de plus, $\sigma' \in \mathcal{E}$.

Soit $s \in [\![1,n]\!]$. Puisque $G_k \subseteq H$, toute $H_{[\sigma'(1),\ldots,\sigma'(s-1)]}$-orbite s'écrit comme réunion de $G_{[\sigma'(1),\ldots,\sigma'(s-1)]}$-orbite et donc

$$\mathcal{M}_{H_{[\sigma'(1),\sigma'(2),\ldots,\sigma'(s-1)]}} \subset \mathcal{M}_{G_{[\sigma'(1),\sigma'(2),\ldots,\sigma'(s-1)]}}\ ,$$

d'où le résultat. □

Proposition 4.3.6. *Avec les notations de la proposition 4.3.5, si l'ensemble $\mathcal{E}$ est non vide alors il existe une permutation $\left(\begin{smallmatrix}1&\cdots&n\\a_1&\cdots&a_n\end{smallmatrix}\right) \in \mathcal{E}$ telle que :*

$$\forall s \in [\![k,n]\!]\,,\ \begin{cases} a_s \in \{Min(O) \mid O \in Orb(G_{[a_1,a_2,\ldots,a_s]})\} \setminus \{a_1,\ldots,a_{s-1}\} \\ \ et \\ P_s(a_1,\ \ldots\ ,a_s)\ . \end{cases} \tag{4.3.1}$$

Démonstration. Supposons que $\mathcal{E}$ soit non vide. D'après la proposition 4.3.5, il existe une permutation σ' vérifiant :

$$\forall s \in [\![k,n]\!],\ \sigma'(s) \in \mathcal{M}_{G_{[\sigma'(1),\sigma'(2),\ldots,\sigma'(s-1)]}}\ .$$

Posons, pour tout $i \in [\![1, n]\!]$, $a_i = \sigma'(i)$. Il vient :

$$\forall s \in [\![k, n]\!],\ a_s \in \{Min(O) | O \in Orb(H_{[a_1, a_2, \ldots, a_s]})\} \setminus \{a_1, \ldots, a_s\}\ . \tag{4.3.2}$$

De plus, la permutation $\sigma' = \left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$ appartient à $\mathrm{Dec}(I)$. Ainsi :

$$\forall s \in [\![1, n]\!],\ P_s(a_1, \ldots, a_s)\ . \tag{4.3.3}$$

Or, pour tout $s \in [\![1, k-1]\!]$, $a_i = i$ car $\sigma' \in \mathcal{E}$; l'assertion (4.3.3) est donc triviale pour tout $s \in [\![1, k-1]\!]$. Cette observation et l'assertion (4.3.2) terminent la preuve. □

La fonction `TUP` du paragraphe suivant repose sur la proposition 4.3.6.

4.3.2 Algorithme de calcul d'un ensemble fort de générateurs du groupe $\mathrm{Dec}(I)$

Fixons k dans $[\![1, n-1]\!]$ et reprenons les notations du paragraphe 4.2.3.

En cours de calcul, la fonction `De_Gk_a_G(k-1)` fait appel à la fonction `TUP` pour déterminer, si elle existe, une permutation σ appartenant à $\mathcal{E} = \{\sigma \in G_{k-1} \mid \sigma(k) \in O\}$, où O désigne une certaine H-orbite de $\{1, \ldots, n\}$.

Plus précisément, le préfixe $[a_1, \ldots, a_k]$ de la permutation recherchée vérifie :

* $a_k = Min(O)$ et
* $a_1 = 1, \ldots, a_{k-1} = k-1$ lorsque $k > 1$.

Soit $[a_1, \ldots, a_k]$ un préfixe vérifiant les conditions (4.3.1) de la proposition 4.3.6 seulement au rang $s = k$.

La fonction `TUP` est une fonction récursive ayant pour argument un entier $s \in [\![k+1, n-1]\!]$ et $l = [a_1, \ldots, a_{s-1}]$ une liste d'entiers deux à deux distincts. Initialement, nous avons $s = k+1$.

Si $s = n+1$, la permutation $\sigma = \left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$ de $\mathcal{E} \setminus \{Id\}$ vérifie les conditions (4.3.1) de la proposition 4.3.6 ; elle sera renvoyée par l'algorithme.

Si $s < n+1$, l'ensemble

$$\mathcal{M} = \{Min(O) | O \in Orb(H_{[a_1, \ldots, a_{s-1}]})\} \setminus \{a_1, \ldots, a_{s-1}\}$$

apparaissant dans les conditions (4.3.1) de la proposition 4.3.6 est calculé. L'algorithme évalue alors le prédicat $P_s(a_1, \ldots, a_{s-1}, a)$ où $a = Min(\mathcal{M})$ pour déterminer si le préfixe $[a_1, \cdots, a_{s-1}, a]$ est celui d'une permutation de $\mathcal{E}$. Deux cas se présentent :

Cas 1 : L'entier a vérifie ce test et donc les conditions (4.3.1) de la proposition 4.3.6 aux rangs $i \in [\![k, s]\!]$. La fonction s'appelle alors récursivement avec pour arguments $s+1$ et $[a_1, \ldots, a_{s-1}, a]$.

Cas 2 : L'entier a ne vérifie pas ce test. Le s-uplet $[a_1, \ldots, a_{s-1}, a]$ ne vérifie donc pas les conditions nécessaires (4.3.1) de la proposition 4.3.6 (au rang s). Il n'existe donc pas de permutation $\mathcal{E}$ de préfixe $[a_1, \ldots, a_{s-1}, a]$. L'entier a est exclu de $\mathcal{M}$ et alors l'une des deux situations suivantes se présente :

Cas 2.1 : L'ensemble $\mathcal{M}$ est non vide. Dans ce cas, l'algorithme réitère sa recherche d'un entier $a \in \mathcal{M}$ pour lequel $P_s(a_1, \ldots, a_{s-1}, a)$ est vrai, en considérant l'entier $a = Min(\mathcal{M})$.

Cas 2.2 : L'ensemble $\mathcal{M}$ est vide, nous avons donc :

$$\forall a \in \mathcal{M},\ P_s(a_1, \ldots, a_{s-1}, a)\ .$$

Les conditions nécessaires (4.3.1) de la proposition 4.3.6 montrent qu'il n'existe pas de permutation de $\mathcal{E}$ admettant pour préfixe le $(s-1)$-uplet $[a_1, \ldots, a_{s-1}]$. Dans ce cas, la fonction renvoie la permutation $\sigma = Id$.

Algorithme 4.3.7.

Fonction TUP $(s, [a_1, \ldots, a_{s-1}], \sigma, \mathcal{P})$
/*
Entrées : . Un entier s de $\{1, \ldots, n+1\}$.
. Une liste $[a_1, \ldots, a_{s-1}]$ d'entiers de $\{1, \ldots, n\}$, distincts deux à deux.
. Une permutation σ égale à Id jusqu'à ce qu'une permutation de $\mathcal{E}$ soit trouvée.
. L'ensemble de conditions $\mathcal{P} = (P_1, \ldots, P_n)$ décrit dans le paragraphe 4.1.2.

Sortie : . Une permutation $\sigma = \left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$ appartenant à $\mathcal{E}$ si elle existe, Id sinon.

Note : . Avec ces entrées, si la fonction TUP s'appelle récursivement, c'est avec un préfixe $[a_1, \ldots, a_{s-1}, a]$ vérifiant les conditions $\forall j \in [\![1, s]\!]$, $P_j(a_1, \ldots, a_j)$ et $P_s(a_1, \ldots, a_{s-1}, a)$.
*/
Si $s = n+1$ **Alors** $\sigma = \left(\begin{smallmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{smallmatrix}\right)$;
Sinon
. $\mathcal{M} = \{Min(O) | O \in Orb(H_{[a_1,\ldots,a_{s-1}]})\} \setminus \{a_1, \ldots, a_{s-1}\}$;
. **Tant que** $\mathcal{M} \neq \emptyset$ **et** $\sigma = Id$ **faire**
. . $a = Min(\mathcal{M})$;
. . $\mathcal{M} = \mathcal{M} \setminus \{a\}$;
. . /* Recherche d'une image possible a de s */
. . **Si** $P_s(a_1, \ldots, a_{s-1}, a)$ **Alors**
. . . $\sigma =$ TUP $(s+1, [a_1, \ldots, a_{s-1}, a], \sigma, S)$;
. . **Fin Si** ;
. **Fin Tant Que** ;
Fin Si ;
Retourner σ ;
Fin Fonction

Nous appelons EFG l'algorithme obtenu en substituant la fonction TUP du paragraphe 4.3.2 à la fonction TrouverUnePermutation dans l'algorithme Generateurs .

Parcours d'arbre effectué par l'algorithme

Pour comparer les parcours d'arbre effectués par les algorithmes `Generateurs` et `EFG`, nous allons considérer l'idéal engendré dans $\mathbb{Q}[X_1, \ldots, X_8]$ par l'ensemble triangulaire de polynômes :

$$
\begin{aligned}
f_1(x_1) &= X_1^8 - 2X_1^7 - 9X_1^6 + 10X_1^5 + 22X_1^4 - 14X_1^3 - 15X_1^2 + 2X_1 + 1 \\
f_2(x_1, x_2) &= X_2 + 1/2X_1^7 - 3/2X_1^6 - 4X_1^5 + 10X_1^4 + 10X_1^3 - 16X_1^2 - 11/2X_1 + 3/2 \\
f_3(x_1, x_2, x_3) &= X_3^2 + X_3X_1^6 - X_3X_1^5 - 9X_3X_1^4 - X_3X_1^3 + 14X_3X_1^2 + 6X_3X_1 - X_3 \\
&\quad + 1/2X_1^7 - 1/2X_1^6 - 5X_1^5 + X_1^4 + 9X_1^3 - 2X_1^2 - 1/2X_1 + 1/2 \\
f_4(x_1, \ldots, x_4) &= X_4 + X_3 + X_1^6 - X_1^5 - 9X_1^4 - X_1^3 + 14X_1^2 + 6X_1 - 1 \\
f_5(x_1, \ldots, x_5) &= X_5^2 - 3/2X_5X_1^7 + 2X_5X_1^6 + 14X_5X_1^5 - 5X_5X_1^4 - 28X_5X_1^3 + 3X_5X_1^2 \\
&\quad + 19/2X_5X_1 + 3/2X_1^6 - X_1^5 - 15X_1^4 - 4X_1^3 + 27X_1^2 + 11X_1 - 9/2 \\
f_6(x_1, \ldots, x_6) &= X_6 + X_5 - 3/2X_1^7 + 2X_1^6 + 14X_1^5 - 5X_1^4 - 28X_1^3 + 3X_1^2 + 19/2X_1 \\
f_7(x_1, \ldots, x_7) &= X_7^2 + X_7X_1^7 - 3/2X_7X_1^6 - 9X_7X_1^5 + 4X_7X_1^4 + 19X_7X_1^3 - X_7X_1^2 - 9X_7X_1 \\
&\quad - 5/2X_7 - 1/2X_1^7 + X_1^6 + 5X_1^5 - 6X_1^4 - 14X_1^3 + 8X_1^2 + 23/2X_1 + 1 \\
f_8(x_1, \ldots, x_8) &= X_8 + X_7 + X_1^7 - 3/2X_1^6 - 9X_1^5 + 4X_1^4 + 19X_1^3 - X_1^2 - 9X_1 - 5/2 \quad .
\end{aligned}
$$

(Cet idéal est l'idéal induit de l'idéal de rupture du polynôme $X^8 - 2X^7 - 9X^6 + 10X^5 + 22X^4 - 14X^3 - 15X^2 + 2X + 1$ de $\mathbb{Q}[X]$. Ce type d'idéaux de Galois est défini au Paragraphe 5.1)

L'algorithme récursif `Generateurs` du paragraphe 4.3.2 appliqué à l'idéal I parcourt l'intégralité de l'arbre 4.2 ci-après. Le sous-arbre de l'arbre 4.2 constitué des parties non grisées est celui parcouru par `EFG`.

À chaque nombre apparaissant dans cet arbre correspond un test d'appartenance à l'idéal, sauf pour la branche supérieure, où seuls les 2 derniers entiers correspondent à des tests non triviaux. Lorsque ce test d'appartenance est négatif, l'entier est barré .

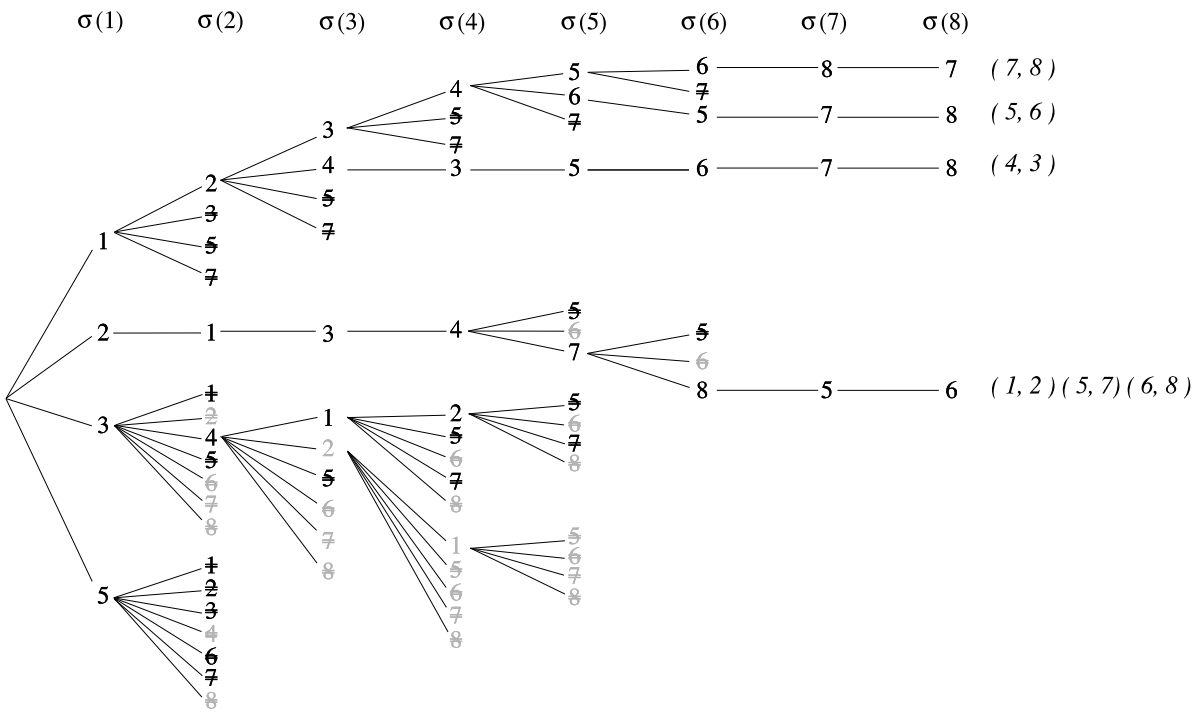


FIG. 4.2 – Arbres parcourus par les algorithmes

Décrivons le calcul de la permutation $(1;2)(5;7)(6;8)$ par la fonction `TUP` à partir de l'appel par la fonction `De_Gk_a_G(k-1)`. Rappelons qu'ici le groupe D est le groupe de décomposition de I, $\mathrm{Dec}(I)$, et que l'ensemble des prédicats $\mathcal{P} = \{P_1, \ldots, P_n\}$ est défini, au paragraphe 4.1.2, par :

$$\forall r \in [\![1, n]\!],\ (P_r(a_1, \ldots, a_r) \text{ est vrai}) \text{ ssi } (f_r(X_{a_1}, X_{a_2}, \ldots, X_{a_r}) \in I)\ .$$

Le calcul de l'ensemble fort de générateurs du fixateur G_1 ayant été effectué, nous avons $G_1 = \langle (3;4), (5;6), (7;8) \rangle$ et, à partir de cet ensemble de générateurs, la fonction `De_Gk_a_G(k-1)` commence le calcul de $\mathrm{Dec}(I)$. Pour cela, la fonction `De_Gk_a_G(k-1)` détermine l'ensemble $\{\{2\}, \{3;4\}, \{5;6\}, \{7;8\}\}$ des G_1-orbites de $\{1, \ldots, n\}$ incluses dans $\{2, \ldots, n\}$ et calcule l'ensemble $\mathcal{M} = \{2, 3, 5, 7\}$ des éléments minimaux de ces orbites. La fonction `TUP` est alors appelée par la fonction `De_Gk_a_G(k-1)` pour rechercher une permutation de préfixe $[Min(E)] = [2]$ via l'appel :

$$\texttt{TUP}(2,\ [2],\ Id,\ \mathcal{P})\ \ .$$

La fonction `TUP` calcule alors l'ensemble

$$\mathcal{M}_{G_{[1,2]}} \setminus \{2\} = \{Min(O) | O \in Orb(G_{[1,2]})\} \setminus \{2\} = \{1, 3, 7\}$$

puis teste pour $a = 1 \in \mathcal{M}_{G_{[1,2]}} \setminus \{2\}$ l'appartenance à l'idéal I du polynôme $f_2(X_2, X_a)$. Ce test retournant la valeur `vraie`, la fonction s'appelle récursivement pour compléter le préfixe $[2, 1]$.

De la même manière, les préfixes $[2, 1, 3]$ et $[2, 1, 3, 4]$ sont obtenus par deux appels récursifs de la fonction `TUP`, en calculant les ensembles $\mathcal{M}_{G_{[2,1]}} \setminus \{2, 1\} = \{3, 5, 7\}$ puis $\mathcal{M}_{G_{[2,1,3]}} \setminus \{2, 1, 3\} = \{4, 5, 7\}$ et en testant l'appartenance des polynômes $f_3(X_2, X_1, X_3)$ et $f_4(X_2, X_1, X_3, X_4)$ à l'idéal I.

La fonction cherche alors à compléter la liste $[2, 1, 3, 4]$ en le préfixe $[2, 1, 3, 4, a]$ d'une permutation $\sigma \in \mathrm{Dec}(I)$ (si toutefois cette permutation existe), où a est un entier appartenant à l'ensemble $\mathcal{M}_{G_{[2,1,3,4]}} \setminus \{2, 1, 3, 4\} = \{5, 7\}$. Le polynôme $f_5(X_2, X_1, X_3, X_4, X_5)$ n'appartenant pas à I, l'entier $a = 5$ apparaît donc barré dans l'arbre 4.2.

Ensuite, l'algorithme détermine alors si $[2, 1, 3, 4, 7]$ est un préfixe possible d'une permutation de $\mathrm{Dec}(I)$; pour cela, il teste l'appartenance du polynôme $f_5(X_2, X_1, X_3, X_4, X_7)$ à l'idéal I.

Ce test étant positif, l'algorithme s'appelle alors récursivement pour compléter la suite $[2, 1, 3, 4, 7]$ en un préfixe $[2, 1, 3, 4, 7, b]$, où $b \in \mathcal{M}_{G_{[2,1,3,4,7]}} \setminus \{2, 1, 3, 4, 7\} = \{5, 8\}$. Le polynôme $f_6(X_2, X_1, X_3, X_4, X_7, X_5)$ n'appartenant pas à l'idéal I, l'entier 5 apparaît barré dans l'arbre 4.2 et l'appartenance de $f_6(X_2, X_1, X_3, X_4, X_7, X_8)$ à l'idéal I est alors testé.

Ce test retournant la valeur `vraie`, la fonction s'appelle récursivement pour compléter le préfixe $[2, 1, 3, 4, 7, 8]$.

Après les deux appels récursifs suivants, la fonction `TUP` retourne la permutation $(1; 2)(5; 7)(6; 8)$.

Les algorithmes `Generateurs` et l'algorithme `EFG` calculent respectivement 73 et 48 formes normales pour calculer $\mathrm{Dec}(I)$.

4.3.3 Complexité - Cas général

Ce paragraphe est consacré à l'étude de la compléxité de l'algorithme `EFG` appliqué à un idéal de Galois I. Comme dans le cas de l'algorithme `IsPurGaloisIdeal`, nous cherchons à majorer le nombre de prédicats calculés par l'algorithme, c'est-à-dire de tests d'appartenance à l'idéal I.

Nous allons, tout d'abord, majorer le nombre de r-liste $[a_1, \ldots, a_r]$ où $1 \leqslant r \leqslant n - 1$ vérifiant les conditions

$$\forall s \in [\![1, r]\!] \, , \, P_s(a_1, \ \ldots \ , a_s) \ ; \tag{4.3.4}$$

$$\forall s \in [\![1, r]\!] \, , \, a_s \in \mathcal{M}_{D_{[a_1, a_2, \ldots, a_s])}} \setminus \{a_1, \ldots, a_{s-1}\}. \tag{4.3.5}$$

Toute r-liste passée comme argument à la fonction `De_Gk_a_G(k-1)` ou à la fonction `TUP` pendant l'exécution de l'algorithme `generateurs2` vérifie les conditions ci-dessus

(voir Paragraphe 4.3.2).

L'ensemble des r-listes d'entiers de $[\![1, n]\!]$ vérifiant les conditions (4.3.4) sera noté E.

Majoration du nombre de r-listes vérifiant les conditions (4.3.4) et (4.3.5)

Soit $r \in [\![1, n-1]\!]$. Notons $\sim$ la relation d'équivalence définie sur E par : pour tout $[a_1, \ldots, a_r] \in E$ et $[a'_1, \ldots, a'_r] \in E$,

$$[a_1, \ldots, a_r] \sim [a'_1, \ldots, a'_r] \quad \text{ssi} \quad \exists d \in \mathrm{Dec}(I),\ [a_1, \ldots, a_r] = [d(a'_1), \ldots, d(a'_r)]\ .$$

Proposition 4.3.8. *L'ensemble des r-listes de E vérifiant la condition (4.3.5) est un système de représentants des classes de $\sim$-équivalence de E.*

Démonstration. En effet, tout élément $\underline{a} \in E$ appartient à la classe $\mathrm{Dec}(I).\underline{a}$ de $\sim$-équivalence de E et l'élément minimal $\underline{b}$ de cette classe, pour l'ordre lexicographique $<_{lex}$ sur E, vérifie la condition (4.3.5). □

L'ensemble de r-listes vérifiant les conditions (4.3.4) et (4.3.5) est donc égal au nombre de classes de $\sim$-équivalence de E.

Considérons un injecteur L de I.

Notons $\sim_D$ la relation d'équivalence définie sur L par : pour tout $\sigma_1 \in L$ et tout $\sigma_2 \in L$,

$$\sigma_1 \sim_D \sigma_2 \quad \text{ssi} \quad \exists d \in \mathrm{Dec}(I),\ \sigma_1 = d\,\sigma_2\ .$$

Proposition 4.3.9. *L'application définie par*

$$\begin{array}{rcl} \Pi_r :\ L/\sim_D & \longrightarrow & E/\sim \\ \sigma & \longrightarrow & (\sigma(1), \ldots, \sigma(r))\ . \end{array}$$

est bien définie et est surjective.

Démonstration. Π_r est bien définie. Soient σ_1 et σ_2 deux permutations de L. Supposons que $\sigma_1 \sim_D \sigma_2$. Il existe donc $d \in \mathrm{Dec}(I)$ telle que $\sigma_1 = d\sigma_2$. Nous avons alors

$$(\sigma_1(1), \ldots, \sigma_1(r)) = (d\sigma_2(1), \ldots, d\sigma_2(r)) = d.(\sigma_2(1), \ldots, \sigma_2(r))\ ;$$

et donc $\Pi_r(\sigma_1) = \Pi_r(\sigma_2)$

Π_r est surjective. En effet, d'après le théorème 4.2.21, toute r-liste de E est le préfixe d'une permutation σ de L. □

Le nombre de classes de $\sim_D$-équivalence de L majore donc le nombre de r-listes vérifiant les conditions (4.3.4) et (4.3.5).

Définition 4.3.10. Le sous-groupe de S_n défini par $\mathrm{Inj}(L) = \{\sigma \in S_n \mid \sigma.L = L\}$ est appelé l'injecteur de L. (Cet ensemble est un groupe car c'est une partie de S_n stable pour le produit dans S_n.)

Lemme 4.3.11. *Soient E_1 et E_2 deux parties de S_n. Si $E_1 = E_2\, E_1$ (resp. $E_1 = E_1\, E_2$) alors E_1 est réunion de classe à droite (resp. à gauche) de E_1 modulo E_2, i.e. il existe $T \subset E_1$ tel que E_1 s'écrive comme l'union disjointe :*

$$E_1 = \bigcup_{\tau \in T} E_2\, \tau \text{ (resp., } E_1 = \bigcup_{\tau \in T} \tau\, E_2\text{).}$$

De plus, nous avons $\mathrm{Card}(T) = \dfrac{\mathrm{Card}(E_1)}{\mathrm{Card}(E_2)}$ *(resp.* $\mathrm{Card}(T) = \dfrac{\mathrm{Card}(E_2)}{\mathrm{Card}(E_1)}$*). L'ensemble T sera appelé une transversale à droite (resp., à gauche) de E_1 modulo E_2.*

Démonstration. En effet, si $\tau \in E_1$ alors $E_1 \supset E_2.\tau$; ainsi, E_1 est réunion d'ensemble $E_2.\tau$ où $\tau \in E_1$. De plus, pour tout $\tau \in E_1$ et tout $\tau' \in E_1$, l'égalité $\tau E_2 \cap \tau' E_2 \neq \emptyset$ implique $\tau E_2 = \tau' E_2$; d'où le résultat. □

Proposition 4.3.12. *Notons $d_1, \ldots, d_t$ une tranversale à droite de L modulo* $\mathrm{Inj}(L)$ *et $\ell_1, \ldots, \ell_s$ une tranversale à gauche de L modulo* $\mathrm{Dec}(I)$*. Nous avons :*

$$t = \mathrm{Card}(L)/\,\mathrm{Card}(\mathrm{Inj}(L)) \text{ et } s = \mathrm{Card}(L)/\,\mathrm{Card}(\mathrm{Dec}(I))\,.$$

Pour toute permutation σ de L, il existe $i \in [\![1, t]\!]$ et $j \in [\![1, s]\!]$ tel que $\sigma \in \mathrm{Dec}(I)\, \ell_j\, d_i$.

Démonstration. Nous avons les égalités $\mathrm{Inj}(L)L = L$ et $L\ \mathrm{Dec}(I) = L$ qui proviennent de la définition de $\mathrm{Inj}(L)$ et de la proposition 2.4.11. Le lemme 4.3.11 justifie l'existence des transversales de L considérées dans la proposition et les égalités $t = \mathrm{Card}(L)/\,\mathrm{Card}(\mathrm{Inj}(L))$ et $s = \mathrm{Card}(L)/\,\mathrm{Card}(\mathrm{Dec}(I))$.
Soit $\sigma \in L$. Puisque $L = \bigcup_{i=1}^{t} \mathrm{Inj}(L)\, d_i$, il existe $i \in [\![1, t]\!]$ et $\rho \in \mathrm{Inj}(L)$ tel que $\sigma = \rho\, d_i$. Or $\mathrm{Inj}(L)$ est un groupe, ainsi $\rho^{-1} \in \mathrm{Inj}(L)$ et, puisque $\mathrm{Inj}(L) \subset L$ (car $\mathrm{Inj}(L)L = L$ et L, étant un injecteur de I, contient Id_{S_n}), $\rho^{-1} \in L$. L'égalité $L = \bigcup_{j=1}^{s} \ell_j\ \mathrm{Dec}(I)$ montre qu'il existe $j \in [\![1, s]\!]$ et $d \in \mathrm{Dec}(I)$ tel que $\rho^{-1} = \ell_j\, d$. Par suite, $\sigma = d\, \ell_j^{-1}\, d_i$. □

Nous allons maintenant majorer le nombre de r-listes vérifiant les conditions (4.3.4) et (4.3.5) à l'aide des classes de $\sim_D$-équivalence de L.

Corollaire 4.3.13. *Le nombre de classes de $\sim_D$-équivalence de L, et donc le nombre de r-listes de E vérifiant la condition (4.3.5), est au plus égal à*

$$\frac{\mathrm{Card}(L)^2}{\mathrm{Card}(\mathrm{Dec}(I))\ \mathrm{Card}(\mathrm{Inj}(L))}\,.$$

Démonstration. D'après la proposition précédente, l'ensemble des permutations $\{\, \ell_j\, d_i \mid i \in [\![1, t]\!],\ j \in [\![1, s]\!]\}$ contient au moins un représentant par classe de $L/\sim_D$. Le nombre de classe de $\sim_D$-équivalence de L est donc majoré par le produit $s\, t$, autrement dit par $\frac{\mathrm{Card}(L)^2}{\mathrm{Card}(\mathrm{Dec}(I))\ \mathrm{Card}(\mathrm{Inj}(L))}$. □

Majoration du nombre de prédicats calculés par l'algorithme EFG

Rappelons tout d'abord que toute r-liste $[a_1, \ldots, a_r]$ où $1 \leqslant r \leqslant n-1$ passée comme argument à la fonction `De_Gk_a_G(k-1)` ou à la fonction `TUP` vérifie les conditions (4.3.4) et (4.3.5). Pour déterminer un entier $a_{r+1} \in [\![1, n]\!] \setminus \{a_1, \ldots, a_s\}$ tel que $P_{r+1}(a_1, \ldots, a_s)$, les fonctions `De_Gk_a_G(k-1)` et `TUP` effectuent au plus $n - r$ calculs de prédicats. Pour compléter une r-liste vérifiant les conditions (4.3.4) et (4.3.5) en des $r+1$ listes vérifiant ces mêmes conditions, l'algorithme `EFG` effectue donc au plus

$$\frac{\mathrm{Card}(L)^2}{\mathrm{Card}(\mathrm{Dec}(I))\ \mathrm{Card}(\mathrm{Inj}(L))}\,(n-r)$$

calculs de prédicats (i.e. le produit du majorant du nombre de r-listes vérifiant les conditions (4.3.4) et (4.3.5) (voir Corollaire 4.3.13) par le majorant du nombre de prédicats par r-liste considérée).
En sommant les majorants des nombres de prédicats calculés pour r parcourant $[\![1, n-1]\!]$, nous obtenons la complexité de l'algorithme `EFG` en terme de calculs de prédicats :

$$O\left(\frac{\mathrm{Card}(L)^2}{\mathrm{Card}(\mathrm{Dec}(I))\ \mathrm{Card}(\mathrm{Inj}(L))}n^2\right).$$

Cas des idéaux de Galois purs

Dans le cas d'un idéal de Galois pur, nous avons $L = \mathrm{Dec}(I) = \mathrm{Inj}(L)$ (voir Proposition 2.4.12 et définition 2.4.13). Le coût de cet algorithme est alors en $O(n^2)$ calculs de prédicats.

4.3.4 Cas où un sous-groupe est connu

Dans cette partie, nous supposons connu un sous-groupe $\overline{G}$ du groupe $G = \mathrm{Dec}(I)$. Ce type de situation sera illustré par le cas des idéaux de rupture. La donnée du groupe $\overline{G}$ permet de déterminer sans calcul de prédicat des permutations recherchées par la fonction `De_Gk_a_G(k-1)`.

Notons $\overline{\mathcal{G}}$ un ensemble fort de générateurs de $\overline{G}$. Posons $\overline{\mathcal{G}}_0 = \overline{\mathcal{G}}$ et, pour tout $k \in [\![2, n]\!]$, $\overline{\mathcal{G}}_{k-1} = \overline{\mathcal{G}} \cap \overline{G}_{k-1}$.

Soit k un entier quelconque de $[\![1, n]\!]$.

Rappelons que la fonction `De_Gk_a_G(k-1)` appelle la fonction `TUP` pour rechercher des permutations σ de $G_{k-1} \setminus G_k$. Les permutations trouvées sont alors adjointes à l'ensemble fort de générateurs de G_k pour construire l'ensemble fort de générateurs de G_{k-1}, cette construction s'appuie sur la proposition 4.2.3.
Or cette proposition peut s'appliquer à tout ensemble de générateurs $\mathcal{L}$ d'un sous-groupe L de $\mathrm{Dec}(I)$ vérifiant $G_k \subset L \subset G_{k-1}$, ce qui est le cas de la réunion de $\overline{\mathcal{G}}_{k-1}$ et de l'ensemble fort de générateurs $\mathcal{G}_k$ de G_k.

Ainsi, pour exploiter la donnée du sous-groupe $\overline{G}$ du groupe de décomposition G, il suffit, lors de l'appel de la fonction `De_Gk_a_G(k-1)` par la fonction `Generateurs`, de passer comme argument l'ensemble de permutations $\mathcal{L} = \overline{\mathcal{G}}_{k-1} \cup \mathcal{G}_k$ et les $\langle\mathcal{L}\rangle$-orbites de $\{1, \ldots, n\}$. Ceci est réalisé par la fonction `SousGroupeConnu` ci-dessous qui vient en substitution à la fonction `Generateurs`.

La fonction `De_Gk_a_G(k-1)` permettra alors de compléter l'ensemble $\mathcal{L}$ en un ensemble fort de générateurs de G_{k-1}.

Algorithme 4.3.14.

La fonction `Orbits` de cet algorithme retourne les orbites dans $\{1, \cdots, n\}$ du groupe engendré par l'ensemble fort de générateurs qui lui est passé comme argument.

Fonction `SousGroupeConnu` ($\mathcal{P}$, $\overline{\mathcal{G}}$)

/*
Entrée : . L'ensemble des conditions $\mathcal{P} = (P_1, \ldots, P_n)$ décrit dans le paragraphe 4.1.2.
. Un ensemble fort de générateurs $\overline{\mathcal{G}}$ du sous-groupe $\overline{G}$ de Dec(I).

Sortie : . Un ensemble, noté $\overline{\mathcal{G}}_0$, de générateurs du groupe $Dec(I)$.
*/

$\overline{\mathcal{G}}_0 := \{Id\}$;
$orbites := \{\{1\}, \ldots, \{n\}\}$;
$k := n - 1$;
Tant que $k \neq 0$ **faire**
. $\overline{\mathcal{G}}_k = \overline{\mathcal{G}} \cap G_k$;
. $\mathcal{L} = \overline{\mathcal{G}}_0 \cup \overline{\mathcal{G}}_k$;
. $orbites =$ `Orbites`($\mathcal{L}$) ;
. $\overline{\mathcal{G}}_0$, $orbites =$ `De_Gk_a_G(k-1)`(k, $\mathcal{L}$, $orbites$, $\mathcal{P}$) ;
. $k := k - 1$;
Fin Tant que ;
Retourner $\overline{\mathcal{G}}_0$;
Fin Fonction ;

Le théorème suivant permet de déterminer facilement un sous-groupe du groupe de décomposition d'un idéal triangulaire. Le paragraphe ci-après présente une situation où il sera appliqué.

Théorème 4.3.15. *(voir [50] et [17]) . Soit $g \in A[X]$ un polynôme à coefficient dans un anneau A de degré d. Notons*

$$C_0(X_1),\ C_1(X_1, X_2),\ \ldots\ ,\ C_d(X_1,\ \ldots\ , X_d)$$

les modules de Cauchy de g (voir Définition 2.2.4). Le groupe de décomposition de l'idéal engendré par $C_0(X_1),\ C_1(X_1, X_2),\ \ldots\ ,\ C_d(X_1,\ \ldots\ , X_d)$ est S_d.

Remarque 4.3.16. Un ensemble fort de générateurs du groupe symétrique S_d est

$$\{(1;2),\,(2;3),\,(3;4),\,\ldots\,,(d-1\,;d)\}\,.$$

Cas des idéaux de rupture

Soit f désigne un polynôme séparable de $K[X]$ de degré n et $\alpha_1,\,\ldots\,,\alpha_n$ les n racines du polynôme f dans une clôture algébrique de K. Nous définissons rapidement la notion d'idéal de départ d'un polynôme qui sera vue au chapitre 5.

Notons $g_1(\alpha_1,X)=X-\alpha_1$, $g_2(\alpha_1,X),\ldots,g_r(\alpha_1,X)$ les facteurs irréductibles de f sur $K(\alpha_1)[X]$ ordonnés dans l'ordre croissant de leurs degrés respectifs $d_1,d_2,\ldots,d_n$ en X.

Posons $s_1=1$, $s_{r+1}=n+1$ et $T_{g_1}(\alpha_1)=\{f(X_1)\}$. Pour tout $i\in[\![2,r]\!]$, posons $s_i=1+d_1+d_2+\cdots+d_{i-1}$ et

$$T_{g_i}(\alpha_1)=\{f_{s_i}(\alpha_1,X_{s_i})=g_i(\alpha_1,X_{s_i}),\,\ldots\,,f_{s_{i+1}-1}(\alpha_1,X_{s_i},\,\ldots\,,X_{s_{i+1}-1})\}\,,$$

l'ensemble des modules de Cauchy du polynôme g_i pris dans $K[X_{s_i},\ldots,X_{s_{i+1}-1}]$.

L'*idéal de départ du polynôme* f est l'idéal triangulaire I_f de $K[X_1,\,\ldots\,,X_d]$ engendré par l'ensemble triangulaire :

$$\begin{aligned} S &= \bigcup_{i=1}^{r} T_{g_i}(X_1) \\ &= \{f_1(X_1),\,f_2(X_1,X_2),\,\ldots\,,f_n(X_1,\ldots,X_n)\}. \end{aligned}$$

Proposition 4.3.17. *Le stabilisateur* $\mathrm{Dec}(I_f)_{[1]}$ *est égal au produit direct de groupes* $S_{\{1\}}\times S_{\{s_2,\ldots,s_3-1\}}\times\cdots\times S_{\{s_r,\ldots,s_{r+1}-1\}}$.

Démonstration. Montrons l'inclusion :

$$S_{\{1\}}\times S_{\{s_2,\ldots,s_3-1\}}\times\cdots\times S_{\{s_r,\ldots,s_{r+1}-1\}}\subset\mathrm{Dec}(I_f)_{[1]}\ . \tag{4.3.6}$$

Soit $\sigma\in S_{\{1\}}\times S_{\{s_2,\ldots,s_3-1\}}\times\cdots\times S_{\{s_r,\ldots,s_{r+1}-1\}}$. Il existe r permutations $\sigma_1,\,\ldots\,,\sigma_r$ appartenant respectivement à $S_{\{1\}}$, $S_{\{s_2,\ldots,s_3-1\}}$, $\ldots$, $S_{\{s_r,\ldots,s_{r+1}-1\}}$ telles que $\sigma=\sigma_1\cdots\sigma_r$. Soit $k\in[\![1,n]\!]$ et considérons le polynôme $f_k(X_1,\ldots,X_k)$ de l'ensemble triangulaire S. Montrons que $\sigma.f_k(X_1,\ldots,X_k)\in I_f$.

Le cas $k=1$ est trivial car 1 est invariant sous l'action de σ. Si $k\in[\![2,n]\!]$, notons m l'entier de $[\![2,r]\!]$ tel que $f_k(X_1,\ldots,X_k)\in T_{g_m}(X_1)$. D'après la proposition 4.3.15, la permutation σ_m appartient au groupe de décomposition de l'idéal des relations symétriques J de g_m. Par suite, le polynôme $\sigma.f_k(X_1,\ldots,X_k)=\sigma_m.f_k(X_1,\ldots,X_k)$ appartient à J. L'inclusion $J\subset I_f$ montre que $\sigma.f_k(X_1,\ldots,X_k)$ appartient à I_f.

Ainsi, pour tout $k \in [\![1, n]\!]$, $\sigma.f_k(X_1, \ldots, X_k) \in I_f$. L'idéal I_f étant engendré par les n polynômes $\{f_1, f_2, \ldots, f_n\}$, ceci implique que $\forall g \in I_f$, $\sigma.g \in I_f$. D'où l'inclusion.

Pour montrer l'inclusion inverse, raisonnons par l'absurde.

Supposons qu'il existe une permutation $\sigma \in \mathrm{Dec}(I_f)_{[1]}$ qui n'appartienne pas à $S_{\{1\}} \times S_{\{s_2,\ldots,s_3-1\}} \times \cdots \times S_{\{s_r,\ldots,s_{r+1}-1\}}$. Sous cette condition, l'un des ensembles

$$\{1\}, \{s_2, \ldots, s_3 - 1\}, \ \ldots \ , \{s_r, \ldots, s_{r+1} - 1\}$$

n'est pas invariant sous l'action de σ. Nous pouvons supposer, sans perte de généralité que σ transforme un entier $a_2 \in \{s_2, \ldots, s_3 - 1\}$ en un entier $a_3 \in \{s_3, \ldots, s_4 - 1\}$. L'inclusion (4.3.6) assure l'existence de deux permutations σ_2 et σ_3 de $\mathrm{Dec}(I_f)_{[1]}$ telles que $\sigma_2(s_2) = a_2$ et que $\sigma_3(s_3) = a_3$. De l'égalité $\sigma_3^{-1}\,\sigma\,\sigma_2(s_2) = s_3$, il vient $\sigma_3^{-1}\,\sigma\,\sigma_2.f_{s_2}(X_1, X_{s_2}) = f_{s_2}(X_1, X_{s_3}) \in I_f$, ainsi $f_{s_2}(\alpha_1, \alpha_3) = 0$. Les facteurs $g_2 = f_{s_2}$ et $g_3 = f_{s_3}$ de f sur $K(\alpha_1)[X]$ ont donc une racine commune et f une racine double. Ceci contredit l'hypothèse de séparabilité de f. □

Remarque 4.3.18. Dans le cas des idéaux de départ, le stabilisateur $\mathrm{Dec}(I_f)_{[1]}$ est donc a priori connu. Ainsi, pour adapter l'algorithme `SousGroupeConnu` au cas des idéaux de départ, il suffit :

1. d'initialiser la variable k à 1 dans la boucle **Tant que** de cette fonction, ce qui a pour effet de ne pas calculer $\mathrm{Dec}(I_f)_{[1]}$.
2. de passer comme argument à cette fonction l'ensemble fort de générateurs du stabilisateur $\mathrm{Dec}(I_f)_{[1]}$:

$$\begin{array}{ll} \{ & (s_2; s_2+1), (s_2+1; s_2+2), \ \ldots \ , (s_2+d_2-2; s_2+d_2-1), \\ & (s_3; s_3+1), (s_3+1; s_3+2), \ \ldots \ , (s_3+d_3-2; s_3+d_3-1), \\ & \vdots \\ & (s_r; s_r+1), (s_r+1; s_r+2), \ \ldots \ , (s_r+d_r-2; s_r+d_r-1) \quad \} \, . \end{array}$$

Parcours d'arbre dans le cas d'un idéal de rupture

L'idéal I de ce paragraphe étant un idéal de départ, la proposition 4.3.17 montre l'égalité

$$\mathrm{Dec}(I_f)_{[1]} = S_{\{1\}} \times S_{\{2,3\}} \times S_{\{3,4\}} \times S_{\{5,6\}} \times S_{\{7,8\}},$$

qui permet d'appliquer l'algorithme `SousGroupeConnu` du paragraphe 4.3.4. Ce dernier ne parcourant, de la branche supérieure de l'arbre 4.2, que le sous-arbre 4.3, le nombre de formes normales est de 36 pour cet algorithme.

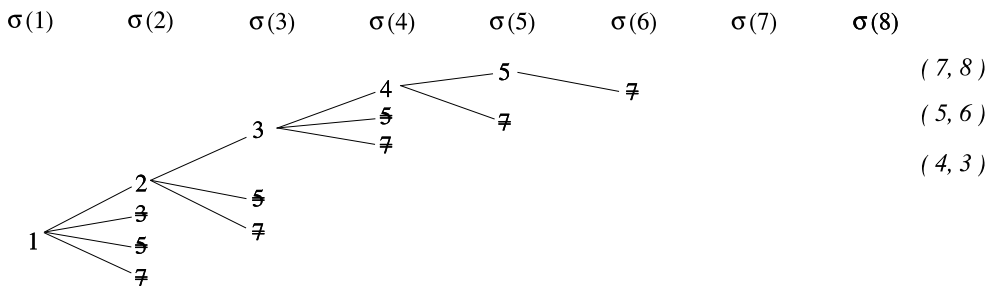


FIG. 4.3 – Branche supérieure parcourue par l'algorithme `SousGroupeConnu`

La remarque 4.3.18 permet d'éviter les calculs de la branche 4.2 et restreint ainsi à 27 le nombre de formes normales nécessaires au calcul d'un ensemble fort de générateurs de Dec(I).

4.4 Comparaison des algorithmes

Dans ce paragraphe, la nomenclature nT_i des sous-groupes transitifs de S_n est celle établie par Butler et McKay (Voir [16]).

Tous les algorithmes de ce chapitre ont été implantés dans le logiciel de calcul formel `Magma` (voir [11]) et nous noterons $f_{n,i}$ le polynôme de groupe de Galois nT_i figurant dans le package `galpol` de ce logiciel.

4.4.1 Algorithmes `STRONG_GENERATORS` et `Generateurs`

Le tableau comparatif 4.1 recense les temps de calcul des algorithmes `STRONG_GENERATORS` d'Anai, Noro et Yokoyama (voir [3]) et `Generateurs` (Algorithme 4.2.12). L'algorithme `STRONG_GENERATORS` ne s'appliquant qu'aux idéaux de relations, nous nous limitons à ce cas pour ce tableau.
Nous avons considéré, pour chacun des groupes transitifs nT_i, un idéal des relations $I_{n,i}$ du polynôme $f_{n,i}$ calculé par la méthode présentée au chapitre 5. Remarquons que, dans ce cas, le groupe de Galois nT_i du polynôme $f_{n,i}$ sur $\mathbb{Q}$ est, à isomorphisme près, le groupe de décomposition de l'idéal $I_{n,i}$. Pour chaque idéal $I_{n,i}$, nous comparons le temps de calcul nécessaire aux algorithmes `STRONG_GENERATORS` et `Generateurs` pour déterminer le groupe $Dec(I_{n,i})$.

Idéal I	$Card(Dec(I))$	`StrongGenerators`	`Generateurs`
$I_{8,10}$	16	0.04	0.01
$I_{8,17}$	32	0.15	1.9
$I_{8,26}$	64	709.6	1.65
$I_{8,35}$	128	55.6	0.129
$I_{9,28}$	648	3.17	0.169
$I_{8,47}$	1152	7.2	0.06
$I_{10,43}$	28 800	> 700	0.611
$I_{8,50}$	40 320	1.719	0.019
$I_{12,299}$	1 036 800	> 700	5.06

TAB. 4.1 – Algorithmes `StrongGenerators` et `Generateurs` .

(Implantation en Magma - AMD Duron 800 Mh - 256 Mo - Temps en s.)

Remarque 4.4.1. L'algorithme `STRONG_GENERATORS` exploite, pour le calcul du groupe de Galois, des propriétés liées à la tour d'extensions de corps :

$$\mathbb{Q}(\alpha_1) \subset \mathbb{Q}(\alpha_1, \alpha_2) \subset \cdots \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n),$$

où $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ est isomorphe à $\mathbb{Q}[X_1, \ldots, X_i]/\langle f_1, \ldots, f_i \rangle$ pour $i \in [\![1, n]\!]$. Ces propriétés ne sont pas utilisées par les algorithmes de ce chapitre.

4.4.2 Algorithmes `Generateurs` et `EFG`

Pour établir le tableau 4.2, deux types d'idéaux ont été utilisés :
- des idéaux de relations obtenus par la méthode décrite au chapitre 5, idéaux marqués d'une astérisque ;
- des idéaux de départ (Voir Paragraphe 4.3.4 ou Chapitre 5).

Pour chaque ligne, la première colonne indique que l'idéal $I_{n,i}$ a été obtenu à partir du polynôme $f_{n,i}$. La seconde colonne précise le cardinal du groupe de décomposition de l'idéal correspondant. Les quatre dernières colonnes indiquent le temps de calcul nécessaire à la détermination d'un ensemble fort de générateurs du groupe $\mathrm{Dec}(I_{n,i})$ respectivement par les algorithmes `Generateurs` (Algorithme 4.2.12), `EFG` (voir Paragraphe 4.3.2), `SousGroupeConnu` et par celui obtenu en effectuant la modification décrite dans la remarque 4.3.18.

Pour les deux dernières colonnes, lorsqu'aucun sous-groupe du groupe de décomposition n'a été utilisé ou que l'algorithme n'est pas applicable à l'idéal considéré le champ a été rempli d'un signe $-$.

Les cas où le cardinal du groupe de décomposition de l'idéal coïncide avec celui de la variété de l'idéal sont repérés par l'astérisque $*$. Lorsqu'un idéal vérifie cette condition, nous savons que le groupe de décomposition de l'idéal $I_{n,i}$ est aussi son stabilisateur. Ceci permet alors d'appliquer l'algorithme `GaloisIdeal` (voir [61]) à l'idéal $I_{n,i}$ qui, pour déterminer le groupe de Galois du polynôme ainsi qu'un idéal des relations de ce polynôme, nécessite de connaître un stabilisateur de l'idéal $I_{n,i}$.

Idéal	Card(Dec(I))	`Generateurs`	`EFG`	`SousGroupeConnu`	Remarque 4.3.18
$I^*_{8,9}$	16	63	56	–	–
$I^*_{8,10}$	16	65	58	–	–
$I^*_{8,11}$	16	57	50	–	–
$I^*_{8,15}$	32	72	60	–	–
$I^*_{8,17}$	32	47	38	–	–
$I^*_{8,26}$	64	66	56	–	–
$I^*_{8,29}$	64	64	54	–	–
$I^*_{8,35}$	128	61	50	–	–
$I_{10,21}$	480	82	57	27	21
$I_{9,8}$	96	82	54	31	25
$I_{12,22}$	2304	147	84	44	33
$I_{12,43}$	8640	129	80	32	25
$I_{13,4}$	13824	125	93	30	18
$I_{14,12}$	40320	152	104	44	32
$I_{14,26}$	181440	134	98	27	18
$I_{15,11}$	1935360	185	115	33	25

TAB. 4.2 – Comparaison des algorithmes de ce chapitre.

Dans le cas des idéaux du tableau ci-dessus, le nombre de formes normales nécessaires au calcul de Dec(I) est, avec l'algorithme `EFG`, de 10 % à 40 % plus faible qu'avec l'algorithme `Generateurs`. La comparaison des trois dernières colonnes montre que la connaissance plus ou moins précise d'un sous-groupe permet d'améliorer grandement le calcul du groupe de décomposition.

Remarque 4.4.2. Il est possible d'améliorer ces trois algorithmes en utilisant le calcul modulaire pour optimiser les tests d'appartenance à l'idéal I : si un polynôme R modulo un entier p n'appartient pas à I modulo p alors R n'appartient pas à I. Sur certains des exemples précédents, ce pré-test modulaire réduit jusqu'à un facteur 20 les temps de calcul et, en général, p égal à 2 ou 3 suffit.

Chapitre 5

Un algorithme mixte de calcul de corps de décomposition

Ce chapitre est consacré à l'étude d'une méthode mixte de calcul du corps de décomposition d'un polynôme f c'est dire de l'un de ses idéaux de relations. Cette méthode rend compatible les algorithmes de calcul d'un idéal de Galois maximal par factorisations successives et l'algorithme `GaloisIdeal` (voir [61]).

L'objectif de cette méthode est de compenser les faiblesses respectives de ce deux types d'algorithmes : lorsque l'ordre du groupe de Galois de f est élevé, les dernières étapes des algorithmes procédant par factorisations successives (voir [59], [36], [3] et [45]) peuvent s'avérer très coûteuses (et éventuellement infaisables) alors que, pour l'algorithme `GaloisIdeal`(voir Paragraphe 5.5.2 et [61]), ce sont les premières étapes qui sont les plus coûteuses.

La méthode mixte de ce chapitre procède en deux temps :

1. Factorisation de f sur un de ses corps de rupture K. Cette factorisation fournit un idéal de Galois de f appelé idéal de rupture de f et permet d'identifier un ensemble de groupes contenant des représentations symétriques du groupe de Galois de f (voir Chapitre 3).
2. Application de l'algorithme `GaloisIdeal` pour le calcul d'un idéal des relations de f.

À partir de la factorisation de f sur K, il est facile d'obtenir un idéal de rupture de f. La principale difficulté est d'obtenir la deuxième entrée nécessaire à l'algorithme `GaloisIdeal` : un injecteur de cet idéal (voir Définition 2.1.25). En effet, la factorisation de f sur K permet d'identifier un ensemble de classes de conjugaison de groupes dont certaines permettent le calcul d'un injecteur de l'idéal. Dans certains cas, il s'avère né-

cessaire de réduire le nombre de classe.
Avant d'appliquer l'algorithme `GaloisIdeal`, il nous sera parfois possible d'obtenir, sans calcul, un idéal de Galois contenant strictement l'idéal de rupture. La difficulté est encore d'identifier un injecteur de l'idéal obtenu.

Dans ce chapitre, nous nous restreignons à la factorisation de f sur l'un de ces corps de rupture tout en veillant à ce que les résultats soient assez généraux pour être applicables aux factorisations de f dans des extensions de degré supérieure. La construction d'un idéal de Galois à partir des facteurs irréductibles de f sur l'un de ses corps de rupture est l'objet du paragraphe 5.1. Nous y définissons les notions d'idéal de rupture et d'idéal induit. Les paragraphes 5.2 et 5.3 sont consacrés aux résultats permettant de calculer un injecteur d'un idéal de rupture. Notre algorithme de calcul de corps de décomposition est décrit au paragraphe 5.5. Au paragraphe 5.6, nous étudions le degré 8 qui offre un panel complet des situations possibles. Est exclu de cette étude, le cas des groupes 2-transitifs : ce cas s'inscrit dans une étude globale des extensions supérieures qui s'appuie sur les résultats de ce chapitre. Le paragraphe 5.7 est dédié à l'implantation et à l'expérimentation.

Les résultats de ce chapitre ont été obtenus en collaboration avec G. Renault et A. Valibouze. Il s'agit d'une version simplifiée et plus algébrique des résultats de [46].

Dans toute la suite de ce chapitre,
– k est corps infini et $\bar{k}$ une clôture algébrique de k ;
– f est un polynôme irréductible univarié à coefficient dans k ;
– $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \bar{k}^n$ désignera un n-uplet de n racines distinctes de f.

5.1 Idéal de rupture et idéal induit

Dans ce paragraphe, nous allons construire un idéal de Galois de f à partir des facteurs irréductibles de f sur son corps de rupture $k(\alpha_1)[x]$. Il s'agit de l'idéal induit (voir Définition 5.1.2) de l'idéal de rupture de f (voir Définition 5.1.6). Au corollaire 5.1.12, nous verrons qu'un ensemble de générateurs de cet idéal est facile à obtenir.

Supposons que f possède trois facteurs dans $k(\alpha_1)[x]$:

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

Notons m le degré en la variable x de g et p celui de h. Ordonnons le n-uplet $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ des racines de f dans $\bar{k}^n$ de telle sorte que $\alpha_2, \ldots, \alpha_{m+1}$ soient les racines de g et $\alpha_{m+2}, \ldots, \alpha_n$ soient celles de h.

Notons $T_g(\alpha_1)$ (respectivement, $T_h(\alpha_1)$) l'ensemble triangulaire formé par les modules de Cauchy de g dans $k(\alpha_1)[x_2, \ldots, x_{m+1}]$ (respectivement, de h dans $k(\alpha_1)[x_{m+2}, \ldots, x_n]$) (voir Définition 2.2.4).

Dans $k(\alpha_1)[x_1, \ldots, x_n]$, l'idéal I_r engendré par l'ensemble triangulaire de polynômes

$$\{x_1 - \alpha_1, T_g(\alpha_1), T_h(\alpha_1)\}$$

est l'idéal de Galois de f sur le corps $k(\alpha_1)$ s'annulant en $\underline{\alpha}$. L'injecteur de cet idéal relativement à $\underline{\alpha}$ est $S_{1,m,p}$. En effet, le cardinal $m!p!$ de $S_{1,m,p}$ est égal au cardinal de la variété de I_r et $S_{1,m,p}$ est naturellement inclus dans le groupe de décomposition de I_r. Ceci montre que le groupe $\mathrm{Dec}(I_r) = S_{1,m,p}$ est l'unique injecteur de I_r dans les idéaux maximaux qui le contiennent (voir Égalité (2.4.7) et Proposition 2.4.12).

Cette construction se généralise naturellement à toute factorisation de f sur $k(\alpha_1)[x]$: notons $f_2, \ldots, f_r$ les facteurs de rupture de f sur $k(\alpha_1)[x]$ (voir Définition 3.2.1). Pour tout $i \in [\![1, n]\!]$, notons $T_{f_i}(\alpha_1)$ l'ensemble triangulaire formé par les modules de Cauchy du facteur f_i dans l'anneau de polynômes adéquat. Rappelons que $\Delta(f)$ est la suite des degrés des facteurs de rupture $f_2, \ldots, f_r$.

Notations 5.1.1. Soit $V \subset \overline{k}^n$. Nous noterons $Id_k(V)$ l'idéal de $k[x_1, \ldots, x_n]$ s'annulant sur V.

Définition 5.1.2. 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.

L'idéal de rupture I_r est engendré dans $k(\alpha_1)[x_1,\ldots,x_n]$ par l'ensemble triangulaire :

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

Exemple 5.1.3. 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 :

$$\begin{aligned}
T_1(\alpha_1) &= \{\ x_3^2-\alpha_1^6+\alpha_1^4+\alpha_1^2-1,\\
&\qquad x_4+x_3\}\text{ dans } k(\alpha_1)[x_3,x_4]\text{ et}\\
T_2(\alpha_1) &= \{\ x_5^4+(\alpha_1^6-\alpha_1^4)x_5^2-1,\\
&\qquad x_6^3+x_5^3+x_5^2x_6+x_5x_6^2+(\alpha_1^6-\alpha_1^4)x_5+(\alpha_1^6-\alpha_1^4)x_6,\\
&\qquad x_7^2+x_5^2+x_5x_6+x_5x_7+x_6^2+x_6x_7+\alpha_1^6-\alpha_1^4,\\
&\qquad x_8+x_7+x_6+x_5\}\text{ dans } k(\alpha_1)[x_5,x_6,x_7,x_8]\,.
\end{aligned}$$

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 5.1.4. 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 5.1.5. Dans toute la suite de ce chapitre, $\underline{\alpha}$ sera un élément de $V(I_1)$ et I_1 désignera un idéal de $k(\alpha_1)[x_1,\ldots,x_n]$ vérifiant :

$$I_r\subset I_1\subset Id_{k(\alpha_1)}(\underline{\alpha}) \tag{5.1.1}$$

L'idéal I_1 est un idéal de Galois de f (voir Définition 2.4.1). Nous supposons que I_1 possède son groupe de décomposition L pour injecteur. D'après la proposition 2.4.18, 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 (5.1.1) s'étendent à $\underline{\beta}$:

$$I_r \subset I_1 \subset Id_{k(\beta_1)}(\underline{\beta})\,. \tag{5.1.2}$$

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 2.4.4) :

Définition 5.1.6. 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 5.1.7. Nous noterons $\mathcal{M}(I)$ l'ensemble des idéaux maximaux de $k[x_1, \ldots, x_n]$ contenant I.

Proposition 5.1.8. *Pour tout $\mathcal{M} \in \mathcal{M}(I)$, nous avons*

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

Ceci s'écrit encore :

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

Démonstration. Les égalités

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

prouvent la proposition. □

Proposition 5.1.9. *Tout $\mathcal{M} \in \mathcal{M}(I)$ vérifie :*
(1) $\mathrm{Dec}(\mathcal{M})_{\{1\}} \subset L \subset S_{1,\Delta(f)}$ *;*
(2) $Orb(\mathrm{Dec}(\mathcal{M})_{\{1\}}) = Orb(L) = Orb(S_{1,\Delta(f)})$ *.*

Démonstration. Nous pouvons supposer que $\mathcal{M} = Id_k(\underline{\alpha})$; i.e. $Dec(\mathcal{M}) = Gal_k(\underline{\alpha})$. Nous obtenons les inclusions inverses des injecteurs (relatifs à $\underline{\alpha}$) des idéaux de (5.1.2) :

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

Des identités $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})_{\{1\}}$ et $Orb(\mathrm{Gal}_k(\underline{\beta})_{\{1\}}) = Orb(S_{1,\Delta(f)})$ (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 :

Proposition 5.1.10. *Soit $\mathcal{M} \in \mathcal{M}(I)$ et soient $\tau_1, \ldots, \tau_n$, des permutations du groupe $Dec(\mathcal{M})$ 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 2.4.11) 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 définition, W est la variété de l'idéal de Galois $Id_k(V)$ (voir Propositon 2.4.11). Ainsi,

$$\mathrm{Id}_k(W) = \mathrm{Id}_k(V) = I_1 \cap k[x_1, \ldots, x_n]$$

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 5.3.2, 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.

□

Notations 5.1.11. Pour tout anneau $\mathcal{A}$ et toute partie non vide E de $\mathcal{A}$, nous noterons $\langle E \rangle_{\mathcal{A}}$ l'idéal engendré par E dans $\mathcal{A}$.

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

Corollaire 5.1.12. *Posons $F_1 = f$ et $\mathcal{A} = k(\alpha_1)[x_1, \ldots, x_n]$. L'idéal I induit de l'idéal $I_1 = \langle x_1 - \alpha_1, F_2, F_3, \ldots, F_n\rangle_{\mathcal{A}}$ 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 5.1.10, 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 $\mathcal{S}$. □

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

Dans ce paragraphe, sont présentés les résultats techniques portant uniquement sur les ensembles de permutations.
Nous utiliserons ces résultats au paragraphe 5.3 pour le calcul d'un injecteur d'un idéal I induit de I_1 lorsque le groupe de décomposition de I ne constitue pas l'unique injecteur de I (voir Proposition 2.4.12). L'ensemble L sera alors l'injecteur $\mathrm{Inj}(I_1, \underline{\alpha})$, l'ensemble $\mathcal{A}(L)$ défini ci-après contiendra l'ensemble des groupes de Galois des éléments de $V(I)$ et l'application Ψ permettra le calcul de l'injecteur de I à partir du groupe de Galois de tout élément de $V(I)$.

5.2.1 Ensemble $\mathcal{A}(L)$ et application Ψ

Considérons un sous-groupe L de $S_{1,n-1}$ (i.e. tel que $\forall \sigma \in L,\ \sigma(1) = 1$).

Définition 5.2.1. Nous appellerons *groupe admissible* tout sous-groupe transitif H de S_n vérifiant $H_{\{1\}} \subset L$ et tel que $Orb(L) = Orb(H_{\{1\}})$. L'ensemble des groupes admissibles sera noté $\mathcal{A}(L)$.

Remarque 5.2.2. Notons $1, e$ la suite croissante des cardinaux des éléments de $Orb(L)$. 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 5.2.3. *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, pour tout $i \in [\![1, n]\!]$, σ_i appartient à L, nous avons $\sigma_i \in H_{\{1\}}\sigma'_1 + \cdots + H_{\{1\}}\sigma'_s$, 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 5.2.4. 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 5.2.5. *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 5.2.6. *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 5.2.7. 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 5.2.8. *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 5.2.5. 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 5.2.5 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 : $G = \sigma_i^{-1}h^{-1}H\,h\,\sigma_i = \sigma_i^{-1}\,H\,\sigma_i$. □

5.2.2 Classes de L-conjugaison

Au paragraphe 5.3, nous serons amenés à rechercher l'ensemble des groupes $H \in \mathcal{A}(L)$ permettant le calcul d'un injecteur d'un idéal de Galois I induit de I_1. Ces groupes se répartissent en différentes classes dites de L-conjugaison. Nous verrons au Théorème 5.3.4 que si un groupe de l'une de ces classes permet le calcul d'un injecteur I alors il en est de même de tout autre groupe de cette classe ; c'est en particulier le cas des groupes de Galois des éléments de $V(I)$ qui ne forment qu'une seule classe de L-conjugaison.

Proposition 5.2.9. *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 :

$$\begin{aligned} (G^\sigma)_{\{1\}} &= (G_{\{\sigma^{-1}(1)\}})^\sigma \text{ et} && (5.2.1)\\ Orb(G^\sigma) &= \sigma.Orb(G)\ . && (5.2.2) \end{aligned}$$

Il s'en suit les égalités successives suivantes :

$$\begin{aligned} Orb((H^\sigma)_{\{1\}}) &= Orb((H_{\{1\}})^\sigma), \text{ d'après l'égalité (5.2.1) et puisque } \sigma(1)=1,\\ &= \sigma.Orb(H_{\{1\}}), \text{ d'après l'égalité (5.2.2)},\\ &= \sigma.Orb(L), \text{ car } H \in \mathcal{A}(L),\\ &= Orb(L), \text{ car } \sigma \in L\ . \end{aligned}$$

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

Nous poursuivons notre étude par celle de $L = S_{1,e} \subset S_n$, avec $e = (e_1, \ldots, e_r) \in \mathbb{N}^r$, un r-uplet d'entiers croissants de somme $n-1$.

Nous rappelons que la suite d'orbites $Orb(S_{1,e}) = (O_0 = (1), O_1, \ldots, O_r)$ est ordonnée par cardinalité croissante (i.e. $\mathrm{Card}(O_i) = e_i$ pour $i = 1, \ldots, r$).

Notations 5.2.10. Dans toute la suite, nous noterons M le sous-groupe de S_n défini par :

$$M = \{\sigma \in S_n \,|\, \sigma(1) = 1 \text{ et } Orb(S_{1,e}) = \sigma.Orb(S_{1,e})\}\ .$$

D'après l'identité (5.2.2), 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 sur $Orb(S_{1,e})$ en laissant fixe une orbite (par les permutations de $S_{1,e}$) ou en l'envoyant sur une autre orbite de même cardinal. Le groupe $S_{1,e}$ est le noyau du morphisme surjectif :

$$\begin{array}{rccl} \phi: & M & \longrightarrow & \mathrm{Fix}_{S_r}(e)\\ & \sigma & \mapsto & \tau : \tau(i) = j \text{ si } \sigma.O_i = O_j \text{ pour } i = 1, \ldots, r\ . \end{array}$$

Le cardinal N du stabilisateur $\mathrm{Fix}_{S_r}(e)$ de e dans S_r est aussi l'ordre du groupe $M/S_{1,e}$. Nous 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 5.2.11. *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 (5.2.1)) :

$$(H^\sigma)_{\{1\}} = (H_{\{\sigma^{-1}(1)\}})^\sigma = (H_{\{1\}})^\sigma \subset S_{1,e}^\sigma = S_{1,e}$$

et d'autre part (voir (5.2.2)) :

$$Orb(H^\sigma) = \sigma.Orb(H) = \sigma.Orb(S_{1,e}) = Orb(S_{1,e}) \ .$$

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, $Orb(S_{1,e}) = \sigma.Orb(S_{1,e})$ puisque $Orb(H^\sigma) = Orb(S_{1,e})$ et que $Orb(H) = Orb(S_{1,e})$. D'où $\sigma \in M$. □

Lemme 5.2.12. *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) $m \leq N$.

Démonstration. Pour montrer (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 (2), considérons une classe. Elle est celle d'un groupe H^σ où $\sigma \in M$ (voir Lemme 5.2.11) ; 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. □

5.3 Calcul des injecteurs d'un idéal induit

Dans ce paragraphe, l'idéal I_1 est celui du paragraphe 5.1 (voir Notation 5.1.5) et I est l'idéal induit de I_1 (voir Définition 5.1.6). D'après la proposition 5.1.9, l'injecteur L de I_1 vérifie $L \subset S_{1,\Delta(f)}$.

Nous cherchons à déterminer les injecteurs de I dans les idéaux de $\mathcal{M}(I)$.

5.3.1 Formulation des injecteurs de l'idéal induit

Le résultat principal de ce paragraphe est le théorème 5.3.4. Ce résultat exprime tout injecteur d'un idéal induit en fonction de certaines représentations symétriques du

groupe de Galois de f.

Dans tout ce paragraphe, K désigne une extension algébrique de k.

Notations 5.3.1. Le groupe de Galois $\mathrm{Gal}_K(\underline{\alpha})$ est isomorphe au groupe des K-automorphismes de $K(\underline{\alpha})$ par l'application qui à tout élément τ de $\mathrm{Gal}_k(\underline{\alpha})$ associe $\overline{\tau}$ dans $Aut_K(K(\underline{\alpha}))$ défini par $\overline{\tau}(\alpha_i) = \alpha_{\tau(i)}$. 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.

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 $g(x_{\tau(1)}, \ldots, x_{\tau(n)})$.

Lemme 5.3.2. *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 :*

$$\mathrm{Inj}(\overline{\tau}(J), \underline{\alpha}) \;=\; \tau\,\mathrm{Inj}(J, \underline{\alpha})\ . \tag{5.3.1}$$

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

$$\overline{\tau}(Id_{k(\underline{\alpha})}(V)) \;=\; Id_{k(\underline{\alpha})}(\tau.V)\ . \tag{5.3.2}$$

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 :

$$\mathrm{Inj}(\overline{\tau}(J), Id_{k(\underline{\alpha})}(\underline{\alpha})) \;=\; \mathrm{Inj}(J, \overline{\tau}^{-1}(\mathrm{Id}_{k(\underline{\alpha})}(\underline{\alpha}))\ . \tag{5.3.3}$$

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 le résultat. Pour terminer, les égalités successives suivantes prouvent l'identité (5.3.1) :

$$\begin{aligned}\mathrm{Inj}(\overline{\tau}(J), Id_{k(\underline{\alpha})}(\underline{\alpha})) &= \mathrm{Inj}(J, \overline{\tau}^{-1}(Id_{k(\underline{\alpha})}(\underline{\alpha}))), \text{ d'après l'identité (5.3.3) ,}\\ &= \mathrm{Inj}(J, Id_{k(\underline{\alpha})}(\tau^{-1}.\underline{\alpha})), \text{ d'après l'identité (5.3.2),}\\ &= \tau\,\mathrm{Inj}(J, Id_{k(\underline{\alpha})}(\underline{\alpha})), \text{ d'après la proposition 2.4.9.}\end{aligned}$$

□

Dans ce chapitre, tous les idéaux considérés seront triangulaires ou bien par construction ou bien par la proposition 2.4.18. Nous supposerons donc, à partir de maintenant, que I est engendré par l'ensemble triangulaire séparable

$$T = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}.$$

Proposition 5.3.3. *Pour tout $\mathcal{M} \in \mathcal{M}(I)$, le groupe de Galois $Dec(\mathcal{M})$ appartient à $\mathcal{A}(L)$ et*

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

où Ψ est l'application définie dans la notation 5.2.4.

Démonstration. Le groupe $Dec(\mathcal{M})$ appartient à $\mathcal{A}(L)$ d'après la propositon 5.1.9. D'après la proposition 5.1.8, 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 $Dec(\mathcal{M})$ telles que, pour tout $i \in [\![1, n]\!]$, $\tau_i(1) = i$. D'après la proposition 5.1.10, 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 :

$$\begin{aligned}\mathrm{Inj}(I, \underline{\alpha}) &= \mathrm{Inj}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I, \underline{\alpha}), \text{ d'après l'égalité (2.4.3),}\\ &= \sum_{i=1}^{n} \mathrm{Inj}(\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha}), \text{ d'après l'égalité (2.4.9),}\\ &= \sum_{i=1}^{n} \tau_i\ \mathrm{Inj}((k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha}), \text{ d'après le lemme 5.3.2,}\\ &= \sum_{i=1}^{n} \tau_i\,\mathrm{Inj}(I_1, \underline{\alpha}), \text{ d'après la remarque 2.4.6,}\\ &= \Psi(Dec(\mathcal{M})),\end{aligned}$$

où la dernière égalité est obtenue en appliquant l'assertion (1) de la proposition 5.2.5 à $L = \mathrm{Inj}(I_1, \underline{\alpha})$. □

Théorème 5.3.4. *Soit $H \in \mathcal{A}(L)$ et $\mathcal{M} \in \mathcal{M}(I)$ tels que $H \cap Dec(\mathcal{M})$ 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 5.1.8 et 5.3.3, l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent est formé des $\mathrm{Inj}(I, \sigma.\mathcal{M}) = \Psi(Dec(\sigma.\mathcal{M}))$ où σ parcourt L. Soit $\sigma \in L$. Comme $H \cap Dec(\mathcal{M})$ est transitif, le groupe $H^\sigma \cap Dec(\mathcal{M})^\sigma = H^\sigma \cap Dec(\sigma.\mathcal{M})$ est aussi transitif. Selon l'assertion (2) de la proposition 5.2.5 appliquée au groupe $G = Dec(\sigma.\mathcal{M})$, nous avons donc $\Psi(H^\sigma) = \Psi(G)$. □

Corollaire 5.3.5. *Reprenons les hypothèses du théorème 5.3.4 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 5.2.6 et du théorème 5.3.4. □

5.3.2 Classes de L-conjugaison associées aux idéaux induits

Si un groupe H vérifiant les hypothèses du théorème 5.3.4 est connu, il est alors possible de calculer un injecteur de I. Il n'est pas toujours immédiat de tester si $H \cap Dec(\mathcal{M})$ est transitif pour un idéal $\mathcal{M} \in \mathcal{M}(I)$; et ce d'autant plus lorsqu'au moins deux des facteurs de rupture de f sont de même degré. Ce paragraphe est consacré aux tests assurant la transitivité du groupe $H \cap Dec(\mathcal{M})$.

Définition 5.3.6. 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 $H \cap Dec(\mathcal{M})$ soit transitif (i.e. si H vérifie les hypothèses du théorème 5.3.4).

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 5.2.9) 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 5.3.4) et $\{\Psi(H') \mid H' \in \mathcal{C}\}$ est l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent (voir Théorème 5.3.4). Nous pouvons donc introduire la définition suivante :

Définition 5.3.7. 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.

Au paragraphe 5.2.2, nous avons étudié les classes de conjugaison par $S_{1,e}$ des conjugués H dans $\mathcal{A}(S_{1,e})$. Nous cherchons à savoir à quels idéaux induits des idéaux de rupture de f ces classes sont associées lorsque :
- $e = \Delta(f)$, la suite croissante des degrés des facteurs de rupture $f_1, \ldots, f_r$ (voir Chapitre 3), que
- H est associé à l'idéal de rupture I_r construit à partir de $f_1, \ldots, f_r$ (voir Paragraphe 5.1) et que
- I est l'idéal induit de I_r (i.e. $I = I_r \cap k[x_1, \ldots, x_n]$).

Rappelons que le groupe M est le normalisateur de $S_{1,e}$ dans $S_{1,n-1}$ et que $\tau_1, \ldots, \tau_N$ sont des représentants respectifs des N classes de $M/S_{1,e}$.

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 distintes (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 (voir Paragraphe 5.2.2), ces N listes sont les

$$(f_{\phi(\tau_i)(1)}, \ldots, f_{\phi(\tau_i)(r)}) \quad i = 1, \ldots, N$$

respectivement aux origines des constructions des N idéaux de rupture $\tau_i.I_r$, d'idéaux induits respectifs :

$$\tau_1.I, \tau_2.I, \ldots, \tau_N.I \ .$$

Remarque 5.3.8. Le groupe $S_{1,e}$ étant celui de décomposition de chaque idéal de rupture, par définition de $\tau_1, \ldots, \tau_N$, l'ensemble $\{\sigma.I \mid \sigma \in M\}$ est l'ensemble des idéaux induits des idéaux de rupture. Soit $\mathcal{M} \in \mathcal{M}(I)$. Nous avons $Dec(\mathcal{M}) \in \mathcal{A}(S_{1,e})$ (voir Proposition 5.1.9). Comme $\mathcal{M}(I) = \{\tau.\mathcal{M} \mid \tau \in S_{1,e}\}$ (voir Proposition 5.1.8) , 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 $Dec(\mathcal{M})^\sigma$ $(=Dec(\sigma.\mathcal{M}))$ où σ parcourt M ; c'est-à-dire l'ensemble des conjugués de $\mathrm{Gal}_k(f)$ (i.e. de $Dec(\mathcal{M})$) appartenant à $\mathcal{A}(S_{1,e})$ (voir Lemme 5.2.11).

Lemme 5.3.9. *Soit $\sigma \in M$. Si le groupe H est associé à l'idéal I alors le groupe H^σ est associé à l'idéal $\sigma.I$ induit de $\sigma.I_r$.*

Démonstration. Soit $\mathcal{M} \in \mathcal{M}(I)$ tel que $H \cap Dec(\mathcal{M})$ soit un sous-groupe transitif de S_n. Alors $H^\sigma \cap Dec(\sigma.\mathcal{M})$ est également transitif avec $\sigma.\mathcal{M} \in \mathcal{M}(\sigma.I)$ (i.e. l'idéal $\sigma.\mathcal{M}$ est un idéal maximal contenant $\sigma.I$). □

Les résultats précédents et ceux du paragraphe 5.2.2 permettent d'énoncer le théorème suivant :

Théorème 5.3.10. *Soit $H \in \mathcal{A}(S_{1,e})$ supposé être associé à l'idéal I induit de I_r. Alors :*
(1) à chaque idéal $\tau_i.I$ 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 $\sigma.I$ induit de l'idéal de rupture $\sigma.I_r$. Donc toute la classe de $S_{1,e}$-conjugaison de H^σ est associée à $\sigma.I$.

Une conséquence directe de ce théorème est le corollaire suivant utilisé pour les précalculs :

Corollaire 5.3.11. *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 I (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 I.*

Remarque 5.3.12. Supposons qu'on ait su déterminer un sous ensemble E de $\mathcal{T}(n)$ auquel appartient le groupe de Galois $\mathrm{Gal}_k(f)$. L'hypothèse du corollaire 5.3.11 est vérifiée lorsque tout groupe de E possède un conjugué dans $\mathcal{A}(S_{1,e})$ d'intersection transitive avec le groupe H.

Remarque 5.3.13. 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 5.2.11).

Considérons désormais L, injecteur d'un idéal I_1 vérifiant la suite d'inclusions (5.1.1). Soit I l'idéal induit de I_1. D'après la proposition 5.2.9, les groupes qui appartiennent à $\mathcal{A}(L)$ se répartissent en classes de L-conjugaison.

Corollaire 5.3.14. *Soit $H \in \mathcal{A}(L)$. 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 5.1.9), il existe $\sigma \in M$ tels que $G = H^\sigma$ (voir Lemme 5.2.11). L'idéal $\sigma.I_1$ contient l'idéal $\sigma.I_r$ qui est de rupture puisque $\sigma \in M$ (voir Remarque 5.3.8). En reprenant la démonstration du lemme 5.3.9, le groupe H^σ est bien associé à l'idéal $\sigma.I$ induit de $\sigma.I_1$. □

Remarque 5.3.15. Pour tout $\mathcal{M} \in \mathcal{M}(I)$, $Dec(\mathcal{M}) \in \mathcal{A}(L)$ (voir Proposition 5.1.9) est associé à 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 classe de L-conjugaison de M.

5.3.3 Association d'une classe de L-conjugaison à l'idéal induit

L'étude des liens entre les classes de $S_{1,e}$-conjugaison et les idéaux induits d'idéaux de rupture du paragraphe précédent ne résoud pas le problème de l'identification de la classe associée à I. Ce paragraphe est consacré à ce problème.

Dans ce paragraphe, I désignera un idéal induit d'un idéal de rupture I_r et $\mathfrak{C}$ l'ensemble des classes de L-conjugaison des groupes appartenant à $\mathcal{A}(L)$. Nous savons qu'au moins une de ces classes est associée à I (voir Remarque 5.3.15) et que cette classe permet le calcul des injecteurs de cet idéal. 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, conséquence du corollaire 6.2.2 du chapitre 6, permet toujours de déterminer un injecteur de I.

Proposition 5.3.16. *Un groupe H de $\mathcal{A}(L)$ est associé à I si et seulement s'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 Corollaire 6.2.2). Puisque $\mathrm{Card}(\Psi(H))$ est le cardinal de tout injecteur de I (voir Corollaire 5.2.6 et Corollaire 5.3.5), $\Psi(H)$ est égal à $\mathrm{Inj}(I, \underline{\beta})$. □

Remarque 5.3.17. Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux classes de $\mathfrak{C}$. D'après les propositions 5.2.5 et 5.2.8, 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 5.3.16 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 5.3.16 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 5.3.16 ne permet pas de préétablir des *critères d'association* entre les classes de $\mathfrak{C}$ et les idéaux induits ce qui sera souvent possible avec la proposition suivante :

Proposition 5.3.18. *Si $\mathcal{C} \in \mathfrak{C}$ est associée à l'idéal induit I, alors*

$$I = \bigcap_{H \in \mathcal{C}} H.I \quad \left(= \bigcap_{H \in \mathcal{C}} \{\sigma.R \ \mid \ \sigma \in H, \quad R \in I\} \right) \ .$$

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 5.3.4). 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 :

$$I = Id_k(\mathrm{Inj}(I, \underline{\alpha}).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k((H\sigma_i).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k(H^{\sigma_i^{-1}}.(\sigma_i.\underline{\alpha})) \ , \tag{5.3.4}$$

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 (5.3.4), nous avons $R \in Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$ et donc, par la proposition 5.4.1, il vient $H^\sigma.I \subset Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$. La décomposition (5.3.4) 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 5.6 fait apparaître, qu'en dehors du cas $\mathrm{Gal}_k(f)\{8T_6, 8T_8\}$, la proposition 5.3.18 est suffisante pour établir des critères d'association tels que ceux présentés dans l'exemple 5.3.19 qui suit.

Exemple 5.3.19. 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 5.3.10, il existe $i \in \{1,2,3\}$ tel que $I = \bigcap_{H \in \mathcal{C}_i} H.I$. La proposition 5.3.18 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 :
i) si $P_1 \in I$ alors la classe $\mathcal{C}_1$ est associée à I ;
ii) si $P_2 \in I$ alors la classe $\mathcal{C}_2$ est associée à I ;
iii) 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 $H_i = Dec(\mathcal{M}_i)$, $i = 1, 2$. 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 5.3.4).

Remarque 5.3.20. Nous constatons sur l'exemple ci-dessus que la proposition 5.3.18 est utilisable pour préétablir 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 5.3.18, mais il est parfois suffisant :

Proposition 5.3.21. *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 5.3.4, les injecteurs de I sont les $\Psi(H)$ où H parcourt la classe $\mathcal{C}$. La proposition 6.1.5 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 5.3.22. La recherche d'un polynôme $g \in I$ de la proposition 5.3.21 peut être restreinte à un ensemble de polynômes engendrant I.

5.4 Adjonction de relations à l'idéal induit

Considérons 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 une telle méthode.

Pour pouvoir appliquer l'algorithme `GaloisIdeal` à ce nouvel idéal, nous devons, comme pour I, connaître un de ses injecteurs.

Proposition 5.4.1. *(voir [61], 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.*

Proposition 5.4.2. *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 5.4.1, 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 2.4.1). □

Une conséquence immédiate de cette proposition est le corollaire suivant :

Corollaire 5.4.3. *Reprenons les notations de la proposition 5.4.2. Si $F = \sigma.R$ est de la forme $x_j^d + g(x_1, \ldots, x_{j-1})$ avec $d > 0$ 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 5.4.3, 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 5.4.4. *Reprenons les notations du corollaire 5.4.3 et supposons que :*
- *F soit de la forme $x_j^d + g(x_1, \ldots, x_{j-1})$, avec $d = \deg_{x_j}(Id_k(H.\underline{\alpha}))$;*
- *pour tout $i \in [\![1, j-1]\!]$, $\deg_{x_i}(I) = \deg_{x_i}(Id_k(H.\underline{\alpha}))$.*

Alors, J est un idéal de Galois de f et il est engendré par l'ensemble S.

Démonstration. D'après le corollaire 5.4.3, il suffit de montrer que $f_j \in \langle S \rangle$. D'après la proposition 5.4.2, nous avons la suite d'inclusions d'idéaux de $k[x_1, \ldots, x_j]$:

$$\langle f_1, \ldots, f_{j-1}, F \rangle \subset \langle f_1, \ldots, f_{j-1}, F, f_j \rangle \subset Id_k(H.\underline{\alpha}) \cap k[x_1, \ldots, x_j].$$

Or l'hypothèse faite sur les degrés initiaux des idéaux

$$Id_k(H.\underline{\alpha}) \cap k[x_1, \ldots, x_j] \text{ et } \langle f_1, \ldots, f_{j-1}, F \rangle$$

montre que ces idéaux sont égaux. Le corollaire s'en suit. □

Soit H un groupe associé à I et contenant $\mathrm{Gal}_k(\underline{\alpha})$, le corollaire 5.4.3 (ou le corollaire 5.4.4) permet d'en déduire un polynôme F et un idéal de Galois $J = I + \langle F \rangle$ de f. Connaissant un ensemble triangulaire de générateurs de J, nous pouvons calculer le cardinal de sa variété (voir Égalité (2.4.7)). Si $\mathrm{Card}(V(J)) = \mathrm{Card}(H)$ alors, d'après la proposition 2.4.12, $J = Id_k(H.\underline{\alpha})$ 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 5.4.5. *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 5.4.5 ; autrement dit, nous devons connaître E_1. La proposition suivante permet, dans certains cas, de calculer cet ensemble :

Proposition 5.4.6. *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 5.4.1 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 5.4

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 5.4.4. Soit

$$\Psi(H) = H\tau_1 + \ldots + H\tau_s \ ,$$

où $\tau_1, \ldots, \tau_r$ sont les permutations telles 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 5.4.6, nous avons $\{\tau_1, \ldots, \tau_r\} \subset E$ et donc :

$$\mathrm{Card}(V(J)) \geq \mathrm{Card}(E_1)\,\mathrm{Card}(H) \geq r\,\mathrm{Card}(H) \ .$$

Le cardinal de $V(J)$ étant connu, si $r\,\mathrm{Card}(H) = \mathrm{Card}(V(J))$ alors, d'après la proposition 5.4.6, nous avons $E_1 = \{\tau_1, \ldots, \tau_r\}$ et

$$\mathrm{Inj}(J, \underline{\alpha}) = \sum_{i=1}^{r} H\tau_i \ .$$

Exemple 5.4.7. 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 de rupture en degré 8 (voir Chapitre 3), 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 de relations de f.

5.5 Construction d'un algorithme

5.5.1 Méthologie de pré-calculs

Dans ce paragraphe, nous décrivons une méthologie à suivre pour établir les pré-calculs d'un algorithme de détermination des injecteurs de tout idéal induit (voir Définition 5.1.6). Cette méthodologie met en œuvre les résultats théoriques des paragraphes précédents.

Nous allons distinguer plusieurs étapes. La première n'intervient que dans le cadre où le polynôme f est factorisé sur l'un de ses corps de rupture. Ceci permet de déterminer les groupes susceptibles d'être injecteurs des idéaux de rupture. À l'aide de la table de rupture en degré n, est déterminé l'ensemble

$$\mathcal{G} = \{G \in \mathcal{T}(n) \ \mid \ \Delta(G) = 1, e\} \ .$$

Remarquons que le groupe $\mathrm{Gal}_k(f)$, qui est un représentant dans $\mathcal{T}(n)$ du groupe des k-automorphismes du corps de décomposition de f, appartient à l'ensemble $\mathcal{G}$.

À partir de la deuxième étape, nous désignerons par L un groupe qui, lors du calcul du corps de décomposition d'un polynôme f de degré n, est susceptible d'être l'injecteur d'un idéal de Galois I_1 de $k(\alpha_1)[x_1, \ldots, x_n]$. Notons $1, e$ la suite croissante des cardinaux des orbites de $\{1, \ldots, n\}$ sous l'action de L (i.e. des éléments de $Orb(L)$).

Les étapes 2 à 5 ont pour objet de prévoir, en fonction du groupe de Galois de f sur k, l'injecteur d'un idéal de Galois de f contenant l'idéal I induit de I_1 (cet idéal sera obtenu en appliquant les résultats du paragraphe 5.4 à I ou bien sera l'idéal I lui-même).

Remarque 5.5.1. L'idéal I_1 peut lui-même provenir d'un idéal induit d'un idéal de Galois I_2 de $k(\alpha_1, \alpha_2)[x_1, \ldots, x_n]$ contenant les polynômes $x_1 - \alpha_1$ et $x_2 - \alpha_2$. Si l'idéal induit de I_2 n'a pas un groupe pour injecteur, il est possible, avec l'algorithme `GaloisIdeal`, de calculer un idéal le contenant ayant cette propriété. Par ce biais, notre algorithme s'applique aussi aux polynômes de groupe de Galois 2-transitifs.

Pour décrire ces étapes, nous devons introduire les relations d'équivalence qui y seront utilisées.

Relations d'équivalence

Pour tout groupe $G \in \mathcal{G}$, nous notons $\mathcal{A}(L, G)$ l'ensemble des S_n-conjugués de G qui appartiennent à $\mathcal{A}(L)$:

$$\mathcal{A}(L, G) = \{G^\sigma \mid \sigma \in S_n\} \cap \mathcal{A}(L) \ .$$

(Pour la définition de $\mathcal{A}(L)$, voir Définition 5.2.1.) Nous avons naturellement :

$$\mathcal{A}(L) = \bigcup_{G \in \mathcal{G}} \mathcal{A}(L, G). \tag{5.5.1}$$

Relation $\sim$ sur l'ensemble $\mathcal{A}(L)$.
Nous noterons $\sim$ la relation d'équivalence induite par la L-conjugaison sur les ensembles $\mathcal{A}(L)$.
Soit $\mathcal{C} \in \mathcal{A}(L)/\sim$ et $H \in \mathcal{C}$. D'après le théorème 5.3.4, si $\Psi(H)$ est l'un des injecteurs de l'idéal I alors l'ensemble des injecteurs de I est égal à $\{\Psi(H') \mid H' \in \mathcal{C}\}$.

Relation $\mathcal{R}$ sur l'ensemble des classes de L-conjugaison $\mathcal{A}(L)/\sim$.
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux classes appartenant à $\mathcal{A}(L)/\sim$. Nous posons

$$\mathcal{C}\ \mathcal{R}\ \mathcal{C}' \text{ ssi } \{\Psi(H) \mid H \in \mathcal{C}\} = \{\Psi(H') \mid H' \in \mathcal{C}'\}.$$

Ainsi, si $\{\Psi(H) \mid H \in \mathcal{C}\}$ est l'ensemble des injecteurs de I alors il en est de même de l'ensemble $\{\Psi(H') \mid H' \in \mathcal{C}'\}$ pour toute classe $\mathcal{R}$-équivalente $\mathcal{C}'$ de $\mathcal{C}$.

Remarque 5.5.2. La proposition 5.2.5 montre que s'il existe $H \in \mathcal{C}$ et $H' \in \mathcal{C}'$ tels que $H \cap H'$ soit un sous-groupe transitif de S_n alors $\mathcal{C}\ \mathcal{R}\ \mathcal{C}'$.

Par ailleurs, la proposition 5.2.9 montre que s'il existe $H_0 \in \mathcal{C}$ et $H_0' \in \mathcal{C}'$ tel que $H_0 \cap H_0'$ soit un sous-groupe transitif de S_n alors, pour tout $H \in \mathcal{C}$, il existe $H' \in \mathcal{C}'$ tel que $H \cap H'$ soit un sous-groupe transitif de S_n.

Relation $\mathcal{R}$ pour les groupes de $\mathcal{G}$.
Soient G et G' deux groupes de $\mathcal{G}$. Nous posons

$$G\ \mathcal{R}\ G' \text{ s'il existe } \mathcal{C} \in \mathcal{A}(L,G)/\sim \text{ et } \mathcal{C}' \in \mathcal{A}(L,G')/\sim \text{ telles que } \mathcal{C}\ \mathcal{R}\ \mathcal{C}'.$$

En cours de calcul, certains groupes peuvent être retirés de l'ensemble $\mathcal{G}$ ou de $\mathcal{A}(L)$. De telles réductions de l'ensemble $\mathcal{A}(L)$ ne modifient pas la méthodologie que nous allons décrire.

Étape 1 : Utilisation des tables de rupture

Avec la table de rupture en degré n, nous déterminons l'ensemble E des entiers e tels que $1, e \in \{\Delta(G) \mid G \in \mathcal{T}(n)\}$. 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.

Étape 2 : Calcul de $\mathcal{A}(L)$ et des ensembles $\mathcal{A}(L,G)$

Avec l'un des systèmes GAP ou Magma, 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 (5.5.1).

Étape 3 : Détermination de la classe de $\mathrm{Gal}_k(f)$ dans $\mathcal{G}$

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 ce chapitre, 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 5.3.5, 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 $Dec(I) \in \mathcal{A}(L,G)$. Comme, dans ce cas particulier, pour tout $\mathcal{M} \in \mathcal{M}(I)$, $Dec(\mathcal{M}) \subset Dec(I)$ (voir Proposition 2.4.12) et $Dec(\mathcal{M}) \in \mathcal{A}(L)$ (voir Remarque 5.3.15), l'algorithme `GaloisIdeal` peut être utilisé avec pour paramètres I, son injecteur $Dec(I)$ et la liste des sous-groupes de $Dec(I)$ dans $\mathcal{A}(L)$.
2. Cas où $Dec(I) \notin \mathcal{A}(L,G)$. 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.

Exemple 5.5.3. En degré $n = 8$.

* Lorsque $e = 1^3, 4$, le critère de parité distingue la classe de T_7 de celles de T_9^+, T_{10}^+ et T_{11}^+.
* Lorsque $e = 1, 2^3$, le test du groupe de décomposition est utilisé.

Remarque 5.5.4. Cette étape est parfois simplifiable en faisant intervenir les étapes 4 et/ou 5. Par exemple, en appliquant les étapes 4 et 5 lorsque $n = 8$, $e = 1^3, 4$ et que $\mathrm{Gal}_k(f)$ est pair, il n'est pas nécessaire de distinguer les classes de T_9^+, T_{10}^+ et T_{11}^+. De manière générale, si nous avons su construire (voir Étape 5) un idéal J contenant strictement I alors le test du groupe de décomposition est utilisable si un groupe $G \in \mathcal{A}(G)$ vérifie $\mathrm{Card}(G) = \mathrm{Card}(V(J))$. Il suffit de tester si $Dec(J)$ appartient où non à $\mathcal{A}(L,G)$.

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 5.3.4).

4.2 L'hypothèse du Cas 4.1 n'est pas vérifiée. Soit $G \in C_0$. Les résultats du paragraphe 5.3.3 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).

Étape 5

Nous utilisons les résultats du paragraphe 5.4 (Corollaire 5.4.4 et Proposition 5.4.5) afin

de savoir s'il sera possible de calculer un idéal J contenant strictement I. Nous avons constaté que cette étape peut intervenir lors de l'étape 3, en passant éventuellement par l'étape 4. Cette étape peut aussi intervenir dans l'étape 4 dans les cas 4.1 et 4.2 (voir $n = 8$ avec $e = 1, 3^2$). Cette étape 5 intervient donc 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. A cet égard, le degré 8 illustrera parfaitement toutes les situations possibles.

5.5.2 Algorithme `GaloisIdeal`

Soit I un idéal de Galois de f donné par un ensemble triangulaire `T` de générateurs. Nous supposons déterminés un injecteur L de I et un ensemble $\mathfrak{A}$ de groupes auquel appartiennent les groupes de Galois $Dec(\mathcal{M})$, $\mathcal{M} \in \mathcal{M}(I)$ (dans le cadre de ce chapitre, $\mathfrak{A}$ est un sous-ensemble de $\mathcal{A}(L)$). L'algorithme

`GaloisIdeal(T,`L`,`$\mathfrak{A}$ `)`

calcule un idéal des relations $\mathcal{M}$ contenant I ainsi que le groupe de Galois $Dec(\mathcal{M})$ (cet algorithme décrit dans [61] nécessite que l'entrée L est un groupe ; sa généralisation à tout injecteur a été réalisée dans [62]). La méthode utilisée pour cet algorithme est celle évoquée dans l'introduction. Il s'agit de construire récursivement une chaîne ascendante d'idéaux de Galois

$$I = I_1 \subset I_2 \subset \cdots \subset I_r = \mathcal{M},$$

où, pour calculer I_{i+1} à partir de I_i (avec $i \in [\![1, r-1]\!]$), il est nécessaire de connaître un ensemble triangulaire engendrant I_i et un injecteur de I_i.

5.6 Étude en degré 8

Pour illustrer ce chapitre, 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 8-uplet 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 [1]).

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 Chapitre 3), nous appliquons la méthodologie prescrite au paragraphe 5.5 en examinant les différentes situations possibles en fonction de $\Delta(f)$.

5.6.1 $\Delta(f) = 1^7$; 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 $\mathcal{M}$ de relations du polynôme f ;

Exemple 5.6.1. 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

$$\begin{aligned}\mathcal{M} \;=\; \langle & f(x_1),\ x_2+x_1,\ x_3-x_1^3-3x_1,\\ & x_4+x_1^3+3x_1,\ x_5-x_1^5-5x_1^3-5x_1,\ x_6+x_1^5+5x_1^3+5x_1,\\ & x_7-x_1^7-7x_1^5-14x_1^3-7x_1,\ x_8+x_1^7+7x_1^5+14x_1^3+7x_1\rangle\ .\end{aligned}$$

5.6.2 $\Delta(f) = 1^3, 2^2$; 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 5.3.19 où est décrit un critère d'association (Etape 4). En utilisant le théorème 5.3.10, 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 corollaire 5.4.4 et la proposition 5.4.5 à $H = G_7$, nous obtenons la relation $r_7 = x_7 + g_3(x_5)$ de T' avec $Dec(\mathcal{M}) = G_7$ (Etape 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 5.3.19, pour chaque groupe $G \in \mathcal{G}^+$, nous obtenons le critère d'association suivant (Etape 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 $r_7 = \sigma.f_2 = x_7 + g_2(x_5)$ (Etape 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 $\mathcal{M} = \langle T' \rangle$.

5.6.3 $\Delta(f) = 1^3, 4$; 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 (Etape 4, Cas 4.1). Á 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 $Dec(\mathcal{M}) = G_{18}$.

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 $Dec(\mathcal{M}) = G_{17}$.

5.6.4 $\Delta(f) = 1, 2^3$; 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. $Dec(I)$ 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 `GaloisIdeal(`$\mathrm{Dec}(I)$`, `T_I`, [`H_{20}`])` ou `GaloisIdeal(`$\mathrm{Dec}(I)$`, `T_I`, [`H_{16}`])`, où H_{16} et H_{20} sont des sous-groupes de $\mathrm{Dec}(I)$ conjugués respectifs de T_{16} et T_{20}^+.

Cas B. $\mathrm{Dec}(I) = G_{31}$ (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 `GaloisIdeal(`G_{31}`,`T_I`,[`G_{21}`])` ou `GaloisIdeal(`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. $\mathrm{Dec}(I) \notin \mathcal{A}(L, T_{27})$ et $\mathrm{Dec}(I) \neq G_{31}$

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 de relations (voir Égalités (2.4.2) et (2.4.3)). 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

`GaloisIdeal(`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 5.3.4 et Proposition 5.4.6). La proposition 5.3.16 permet d'identifier le groupe de Galois en déterminant lequel des ensembles L_6 ou L_8 est un injecteur de J.

5.6.5 $\Delta(f) = 1, 2, 4$; 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 :

$$\texttt{GaloisIdeal}(G_{35}, T_J, [G_{29}, G_{19}, H_{19}]) \quad \text{et}$$
$$\texttt{GaloisIdeal}(G_{35}, T_J, [G_{26}, G_{28}, G_{30}, G_{15}, H_{15}]),$$

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, d'après les tables de ruptures en degré 8 (voir Annexe A), la parité de ce groupe de Galois détermine si $\mathrm{Gal}_k(f)$ est ou non T_{15}.

5.6.6 $\Delta(f) = 1, 3^2$; 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 5.4.4). 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

$$\texttt{GaloisIdeal}(G_{24}, T_J, [G_{13}, G_{14}]).$$

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 5.3.4, 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

$$\texttt{GaloisIdeal(}\ G_{12} + G_{12}(3,4)(6,7)\texttt{,}\ T_J\texttt{,}\ [G_{12}]\texttt{).}$$

Remarque 5.6.2. D'après les tables de rupture en degré 8, si le groupe de Galois d'un des facteurs de rupture de degré 3 est $3T_2$ (i.e. S_3) alors $\mathrm{Gal}_k(f) = T_{24}^+$.

5.6.7 $\Delta(f) = 1, 6$; 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 $x_2 + g_2(x_1)$. Á 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 l'un des appels :

- $\texttt{GaloisIdeal(}G_{44}\texttt{,}T_J\texttt{,[}G_{39}^+\texttt{,}\ G_{19}^+\texttt{])}$ ou
- $\texttt{GaloisIdeal(}G_{44}\texttt{,}T_J\texttt{,[}G_{40}, G_{38}, G_{23}\texttt{])}$.

5.6.8 $\Delta(f) = 3, 4$, $L = S_{1,3,4}$ 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 2.4.12, 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 l'appel

$$\texttt{GaloisIdeal(}G_{47}\texttt{,}T_I\texttt{,[}G_{45}^+, G_{42}^+, G_{41}^+, G_{34}^+, G_{33}^+\texttt{])}$$

ou l'appel $\texttt{GaloisIdeal(}G_{47}\texttt{,}T_I\texttt{,[}G_{46}\texttt{])}$.

5.7 Implantation et résultats expérimentaux

Nous appellerons `FEGI` (algorithme de Factorisation dans les Extensions puis algorithme `GaloisIdeal`) l'algorithme que nous proposons dans ce chapitre. Nous allons le comparer à celui de [3] 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 ...).

Nous avons rencontré un problème pour la factorisation de polynômes à coefficients dans un corps de nombres (d'après [58], ce problème sera corrigé dans une prochaine version du logiciel Magma). Nous avons donc implanté l'algorithme de factorisation donné dans [3], version améliorée de celui de Trager (voir [60]).

Pour nos comparaisons, nous avons utilisé des polynômes de la base de données de G. Malle et J. Kluners (voir [33]). 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 [27]. Remarquons que l'implantation de l'algorithme `FE` faite dans le logiciel RISA/ASIR [51] (interfacé avec PARI [49] 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	3732.05	0.21
$x^8 + 7x^7 - 10x^6 - 131x^5 - 200x^4 + 131x^3 + 382x^2 - 191$	$8T_{46}$	576	8400.61	519.29
$x^8 + x^7 - 14x^6 - 3x^5 + 62x^4 - 25x^3 - 63x^2 + 24x + 16$	$8T_{45}$	576	6040.89	179.55
$x^8 - x^5 - x^4 - x^3 + 1$	$8T_{44}$	384	66.35	0.19
$x^8 + x^4 - 4x^2 + 1$	$8T_{39}$	192	10.54	0.17
$x^8 + 2x^6 - 12x^4 - 3x^2 + 11$	$8T_{35}$	128	3.53	0.32
$x^8 + 12x^6 + 48x^4 + 72x^2 + 31$	$8T_{31}$	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
$x^8 + x^6 + 2x^2 + 4$	$8T_{19}$	32	0.63	0.82

TAB. 5.1 – Temps de calcul.

Les temps de calcul peuvent être améliorés en employant :
- l'algorithme de factorisation de van Hoeij (voir [63]) adapté aux polynômes à coefficients dans une tour d'extensions algébriques (une telle factorisation existe dans le système PARI version 2.2.5 dans le cas où les coefficients appartiennent à une extension simple de $\mathbb{Q}$ (voir [49]))
- et des méthodes p-adiques pour l'algorithme `FEGI` (voir [65]).

5.8 Conclusion

Comme le montre le tableau 5.1, notre méthode de calcul d'un corps de décomposition s'avère comparativement d'autant plus efficace que son degré sur le corps de base est élevé. Lorsque le groupe de Galois est connu, cette méthode peut être éventuellement améliorée en utilisant des méthodes d'interpolation pour rechercher les relations de degré 1 (voir [43]).
Nous avons supposé tout au long de ce chapitre que le polynôme f est irréductible sur k, mais notre méthode est généralisable aux polynômes réductibles en l'appliquant à chacun de ses facteurs et en utilisant les résultats de l'article [47].

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 5.1. Elle pourra donc, en particulier, être appliquée à certains polynômes de groupe de Galois 2-transitif.

Chapitre 6

Permutations et calcul d'idéaux de Galois

Introduction

Dans [61] et dans le chapitre 5, un corps de décomposition d'un polynôme est obtenu par le calcul d'une chaîne croissante d'idéaux de Galois de dernier terme un idéal des relations. Pour chaque idéal construit, un ensemble de permutations, un injecteur de cet idéal (voir Définition 2.1.25), doit être connu. Pour déterminer un idéal de Galois I', à partir d'un polynôme f ou d'un idéal de Galois I de ce polynôme, trois méthodes sont utilisées :

i) calculs de résolvantes pour obtenir une nouvelle relation entre les racines de f, puis calcul de l'idéal engendré par cette relation et par un ensemble de générateurs de I ;

ii) construction d'un idéal de rupture I' (voir Définition 5.1.2) à partir des facteurs irréductibles de f sur l'un de ces corps de rupture ;

iii) substitution de polynômes dans un ensemble de générateurs de I.

Lorsque la méthode ii) est appliquée, un injecteur de I' n'est pas nécessairement connu mais seulement des ensembles de permutations dont l'un est un injecteur de I'.

Dans la méthode iii), un injecteur de l'idéal I' n'est pas connu lorsqu'il diffère du groupe de décomposition de I'. (L'algorithme `IsPurGaloisIdeal` du Chapitre 4 permet de tester si le groupe de décomposition de I' est l'injecteur de l'idéal).

Dans ce chapitre, nous caractérisons les permutations d'un injecteur de I' : ceci assure la détermination de l'un des injecteurs de tout idéal obtenu par la méthode ii).

Si le groupe de décomposition d'un idéal de Galois I ne coïncide pas avec son groupe de décomposition, nous montrons qu'il est toujours possible, à partir de I et de l'un de

ces injecteurs, de calculer un idéal de Galois I' contenant strictement I tel que l'injecteur de I' soit son groupe de décomposition. De plus, avant tout calcul d'une base de Gröbner de I', le théorème 6.2.1 montre que :

– I' est un idéal triangulaire ;

– l'injecteur et les monômes initiaux de I' se calculent uniquement à partir de L.

Ce théorème s'applique, en particulier, à tout idéal obtenu par la méthode iii).

Dans le paragraphe 6.1, sont rappelés les résultats et les notions utilisés. Le paragraphe 6.2 est consacré aux résultats principaux de ce chapitre. L'application de ces résultats aux idéaux de rupture est l'objet du paragraphe 6.3 : le corollaire 6.2.2 de ce chapitre est utilisé pour la détermination d'un injecteur d'un idéal de Galois et le théorème 6.2.1 pour l'obtention d'une base de Gröbner et de l'injecteur d'un idéal de Galois.

Notations

Dans toute la suite de ce chapitre, nous utiliserons les notations suivantes :
- S_n est le groupe symétrique de degré n ;
- $K[x_1, \ldots, x_n]$ est l'anneau des polynômes à coefficient dans le corps K en les n variables algébriquement indépendantes $x_1, \ldots, x_n$. Nous munirons cet anneau de l'ordre lexicographique induit par les inégalités $x_1 < \cdots < x_n$;
- pour tout ensemble non vide $\mathcal{E}$ de $K[x_1, \ldots, x_n]$, l'idéal engendré par $\mathcal{E}$ est noté $\mathrm{Id}(\mathcal{E})$.

Conformément aux notations du chapitre 2, le groupe symétrique S_n agit naturellement sur l'anneau $K[x_1, \ldots, x_n]$: pour tout $\sigma \in S_n$ et tout $g \in K[x_1, \ldots, x_n]$, le polynôme $\sigma.g$ est défini par :

$$\sigma.g(x_1, \ldots, x_n) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \ .$$

Pour tout $P \subset S_n$ et tout $\mathcal{E} \subset K[x_1, \ldots, x_n]$, l'ensemble $P.\mathcal{E}$ est défini par :

$$P.\mathcal{E} = \{\, \pi \,.\, g \mid \pi \in P,\ g \in K[x_1, \ldots, x_n] \,\} \ .$$

Pour tout $P_1 \subset S_n$ et tout $P_2 \subset S_n$, nous noterons $P_1\, P_2$ l'ensemble des permutations :

$$P_1\, P_2 = \{\, \pi_1\, \pi_2 \mid \pi_1 \in P_1,\ \pi_2 \in P_2 \,\} \ .$$

6.1 Galois ideals

6.1.1 Galois ideals and injectors

From now on, f denotes an irreducible polynomial of degree n and $\underline{\alpha}$ a tuple $(\alpha_1, \ldots, \alpha_n)$ of the roots of f in an algebraic closure of K.

Definition 6.1.1. A $\underline{\alpha}$-*Galois ideal* I is a radical proper ideal of $K[x_1, \ldots, x_n]$ such that the variety of I, $V(I)$, is included in $S_n.\underline{\alpha}$.

In particular, the $\underline{\alpha}$-Galois ideal defined by

$$\mathcal{M}_{\underline{\alpha}} = \{R \in K[x_1, x_2, \ldots, x_n] \mid \ R(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\},$$

is a maximal ideal of $K[x_1, \ldots, x_n]$ called $\underline{\alpha}$-*relations ideal.*

Any splitting field K of the polynomial f is isomorphic to the quotient ring :

$$K[x_1, x_2, \ldots, x_n]/\mathcal{M}_{\underline{\alpha}}.$$

Definition 6.1.2. Let I and I' be two ideals of $K[x_1, x_2, \ldots, x_n]$, *the injector of* I *in* I' is the set of permutations defined by :

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

We call *injector of* I any injector of I in one of the maximal ideals containing I.

The next proposition shows that injectors of an Galois ideal is uniquely determined by its algebraic variety $V(I)$.

Proposition 6.1.3. *Let I be a $\underline{\alpha}$-Galois ideal and $L = \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}})$. We have :*

$$V(I) = L.\underline{\alpha}. \tag{6.1.1}$$

The set of injectors of the Galois ideal I is $\{l^{-1} L \subset S_n \mid l \in L\}$.

Proof. The first assertion comes from [61]. Equality (6.1.1) implies that the set of maximal ideals containing I is $\{\mathcal{M}_{l.\underline{\alpha}} \mid l \in L\}$. The equality $\mathrm{Inj}(I, \mathcal{M}_{l.\underline{\alpha}}) = l^{-1}\ \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}}) = l^{-1} L$ shows then the second assertion.

Remark 6.1.4. As the polynomial f is supposed irreducible, the group S_n acts faithfully on the set $S_n.\alpha$. Thus, there is a one-to-one map between L and the variety $V(I)$.

6.1.2 Decomposition group and injectors

Definition 6.1.5. The decomposition group $\mathrm{Dec}(I)$ of I is the stabilizer of I for the natural action of S_n on $K[x_1, \ldots, x_n]$:

$$\mathrm{Dec}(I) = \mathrm{Inj}(I, I) .$$

In particular, the *Galois group of $\underline{\alpha}$ on K*, denoted by $\mathrm{Gal}_K(\underline{\alpha})$, is the decomposition group of the ideal $\mathcal{M}_{\underline{\alpha}}$. This group is isomorphic to the Galois group of K-automorphisms of any splitting field of f.

The computation of the decomposition group of a triangular ideal can be realized by the algorithm `DecompositionGroup` of [1]. Injectors and decomposition group of a Galois ideal are linked by the following proposition.

Proposition 6.1.6. *The decomposition group $\mathrm{Dec}(I)$ of a Galois ideal I is the intersection of all injectors of I.*
In particular, if L is an injector of I, we have :

$$\mathrm{Dec}(I) = \bigcap_{l \in L} l^{-1} L. \tag{6.1.2}$$

Proof. By definition of the decomposition group, we have :

$$\begin{aligned} \mathrm{Dec}(I) &= \{\sigma \in S_n \,|\, \sigma.I \subset \cap_{l \in L} \mathcal{M}_{l.\underline{\alpha}}\} \\ &= \cap_{l \in L} \{\sigma \in S_n \,|\, \sigma.I \subset \mathcal{M}_{l.\underline{\alpha}}\} \\ &= \cap_{l \in L} \mathrm{Inj}(I, \mathcal{M}_{l.\underline{\alpha}}) . \end{aligned}$$

The first assertion follows. Equality (6.1.2) is a direct consequence of Proposition 6.1.3.

The next proposition can be seen as a consequence of Corollary 3.12 of [61] or as a direct application of Proposition 6.1.3 and Equality (6.1.2).

Proposition 6.1.7. *Let I be an $\underline{\alpha}$-ideal. The following assertions are equivalent :*
- *I admits an unique injector;*
- *$Dec(I) = \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}})$.*

Definition 6.1.8. A $\underline{\alpha}$-Galois ideal is said to be *pure* if I satisfies equivalent conditions of Proposition 6.1.7.

In the case of triangular ideals, the Algorithm `IsPureGaloisIdeal` of [1] can be used in order to test whether a Galois ideal is pure.

6.1.3 Equiprojectable parts of S_n

This section is about two results of [7]. These results use the notion of equiprojectability of a zero dimentional variety. In the case of an $\underline{\alpha}$-Galois ideal I, we have the one-to-one map between the variety $V(I)$ and the injector of I in the ideal $\mathcal{M}_{l.\underline{\alpha}}$ (See Equality (6.1.1)). Definition 6.1.9 expresses the notion of equiprojectability defined in [7] in terms of equiprojectable subsets of S_n.

Definition 6.1.9. Let $\sigma \in S_n$ and $k \in [\![1, n]\!]$. The *first k-part of σ* is the finite sequence $[\sigma(1), \ldots, \sigma(k)]$.

A subset L of S_n is said *equiprojectable* if, for all $k \in [\![1, n]\!]$ and all permutations $\sigma \in L$, the cardinal c of the set of all permutations of L which admits $[\sigma(1), \ldots, \sigma(k)]$ as first k-part depends only on k :

$$\#\left(\{\tau \in L \mid \forall i \in [\![1, k]\!],\ \sigma^{-1}\tau(i) = i\}\right) = c\,.$$

Notations 6.1.10. For all $p \in K[x_1, x_2, \ldots, x_n]$, let $init(p)$ be the leading monomial of p for the induced order on $K[x_1, x_2, \ldots, x_n]$ by $x_1 < \cdots < x_n$.

Definition 6.1.11. An ideal I is said *triangular* if I is separable and generated by triangular set of generators $\mathcal{G} = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ with, for all $i \in [\![1, n]\!]$, $init(f_i) = x_i^{di}$ where $d_i > 0$.

As the list $[d_1, \ldots d_n]$ does not depend on triangular set of generators, it makes sense to set the following definition.

The list $[d_1, \ldots d_n]$ is called the *list of the initial degrees* of I.

The following theorem is a direct reformulation of Theorems 4.5 and 5.3 of [7] applied to the Galois ideal I of injector $L = \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}})$.

Theoreme 6.1.1. *Let L be an injector of a triangular Galois ideal I. The following conditions are equivalent :*

– *a triangular set* $\mathcal{G} = \{f_1, f_2, \ldots, f_n\}$ *generates* I *;*
– L *is equiprojectable.*

Moreover, the degree of each polynomial f_i *relatively to the variable* x_i *satisfies the equality :*

$$\deg_{x_i}(f_i) = \mathrm{Card}(L_{i-1})/\,\mathrm{Card}(L_i).$$

When L *is a subgroup of* S_n*, the conditions below are true.*

By definition of a pure Galois ideal, we have :

Corollary 6.1.12. *Any pure Galois ideal is triangular.*

Theorem 6.1.1 gives an effective condition on an injector of a Galois ideal I to test whether I is triangular and, if this condition is satisfied, this theorem enables the computation, only from this injector, of the initial monomials of a triangular set generating I.

6.2 Ideals $\mathrm{Id}(P.I)$ where $P \subset S_n$

Throughout this section, I denotes an $\underline{\alpha}$-Galois ideal and $L = \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}})$ the injector of I in the $\underline{\alpha}$-relations ideal $\mathcal{M}_{\underline{\alpha}}$. Note that, under these conditions, L contains the permutation Id_{S_n}.

6.2.1 Subset $P \subset S_n$ such that $\mathrm{Id}(P.I)$ is a Galois ideal

Proposition 6.2.1. *Let's consider a non empty set* $\mathcal{E}$ *of* $K[x_1, \ldots, x_n]$*. The following conditions are equivalent :*

1. $\mathrm{Id}(\mathcal{E} \cup I)$ *is an* $\underline{\alpha}$*-Galois ideal.*
2. *There exists* $l \in L$ *such that* $\mathcal{E} \subset \mathcal{M}_{l.\underline{\alpha}}$*.*

Proof. By Seidenberg's lemma (See [8], Lemma 8.13), the condition (1) of the proposition is equivalent to $\mathrm{Id}(\mathcal{E} \cup I) \neq K[x_1, \ldots, x_n]$.

If the ideal $\mathrm{Id}(\mathcal{E} \cup I)$ is a proper ideal of $K[x_1, \ldots, x_n]$ then $\mathrm{Id}(\mathcal{E} \cup I)$ is contained in a maximal ideal $\mathcal{M}$. As $\mathcal{M}$ contains I, Proposition 6.1.3 implies that $\mathcal{M} = \mathcal{M}_{l.\underline{\alpha}}$ where $l \in L$. The inclusion $\mathcal{E} \subset \mathcal{M}_{l.\underline{\alpha}}$ follows.

The reciprocal is obvious.

The next corollary is a new tool to determine an injector of the Galois ideal I (see Example 6.3.1) and can also be used to determine an injector of any ideal $\mathrm{Id}\,(P.I)$ where P is a non-empty part of an injector of I containing Id_{s_n}.

Corollary 6.2.2. *Let* P *be a non-empty subset of* S_n *containing the permutation* Id_{s_n}*. The two following conditions are equivalent :*

1. $\mathrm{Id}\,(P.I)$ *is an* $\underline{\alpha}$*-Galois ideal;*
2. *an injector of* I *contains* P.

Moreover, if the above conditions are satisfied, the injector of I *in* $\mathcal{M}_{\underline{\alpha}}$ *is :*

$$\mathrm{Inj}(\mathrm{Id}(P.I), \mathcal{M}_{\underline{\alpha}}) = \{\sigma \in S_n \mid \sigma.P \subset L\}\ .$$

Proof. The first assertion is a direct consequence of Proposition 6.2.1. If the ideal $\mathrm{Id}(P.I)$ is an $\underline{\alpha}$-Galois ideal then the second assertion comes from the successive equalities :

$$\begin{aligned}\mathrm{Inj}(\mathrm{Id}(P.I), \mathcal{M}_{\underline{\alpha}}) &= \{\sigma \in S_n \mid \sigma.\,\mathrm{Id}(P.I) \subset \mathcal{M}_{\underline{\alpha}}\}\\ &= \{\sigma \in S_n \mid (\sigma\, P).I \subset \mathcal{M}_{\underline{\alpha}}\}\\ &= \{\sigma \in S_n \mid \sigma.P \subset L\}\,.\end{aligned}$$

6.2.2 The ideal $\mathrm{Id}(L.I)$

The Galois ideal $\mathrm{Id}(L.I)$ is studied in Section 6.2.2. Theorem 6.2.1 shows that this ideal is a pure Galois ideal which injector and initial monomials can be known before any computation by Theorem 2.4.17.

Definition 6.2.3. Let L be a subset of S_n. The *injector of* L, denoted by $\mathrm{Inj}(L)$, is the group defined by :

$$\mathrm{Inj}(L) = \{\sigma \in S_n \mid \sigma L = L\} = \bigcap_{\sigma \in L} L.\sigma^{-1}\ . \tag{6.2.1}$$

Remark 6.2.4. A comparison between Equalities 6.2.1 and 6.1.2 shows that the decomposition group of I can be written as the injector of L^{-1} :

$$\mathrm{Dec}(I) = \mathrm{Inj}(L^{-1})\ .$$

The computation of groups $\mathrm{Dec}(I)$ and $\mathrm{Inj}(L)$ can be computed, from the injector L, by a unique algorithm of backtrack search (see [15]).

Theoreme 6.2.1. *The ideal* $\mathrm{Id}(L.I)$ *is a pure Galois ideal an its injector is the group* $\mathrm{Inj}(L)$.

Moreover, if $L = \mathrm{Inj}(L)\ \mathrm{Dec}(I)$ *then the ideal* $\mathrm{Id}(L.I)$ *is the smallest pure* $\underline{\alpha}$*-Galois ideal containing* I *and* $\mathrm{Inj}(L)$ *is the greater group included in* L *containing* $\mathrm{Gal}_K(\underline{\alpha})$.

Proof. By Corollary 6.2.2, $\mathrm{Id}(L.I)$ is a Galois ideal. As $L = \mathrm{Inj}(I, \mathcal{M}_{\underline{\alpha}})$, the $\mathrm{Id}(L.I)$ is included in $\mathcal{M}_{\underline{\alpha}}$ and is then an $\underline{\alpha}$-Galois ideal. The injector $\mathrm{Inj}(\mathrm{Id}(L.I), \mathcal{M}_{\underline{\alpha}})$ can be written :

$$\begin{aligned}\mathrm{Inj}(\mathrm{Id}(L.I), \mathcal{M}_{\underline{\alpha}}) &= \{\sigma \in S_n \mid \sigma L.I \subset \mathcal{M}_{\underline{\alpha}}\}\\ &= \{\sigma \in S_n \mid \sigma L \subset L\},\ \text{by definition of } L,\\ &= \mathrm{Inj}(L),\ \text{by definition of } \mathrm{Inj}(L).\end{aligned}$$

Let J be a pure $\underline{\alpha}$-Galois ideal containing I and let's denote by H the injector of J in $\mathcal{M}_{\underline{\alpha}}$. We have $I \subseteq J \subseteq \mathcal{M}_{\underline{\alpha}}$ and it follows $L \supseteq H \supseteq \mathrm{Inj}(L)$. Equalities $L = L\ \mathrm{Dec}(I)$ and $L = \mathrm{Inj}(L)\ \mathrm{Dec}(I)$ shows $L = H\ \mathrm{Dec}(I)$, then $H\,L = L$. The group H is therefore a subgroup of $\mathrm{Inj}(L)$. This shows the inclusion $\mathrm{Id}(L.I) \subseteq J$.

The injector $\mathrm{Inj}(L)$ of $\mathrm{Id}(L.I)$ being a group, Theorem 2.4.17 shows that the ideal $\mathrm{Id}(L.I)$ is triangular and that initial monomials of a triangular set of generators of $\mathrm{Id}(L.I)$ can be uniquely computed from $\mathrm{Inj}(L)$ and thus from L.

Proposition 6.2.5. *A decomposition of the Galois ideal I into pure Galois ideals is :*

$$I = \bigcap_{\tau \in T} \tau\,.\,\mathrm{Id}(L.I)\ , \tag{6.2.2}$$

where T is a subset of L such that $L = \sum_{\tau \in T} \mathrm{Inj}(L)\,\tau$.

Proof. One can easily shows that such a subset T of L exists from the equality $\mathrm{Inj}(L)\,L = L$. The proposition is then a straighforward consequence of equality $\mathrm{Id}(\mathrm{Inj}(L)\,\tau\,.\underline{\alpha}) = \tau\,.\,\mathrm{Id}(\mathrm{Inj}(L)\,.\underline{\alpha})$ verified for all $\tau \in S_n$.

Note that ideals of this decomposition are triangular and relatively prime.

6.3 Applications to stem ideals

In this section, we apply results of Section 6.2 to Galois ideals called stem ideals defined in [46].

In sections 6.3.1 and 6.3.2 below, the nomenclature nT_i of transitive subgroups of S_n is the one of Greg Butler and John McKay (See [16]). The list, denoted $\mathcal{T}_n$, of transitive subgroups of S_n is available up to degree 22 in the Computer Algebra System Magma (See [11]).

Let's consider an irreducible polynomial f of degree n on a perfect field K. As the factorization of a polynomial f on the stem field $K[x]/f(x)$ depends on the Galois group of f, from the list of irreducible factors of f on this stem field, the authors of [46] deduce :

- a triangular set generating a Galois ideal I called stem ideal ;
- a list of transitive subgroups of S_n containing the Galois group of any element of the variety $V(I)$.

For any element of the variety $V(I)$, Theorem 6.9 of [46] shows that the injector of I in the relation ideal $\mathcal{M}_{\underline{\alpha}}$ is given by

$$L = \mathrm{Gal}_K(\underline{\alpha})\ \mathrm{Dec}(I)\,. \tag{6.3.1}$$

6.3.1 Determination of an injector

From the list of the possible Galois group, a list of permutations sets containing all injectors of I can be then computed by using Equality (6.3.1). If this list is not reduced to an injector of I, Corollary 6.2.2 ensures that the determination of an injector of I can always be determined by elimination. The following example illustrates this situation.

Example 6.3.1. Let's consider the case C. of the Section 10.1.4 of [46]. The authors compute a stem ideal from a polynomial f with Galois group $8T_6$ or $8T_8$.

The decomposition group of any stem ideal is the direct product of symmetric groups $S_{\{1\}} \times S_{\{2\}} \times S_{\{3,4\}} \times S_{\{5,6\}} \times S_{\{7,8\}}$. Using results of [46], a stem ideal I of f can be determined with, as injector, one of the two sets L_6 and L_8 :

- $L_6 = G_6$ Dec(I) where G_6 is the S_8-conjugate of $8T_6$ generated by the permutations $(1,7,5,3,2,4,6,8)$ and $(1,8)(2,3)(4,5)(6,7)$;
- $L_8 = G_8$ Dec(I) where G_8 is the S_8-conjugate of $8T_8$ generated by the permutations $(1,8,5,7,2,4,6,3)$ and $(3,4)(5,6)(7,8)$.

Let's consider a permutation $\sigma \in L_6 \setminus L_8$ (respectively, $\sigma \in L_8 \setminus L_6$). By Corollary 6.2.2, the injector of I is L_6 (respectively, L_8) if and only if the ideal Id$(I \cup \sigma.I)$ is a proper ideal of $K[x_1, \ldots, x_n]$.

Hence, we can determine an injector of I.

6.3.2 Computation of a pure Galois ideal from a stem ideal

In this section, Theorem 6.2.1 is applied to stem ideal to obtain a triangular set of generators of the pure Galois ideal Id$(L.I)$.

Any stem ideal satisfies the equality $L =$ Inj(L) Dec(I) of Theorem 6.2.1 (see Corollary 3.12 of [61] and definition of Inj(L)). Therefore, the group Inj(L) can be searched in the list of the transitive subgroups of S_n ordered by inclusion.

For any irreducible polynomial f, we denote by $\Delta(f)$ the list of the degrees of the irreducible factors of f on the stem field $K[x]/f(x)$. By construction, the leading monomial of each polynomial of a triangular set $\mathcal{G}$ generating a stem ideal is completely determined from $\Delta(f)$; therefore, some leading term of polynomials $\sigma.g$ for $\sigma \in L$ and $g \in \mathcal{G}$ are known before any computation. This can be used to determine if a triangular set of generators of Id$(L.I)$ is contained in the set $L.\mathcal{G}$. This method simplifies the one of [46] : results of [46] consist in determining conjugacy classes of transitive subgroups of S_n containing the Galois groups of elements of $V(I)$. In each of these classes, a group and a permutation of this group are searched in order to obtain, as we do here, polynomials of a triangular set generating the ideal Id$(L.I)$. The search of such permutations is made easier by the use of injectors of I as many groups can define the same injector.

In Table 6.1, in function of the list $\Delta(f)$ for a polynomial f of degree 9, are collected the following informations :

- the cardinal of the variety $V(I)$ of any stem ideal I of f ;
- the group $9T_i \in \mathcal{T}_9$ which is S_9-conjugate to the group $\mathrm{Inj}(L)$, where L denotes any injector of I ;
- the cardinal of the group $\mathrm{Inj}(L)$ which is also the cardinal of the variety of the pure Galois ideal $\mathrm{Id}(L.I)$;
- the last column indicates if the set of polynomials $L.\mathcal{G}$ contains a triangular set of generators of the ideal $\mathrm{Id}(L.I)$ (i.e. if a Gröbner basis computation is useless to obtain such a triangular set) ; remark that changing the injector considered is sometimes necessary to find such a triangular set.

In Table 6.1, when the degrees of the irreducible factors $\Delta(f)$ are sufficient to know that the stem ideal is a pure Galois ideal, the corresponding line has been omitted (in such a case, Theorem 6.2.1 is useless). Note that, in the particular case of degree 9, the stem ideal of a polynomial is not pure if and only if $\Delta(f)$ appears in the first column of this table.

$\Delta(f)$	$\mathrm{Card}(V(I))$	$\mathrm{Inj}(L)$	$\mathrm{Card}(V(\mathrm{Id}(L.I)))$	Does $L.\mathcal{G}$ contains a Gröbner basis of $\mathrm{Id}(L.I)$?
$1^3,\ 2^3$	72	$9T_4$	18	yes
$1^3,\ 3^2$	81	$9T_{17}$	27	yes
$1^3,\ 6$	6480	$9T_{20}$	162	yes
$1,\ 2^4$	144	$9T_3$	18	yes
$1,\ 2^4$	144	$9T_5$	18	no
$1,\ 2^2,\ 4$	864	$9T_8$	36	no
$1,\ 2,\ 6$	12960	$9T_{31}$	1296	yes
$1,\ 4^2$	5184	$9T_{16}$	72	no

TAB. 6.1 – Application to stem ideals of degree 9

This table shows that, when a stem ideal of degree 9 is not pure, a triangular set generating the pure Galois ideal $\mathrm{Id}(L.I)$ may be found without Gröbner basis computation.

6.4 Conclusion

The study in Section 6.2 of ideals $\mathrm{Id}(P.I)$ where I is a Galois ideal and P a non-empty subset of an injector L of I,

- gives a caracterisation of subsets of an injector of a Galois ideal, see Corollary 6.2.2, which can be used as a new mean to determine an injector of a Galois ideal (see

Section 6.3.1) ;
– shows that the ideal $\mathrm{Id}(L.I)$ is a pure Galois ideal which injector is computable uniquely from L, see Theorem 6.2.1. The knowleddge of this injector can then be exploited for the computation of a triangular set of generators of $\mathrm{Id}(L.I)$ as it can be used for determining the initial degrees of this ideal (see Section 6.3.2).

Chapitre 7

Relations entre les racines de polynômes réductibles

Nous nous intéressons dans ce chapitre au calcul d'un corps de décomposition d'un polynôme f supposé réductible et séparable (c'est à dire sans racine multiple) à coefficients dans un corps calculable K.

Conformément aux notations du chapitre 2, nous noterons $\bar{K}$ une clôture algébrique du corps K et $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \bar{K}^n$ un n-uplet des racines distinctes du polynôme f. Pour pouvoir calculer un corps de décomposition en appliquant l'algorithme mixte du chapitre 5 aux facteurs irréductibles de f sur $K(\alpha_1, \ldots, \alpha_i)$ $(i \geqslant 2)$ ou en exploitant la notion d'injecteur dans les algorithmes procédant par factorisations successives à l'aide des techniques du paragraphe 5.4 ou du chapitre 6, nous devons savoir construire un idéal de Galois d'un polynôme réductible à partir des idéaux de Galois de ses facteurs et d'injecteurs de ces idéaux. Le théorème 7.1.2 de ce chapitre apporte une solution à ce problème. Il s'agit d'une généralisation, à l'aide de la notion d'injecteur, d'un théorème établi par A. Colin pour les idéaux de relations (voir [18]).

Le paragraphe 7.1 présente le résultat principal de ce chapitre, le théorème 7.1.2, que nous illustrerons par des exemples au paragraphe 7.2.

Les résultats de ce chapitre, issus d'un travail collaboratif réalisé avec G. Renault et A. Valibouze, font l'objet de l'article [47].

Dans toute la suite de ce chapitre, nous conviendrons que la donnée d'un idéal de Galois consiste en celle d'une base de Gröbner et de l'un de ses injecteurs.

7.1 Idéaux de Galois de polynômes réductibles

Soient $\mathcal{A} = K[x_1, \ldots, x_n]$ et L une partie non vide de S_n. Notons I l'idéal de Galois $I = \mathrm{Id}_{\mathcal{A}}(L.\underline{\alpha})$ (voir Notation 2.4.20) et rappelons que la partie de S_n définie par

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

où $\sigma.I = \{R(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \mathcal{A} \mid R \in I\}$, est appelée l'*injecteur de I dans $M_{\underline{\alpha}}$* ou encore l'*injecteur de I relatif à $\underline{\alpha}$* et est notée $\mathrm{Inj}(I, \underline{\alpha})$.

Nous dirons que l'idéal I est l'*$\underline{\alpha}$-idéal de Galois d'injecteur* $\mathrm{Inj}(I, \underline{\alpha})$ *relatif à* $\underline{\alpha}$.

Supposons, dans cette partie, que le polynôme f se factorise sur K en deux polynômes g et h de degrés respectifs m et $p = n-m$. Ordonnons le n-uplet $\underline{\alpha}$ des racines de f de telle sorte que $\underline{\beta} = (\alpha_1, \ldots, \alpha_m)$ soit un m-uplet des racines de 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 la suite de ce chapitre, les bases de Gröbner considérées le seront toujours relativement à cet ordre.

Nous avons le résultat bien connu suivant :

Lemme 7.1.1. *$Gal_K(\underline{\alpha}) \subset Gal_K(\underline{\beta}) \times Gal_K(\underline{\gamma})$.*

Dans cette partie, nous allons démontrer le résultat plus général suivant :

Théorème 7.1.2. *Soient G une partie de S_m et H une partie de S_p. Si G (resp. H) est l'injecteur de l'idéal $\mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})$ (resp. $\mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})$) relativement à $\underline{\beta}$ (resp. $\underline{\gamma}$) alors l'$\underline{\alpha}$-idéal de Galois $\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$ possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$ et il vérifie :*

$$\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha}) \;=\; \mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})\,\mathcal{A} + \mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})\,\mathcal{A} . \tag{7.1.1}$$

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

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

Puisque G (resp. H) est l'injecteur de I_1 (resp. I_2) relatif à $\underline{\beta}$ (resp. $\underline{\gamma}$), nous avons, d'après l'égalité (2.4.1),

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

Donc $V(I_1\mathcal{A}) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}, u_1, \ldots, u_p) \mid \sigma \in G,\ u_i \in \bar{K}\}$ et $V(I_2\mathcal{A}) = \{(v_1, \ldots, v_m, \alpha_{\tau(m+1)}, \ldots, \alpha_{\tau(n)}) \mid \tau \in H,\ v_i \in \bar{K}\}$. Ainsi,

$$V(J) = V(I_1\mathcal{A} + I_2\mathcal{A}) = V(I_1\mathcal{A}) \cap V(I_2\mathcal{A}) = (G \times H).\underline{\alpha}\,. \tag{7.1.2}$$

Le radical de l'idéal J est donc l'idéal de Galois $\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$ qui, d'après les identités (2.4.2) et (7.1.2), possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$. Il reste donc à démontrer que l'idéal J, de dimension 0, est radical.
D'après le théorème 2.4.3, 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 :

$$\mathrm{Dim}(\mathcal{B}/I_1) = \mathrm{Card}(V(I_1)) = \mathrm{Card}(\{\underline{x}^{\underline{a}} \in \mathcal{B} \,|\, \underline{a} \notin \mathrm{In}(\mathcal{G}_1) + \mathbb{N}^m\})\,, \tag{7.1.3}$$

où $\underline{x}^{\underline{a}} = x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m}$ 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 (2.4.2), 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'aprés l'égalité (7.1.3), 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 :

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

À partir de cet idéal, pourra être construit l'idéal maximal $M_{\underline{\alpha}}$.

Définition 7.1.3. Un sous-ensemble T de $K[x_1, \ldots, x_n]$ est dit *triangulaire* si T est constitué de n polynômes $f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n)$ tels que le plus grand monôme de f_i pour l'ordre lexicographique soit de la forme $x_i^{d_i}$ où $d_i \in \mathbb{N}^*$.

Remarquons qu'un ensemble triangulaire de générateurs d'un idéal de $K[x_1, \ldots, x_n]$ constitue une base de Gröbner de cet idéal.

Remarque 7.1.4.

- Par induction, le théorème 7.1.2 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 7.1.2 généralise le résultat d'A. Colin qui établit l'identité (7.1.1) lorsque $G = \mathrm{Gal}_K(\underline{\beta})$, $H = \mathrm{Gal}_K(\underline{\gamma})$ et $G \times H = \mathrm{Gal}_K(\underline{\alpha})$ (voir [18]).

Nous présentons maintenant quelques exemples.

7.2 Exemples

Le lemme suivant est utilisé dans les exemples de ce paragraphe ; nous l'utilisons sans y faire référence.

Lemme 7.2.1. *Si g et h sont K-irréductibles alors les $Gal_K(\underline{\alpha})$-orbites de $\{1, \ldots, n\}$ sont $\{1, 2, \ldots, m\}$ et $\{m+1, m+2, \ldots, n\}$.*

Démonstration. Les racines $\alpha_1, \alpha_2, \ldots, \alpha_m$ du polynôme g sont les $\alpha_{\sigma(i)}$ où σ parcourt $\mathrm{Gal}_K(\underline{\alpha})$ puisque g est irréductible sur K. Donc $\{1, 2, \ldots, m\}$ est l'orbite de 1 sous l'action $\mathrm{Gal}_K(\underline{\alpha})$. De même $\{m+1, m+2, \ldots, n\}$ est l'orbite de $m+1$ sous l'action $\mathrm{Gal}_K(\underline{\alpha})$. □

Exemple 7.2.2. Posons $m = 5$ et $p = 2$.

Supposons que $\mathrm{Gal}_K(\underline{\beta})$ soit le groupe cyclique $C_5 = \langle (1, 3, 2, 4, 5) \rangle$ et que $\mathrm{Gal}_K(\underline{\gamma}) = S_2$. 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 $\mathrm{Gal}_K(\underline{\alpha}) = C_5 \times S_2$.

Exemple 7.2.3. Posons $m = 5$ et $p = 2$. Supposons que $\mathrm{Gal}_K(\underline{\beta})$ soit le groupe diédral $D_5 = \langle \sigma = (1, 5, 2, 3, 4), \tau = (1, 3)(2, 5) \rangle$ et que $\mathrm{Gal}_K(\underline{\gamma}) = S_2$. Le seul sous-groupe propre de $D_5 \times S_2$ qui ait 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 $D_5 \times S_2$ ou bien G_2.

Exemple 7.2.4. Ici $m = 5$ et $p = 2$. Soient les polynômes $\mathbb{Q}$-irréductibles $g = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ et $h = x^2 + 1$ et $f = g.h$. 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 $\mathrm{Id}_{\mathcal{B}}(\underline{\beta})$ des $\underline{\beta}$-relations d'injecteur le groupe cyclique $C_5 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\beta})$. L'ensemble $T_2 = \{x_6^2 + 1, x_7 + x_6\}$ engendre l'idéal $\mathrm{Id}_{\mathcal{C}}(\underline{\gamma})$ des $\underline{\gamma}$-relations d'injecteur le groupe symétrique $S_2 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\gamma})$. L'ensemble triangulaire T_1 se calcule rapidement en factorisant le polynôme g dans son corps de rupture de degré 5. D'après le théorème 7.1.2 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, d'après l'exemple 7.2.2, $C_5 \times S_2$ est le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$, l'idéal I est l'idéal des $\underline{\alpha}$-relations $\mathcal{M}$.

Exemple 7.2.5. Ici $m = 5$ et $p = 2$. Soient les polynômes $\mathbb{Q}$ irréductibles $g = x^5 - 2x^4 + 2x^3 - x^2 + 1$ et $h = x^2 + 1$ et $f = g.h$. Nous procédons de même que pour l'exemple précédent. L'ensemble triangulaire

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

engendre l'idéal I_1 des $\underline{\beta}$-relations d'injecteur le groupe diédral $D_5 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\beta})$ 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. D'après le théorème 7.1.2, l'idéal I engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois d'injecteur $D_5 \times S_2$.

Montrons comment, à partir de l'idéal I, l'algorithme `GaloisIdeal` calcule l'idéal des $\underline{\alpha}$-relations. Le groupe de Galois de $\underline{\alpha}$ sur $\mathbb{Q}$ est ou bien $G_1 = D_5 \times S_2$ ou bien son sous-groupe $G_2 = \langle \sigma, \tau(6,7) \rangle$ (voir Exemple 7.2.3). 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 $R = (x - \Theta(\underline{\alpha}))(x - \tau.\Theta(\underline{\alpha}))$ s'appelle une *résolvante G_1-relative de $\underline{\alpha}$ par 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 (ce résultat est ancien : par exemple, dans [57], l'auteur l'utilise pour déterminer le groupe de Galois) ; 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 [7]) :

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

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 $M_{\underline{\alpha}}$ est donc l'idéal I.

Annexe A

Tables de rupture

Table de rupture en degré 3

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^3]$	$(1T_1)^3$	$3T_1^{+*}$	$3!\,/\,2$	$[3,\ 1^2]$
$[2,\ 1]$	$1T_1,\ 2T_1$	$3T_2^{*}$	$3!$	$[3,\ 2,\ 1]$

G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture

Table de rupture en degré 4

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^4]$	$(1T_1)^4$	$4T_1^{*}$	4	$[4,\ 1^3]$
$[1^4]$	$(1T_1)^4$	$4T_2^{+*}$	4	$[4,\ 1^3]$
$[2,\ 1^2]$	$(1T_1)^2,\ 2T_1$	$4T_3^{*}$	8	$[4,\ 2,\ 1^2]$
$[3,\ 1]$	$1T_1,\ 3T_1^{+*}$	$4T_4^{+*}$	$4!\,/\,2$	$[4,\ 3,\ 1^2]$
$[3,\ 1]$	$1T_1,\ 3T_2^{*}$	$4T_5^{*}$	$4!$	$[4,\ 3,\ 2,\ 1]$

G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture

Table de rupture en degré 5

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^5]$	$(1T_1)^5$	$5T_1^{+*}$	5	$[5,\ 1^4]$
$[2^2,\ 1]$	$1T_1,\ (2T_1)^2$	$5T_2^{+*}$	10	$[5,\ 2,\ 1^3]$
$[4,\ 1]$	$1T_1,\ 4T_1^*$	$5T_3^*$	20	$[5,\ 4,\ 1^3]$
$[4,\ 1]$	$1T_1,\ 4T_4^{+*}$	$5T_4^+$	$5!\,/\,2$	$[5, \ldots, 3, 1^2]$
$[4,\ 1]$	$1T_1,\ 4T_5^*$	$5T_5$	$5!$	$[5, \ldots, 1]$
G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture				

Table de rupture en degré 6

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^6]$	$(1T_1)^6$	$6T_1^*$	6	$[6,\ 1^5]$
$[1^6]$	$(1T_1)^6$	$6T_2^*$	6	$[6,\ 1^5]$
$[3,\ 1^3]$	$(1T_1)^3,\ 3T_1^{+*}$	$6T_5^*$	18	$[6,\ 3,\ 1^4]$
$[2^2,\ 1^2]$	$(1T_1)^2,\ (2T_1)^2$	$6T_3^*$	12	$[6,\ 2,\ 1^4]$
$[2^2,\ 1^2]$	$(1T_1)^2,\ (2T_1)^2$	$6T_4^{+*}$	12	$[6,\ 2,\ 1^4]$
$[2^2,\ 1^2]$	$(1T_1)^2,\ (2T_1)^2$	$6T_6^*$	24	$[6,\ 2^2,\ 1^3]$
$[4,\ 1^2]$	$(1T_1)^2,\ 4T_1^*$	$6T_8^*$	24	$[6,\ 4,\ 1^4]$
$[4,\ 1^2]$	$(1T_1)^2,\ 4T_2^{+*}$	$6T_7^{+*}$	24	$[6,\ 4,\ 1^4]$
$[4,\ 1^2]$	$(1T_1)^2,\ 4T_3^*$	$6T_{11}^*$	48	$[6,\ 4,\ 2,\ 1^3]$
$[3,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 3T_2^*$	$6T_9^*$	36	$[6,\ 3,\ 2,\ 1^3]$
$[3,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 3T_2^*$	$6T_{10}^{+*}$	36	$[6,\ 3,\ 2,\ 1^3]$
$[3,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 3T_2^*$	$6T_{13}^*$	72	$[6,\ 3,\ 2^2,\ 1^2]$
$[5,\ 1]$	$1T_1,\ 5T_2^{+*}$	$6T_{12}^+$	60	$[6,\ 5,\ 2,\ 1^3]$
$[5,\ 1]$	$1T_1,\ 5T_3^*$	$6T_{14}$	120	$[6,\ 5,\ 4,\ 1^3]$
$[5,\ 1]$	$1T_1,\ 5T_4^+$	$6T_{15}^+$	$6!\,/\,2$	$[6, \ldots, 3, 1^2]$
$[5,\ 1]$	$1T_1,\ 5T_5$	$6T_{16}$	$6!$	$[6, \ldots, 1]$
G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture				

Table de rupture en degré 7

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^7]$	$(1T_1)^7$	$7T_1^{+*}$	7	$[7,\ 1^6]$
$[2^3,\ 1]$	$1T_1,\ (2T_1)^3$	$7T_2^*$	14	$[7,\ 2,\ 1^5]$
$[3^2,\ 1]$	$1T_1,\ (3T_1^{+*})^2$	$7T_3^{+*}$	21	$[7,\ 3,\ 1^5]$
$[6,\ 1]$	$1T_1,\ 6T_1^*$	$7T_4^*$	42	$[7,\ 6,\ 1^5]$
$[6,\ 1]$	$1T_1,\ 6T_7^{+*}$	$7T_5^+$	168	$[7,\ 6,\ 4,\ 1^4]$
$[6,\ 1]$	$1T_1,\ 6T_{15}^+$	$7T_6^+$	$7!\,/\,2$	$[7, \ldots, 3, 1^2]$
$[6,\ 1]$	$1T_1,\ 6T_{16}$	$7T_7$	$7!$	$[7, \ldots, 1]$
G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture				

Table de rupture en degré 8

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^8]$	$(1T_1)^8$	$8T_1^*$	8	$[8,\ 1^7]$
$[1^8]$	$(1T_1)^8$	$8T_2^{+*}$	8	$[8,\ 1^7]$
$[1^8]$	$(1T_1)^8$	$8T_3^{+*}$	8	$[8,\ 1^7]$
$[1^8]$	$(1T_1)^8$	$8T_4^{+*}$	8	$[8,\ 1^7]$
$[1^8]$	$(1T_1)^8$	$8T_5^{+*}$	8	$[8,\ 1^7]$
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_7^*$	16	$[8,\ 2,\ 1^6]$
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_9^{+*}$	16	$[8,\ 2,\ 1^6]$
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_{10}^{+*}$	16	$[8,\ 2,\ 1^6]$
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_{11}^{+*}$	16	$[8,\ 2,\ 1^6]$
$[4,\ 1^4]$	$(1T_1)^4,\ 4T_1^*$	$8T_{17}^*$	32	$[8,\ 4,\ 1^6]$
$[4,\ 1^4]$	$(1T_1)^4,\ 4T_2^{+*}$	$8T_{18}^{+*}$	32	$[8,\ 4,\ 1^6]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_6^*$	16	$[8,\ 2,\ 1^6]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_8^*$	16	$[8,\ 2,\ 1^6]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{16}^*$	32	$[8,\ 2^2,\ 1^5]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{20}^{+*}$	32	$[8,\ 2^2,\ 1^5]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{21}^*$	32	$[8,\ 2^2,\ 1^5]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{22}^{+*}$	32	$[8,\ 2^2,\ 1^5]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{27}^*$	64	$[8,\ 2^3,\ 1^4]$
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{31}^*$	64	$[8,\ 2^3,\ 1^4]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_1^*$	$8T_{19}^{+*}$	32	$[8,\ 2^2,\ 1^5]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_2^{+*}$	$8T_{15}^*$	32	$[8,\ 4,\ 1^6]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{26}^*$	64	$[8,\ 4,\ 2,\ 1^5]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{28}^*$	64	$[8,\ 4,\ 2,\ 1^5]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{29}^{+*}$	64	$[8,\ 4,\ 2,\ 1^5]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{30}^*$	64	$[8,\ 4,\ 2,\ 1^5]$
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{35}^*$	128	$[8,\ 4,\ 2^2,\ 1^4]$
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{12}^{+*}$	24	$[8,\ 3,\ 1^6]$
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{13}^{+*}$	24	$[8,\ 3,\ 1^6]$
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{14}^{+*}$	24	$[8,\ 3,\ 1^6]$
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_2^*)^2$	$8T_{24}^{+*}$	48	$[8,\ 3,\ 2,\ 1^5]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_2^*$	$8T_{23}^*$	48	$[8,\ 6,\ 1^6]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_4^{+*}$	$8T_{32}^{+*}$	96	$[8,\ 6,\ 2,\ 1^5]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_6^*$	$8T_{38}^*$	192	$[8,\ 6,\ 2^2,\ 1^4]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_7^{+*}$	$8T_{39}^{+*}$	192	$[8,\ 6,\ 4,\ 1^5]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_8^*$	$8T_{40}^*$	192	$[8,\ 6,\ 4,\ 1^5]$
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_{11}^*$	$8T_{44}^*$	384	$[8,\ 6,\ 4,\ 2,\ 1^4]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{33}^{+*}$	96	$[8,\ 4,\ 3,\ 1^5]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{34}^{+*}$	96	$[8,\ 4,\ 3,\ 1^5]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{42}^{+*}$	288	$[8,\ 4,\ 3^2,\ 1^4]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{41}^{+*}$	192	$[8,\ 4,\ 3,\ 2,\ 1^4]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{45}^{+*}$	576	$[8,\ 4,\ 3^2,\ 2,\ 1^3]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{46}^*$	576	$[8,\ 4,\ 3^2,\ 2,\ 1^3]$
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{47}^*$	1152	$[8,\ 4,\ 3^2,\ 2^2,\ 1^2]$
$[7,\ 1]$	$1T_1,\ 7T_1^{+*}$	$8T_{25}^{+*}$	56	$[8,\ 7,\ 1^6]$
$[7,\ 1]$	$1T_1,\ 7T_3^{+*}$	$8T_{36}^{+*}$	168	$[8,\ 7,\ 3,\ 1^5]$
$[7,\ 1]$	$1T_1,\ 7T_3^{+*}$	$8T_{37}^{+}$	168	$[8,\ 7,\ 3,\ 1^5]$
$[7,\ 1]$	$1T_1,\ 7T_4^*$	$8T_{43}^*$	336	$[8,\ 7,\ 6,\ 1^5]$
$[7,\ 1]$	$1T_1,\ 7T_5^{+}$	$8T_{48}^{+}$	1344	$[8,\ 7,\ 6,\ 4,\ 1^4]$
$[7,\ 1]$	$1T_1,\ 7T_6^{+}$	$8T_{49}^{+}$	$8!\,/\,2$	$[8,\ \ldots,\ 3,1^2]$
$[7,\ 1]$	$1T_1,\ 7T_7$	$8T_{50}$	$8!$	$[8,\ \ldots,\ 1]$

G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture

Table de rupture en degré 9

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^9]$	$(1T_1)^9$	$9T_1^{+*}$	9	$[9,\ 1^8]$
$[1^9]$	$(1T_1)^9$	$9T_2^{+*}$	9	$[9,\ 1^8]$
$[2^3,\ 1^3]$	$(1T_1)^3,\ (2T_1)^3$	$9T_4^{*}$	18	$[9,\ 2,\ 1^7]$
$[3^2,\ 1^3]$	$(1T_1)^3,\ (3T_1^{+*})^2$	$9T_6^{+*}$	27	$[9,\ 3,\ 1^7]$
$[3^2,\ 1^3]$	$(1T_1)^3,\ (3T_1^{+*})^2$	$9T_7^{+*}$	27	$[9,\ 3,\ 1^7]$
$[3^2,\ 1^3]$	$(1T_1)^3,\ (3T_1^{+*})^2$	$9T_{17}^{+*}$	81	$[9,\ 3^2,\ 1^6]$
$[6,\ 1^3]$	$(1T_1)^3,\ 6T_2^{*}$	$9T_{12}^{*}$	54	$[9,\ 6,\ 1^7]$
$[6,\ 1^3]$	$(1T_1)^3,\ 6T_5^{*}$	$9T_{20}^{*}$	162	$[9,\ 6,\ 3,\ 1^6]$
$[2^4,\ 1]$	$1T_1,\ (2T_1)^4$	$9T_3^{+*}$	18	$[9,\ 2,\ 1^7]$
$[2^4,\ 1]$	$1T_1,\ (2T_1)^4$	$9T_5^{+*}$	18	$[9,\ 2,\ 1^7]$
$[4,\ 2^2,\ 1]$	$1T_1,\ (2T_1)^2,\ 4T_2^{+*}$	$9T_8^{*}$	36	$[9,\ 2^2,\ 1^6]$
$[3^2,\ 2,\ 1]$	$1T_1,\ 2T_1,\ (3T_2^{*})^2$	$9T_{13}^{*}$	54	$[9,\ 3,\ 2,\ 1^6]$
$[3^2,\ 2,\ 1]$	$1T_1,\ 2T_1,\ (3T_2^{*})^2$	$9T_{22}^{*}$	162	$[9,\ 3^2,\ 2,\ 1^5]$
$[3^2,\ 2,\ 1]$	$1T_1,\ 2T_1,\ (3T_2^{*})^2$	$9T_{25}^{+*}$	324	$[9,\ 3^2,\ 2^2,\ 1^4]$
$[3^2,\ 2,\ 1]$	$1T_1,\ 2T_1,\ (3T_2^{*})^2$	$9T_{28}^{*}$	648	$[9,\ 3^2,\ 2^3,\ 1^3]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_1^{*}$	$9T_{10}^{+*}$	54	$[9,\ 6,\ 1^7]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_1^{*}$	$9T_{11}^{+*}$	54	$[9,\ 3,\ 2,\ 1^6]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_3^{*}$	$9T_{18}^{*}$	108	$[9,\ 6,\ 2,\ 1^6]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_5^{*}$	$9T_{21}^{+*}$	162	$[9,\ 3^2,\ 2,\ 1^5]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_9^{*}$	$9T_{24}^{*}$	324	$[9,\ 6,\ 3,\ 2,\ 1^5]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_{13}^{*}$	$9T_{29}^{*}$	648	$[9,\ 6,\ 3,\ 2^2,\ 1^4]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_{13}^{*}$	$9T_{30}^{+*}$	648	$[9,\ 6,\ 3,\ 2^2,\ 1^4]$
$[6,\ 2,\ 1]$	$1T_1,\ 2T_1,\ 6T_{13}^{*}$	$9T_{31}^{*}$	1296	$[9,\ 6,\ 3,\ 2^3,\ 1^3]$
$[4^2,\ 1]$	$1T_1,\ (4T_1^{*})^2$	$9T_9^{+*}$	36	$[9,\ 4,\ 1^7]$
$[4^2,\ 1]$	$1T_1,\ (4T_3^{*})^2$	$9T_{16}^{*}$	72	$[9,\ 4,\ 2,\ 1^6]$
$[8,\ 1]$	$1T_1,\ 8T_1^{*}$	$9T_{15}^{*}$	72	$[9,\ 8,\ 1^7]$
$[8,\ 1]$	$1T_1,\ 8T_5^{+*}$	$9T_{14}^{+*}$	72	$[9,\ 8,\ 1^7]$
$[8,\ 1]$	$1T_1,\ 8T_8^{*}$	$9T_{19}^{*}$	144	$[9,\ 8,\ 2,\ 1^6]$
$[8,\ 1]$	$1T_1,\ 8T_{12}^{+*}$	$9T_{23}^{+*}$	216	$[9,\ 8,\ 3,\ 1^6]$
$[8,\ 1]$	$1T_1,\ 8T_{23}^{*}$	$9T_{26}^{*}$	432	$[9,\ 8,\ 6,\ 1^6]$
$[8,\ 1]$	$1T_1,\ 8T_{25}^{+*}$	$9T_{27}^{+}$	504	$[9,\ 8,\ 7,\ 1^6]$
$[8,\ 1]$	$1T_1,\ 8T_{36}^{+*}$	$9T_{32}^{+}$	1512	$[9,\ 8,\ 7,\ 3,\ 1^5]$
$[8,\ 1]$	$1T_1,\ 8T_{49}^{+}$	$9T_{33}^{+}$	$9!\,/\,2$	$[9,\ \ldots,\ 3, 1^2]$
$[8,\ 1]$	$1T_1,\ 8T_{50}$	$9T_{34}$	$9!$	$[9,\ \ldots,\ 1]$

G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture

Table de rupture en degré 10

$D(G)$	$S(G)$	G	$\lvert G \rvert$	$\mathcal{L}(G)$
$[1^{10}]$	$(1T_1)^{10}$	$10T_1^*$	10	$[10,\ 1^9]$
$[1^{10}]$	$(1T_1)^{10}$	$10T_2^*$	10	$[10,\ 1^9]$
$[5,\ 1^5]$	$(1T_1)^5,\ 5T_1^{+*}$	$10T_6^*$	50	$[10,\ 5,\ 1^8]$
$[2^4,\ 1^2]$	$(1T_1)^2,\ (2T_1)^4$	$10T_3^*$	20	$[10,\ 2,\ 1^8]$
$[2^4,\ 1^2]$	$(1T_1)^2,\ (2T_1)^4$	$10T_4^*$	20	$[10,\ 2,\ 1^8]$
$[2^4,\ 1^2]$	$(1T_1)^2,\ (2T_1)^4$	$10T_8^{+*}$	80	$[10,\ 2^3,\ 1^6]$
$[2^4,\ 1^2]$	$(1T_1)^2,\ (2T_1)^4$	$10T_{14}^*$	160	$[10,\ 2^4,\ 1^5]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_1^*)^2$	$10T_5^*$	40	$[10,\ 4,\ 1^8]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_3^*)^2$	$10T_{15}^{+*}$	160	$[10,\ 4,\ 2^2,\ 1^6]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_3^*)^2$	$10T_{16}^*$	160	$[10,\ 4,\ 2^2,\ 1^6]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_3^*)^2$	$10T_{23}^*$	320	$[10,\ 4,\ 2^3,\ 1^5]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_4^{+*})^2$	$10T_{11}$	120	$[10,\ 4,\ 3,\ 1^7]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_4^{+*})^2$	$10T_{12}$	120	$[10,\ 4,\ 3,\ 1^7]$
$[4^2,\ 1^2]$	$(1T_1)^2,\ (4T_5^*)^2$	$10T_{22}$	240	$[10,\ 4,\ 3,\ 2,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{16}^*$	$10T_{25}^*$	320	$[10,\ 8,\ 2^2,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{20}^{+*}$	$10T_{24}^{+*}$	320	$[10,\ 8,\ 2^2,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{27}^*$	$10T_{29}^*$	640	$[10,\ 8,\ 2^3,\ 1^5]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{32}^{+*}$	$10T_{34}^+$	960	$[10,\ 8,\ 6,\ 2,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{38}^*$	$10T_{36}$	1920	$[10,\ 8,\ 6,\ 2^2,\ 1^5]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{39}^{+*}$	$10T_{37}^+$	1920	$[10,\ 8,\ 6,\ 4,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{40}^*$	$10T_{38}$	1920	$[10,\ 8,\ 6,\ 4,\ 1^6]$
$[8,\ 1^2]$	$(1T_1)^2,\ 8T_{44}^*$	$10T_{39}$	3840	$[10,\ 8,\ 6,\ 4,\ 2,\ 1^5]$
$[5,\ 2^2,\ 1]$	$1T_1,\ (2T_1)^2,\ 5T_2^{+*}$	$10T_9^*$	100	$[10,\ 5,\ 2,\ 1^7]$
$[5,\ 2^2,\ 1]$	$1T_1,\ (2T_1)^2,\ 5T_2^{+*}$	$10T_{10}^*$	100	$[10,\ 5,\ 2,\ 1^7]$
$[5,\ 2^2,\ 1]$	$1T_1,\ (2T_1)^2,\ 5T_2^{+*}$	$10T_{21}^*$	200	$[10,\ 5,\ 2^2,\ 1^6]$
$[6,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 6T_2^*$	$10T_7^+$	60	$[10,\ 6,\ 1^8]$
$[6,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 6T_3^*$	$10T_{13}$	120	$[10,\ 6,\ 2,\ 1^7]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{17}^*$	200	$[10,\ 5,\ 4,\ 1^7]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{18}^{+*}$	200	$[10,\ 5,\ 4,\ 1^7]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{19}^*$	200	$[10,\ 5,\ 4,\ 1^7]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{20}^*$	200	$[10,\ 5,\ 4,\ 1^7]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{27}^*$	400	$[10,\ 5,\ 4,\ 2,\ 1^6]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{28}^{+*}$	400	$[10,\ 5,\ 4,\ 2,\ 1^6]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_1^*,\ 5T_3^*$	$10T_{33}^*$	800	$[10,\ 5,\ 4^2,\ 1^6]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_4^{+*},\ 5T_4^+$	$10T_{40}$	7200	$[10,\ 5,\ 4^2,\ 3^2,\ 1^4]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_5^*,\ 5T_5$	$10T_{41}$	14400	$[10,\ 5,\ 4^2,\ 3^2,\ 2,\ 1^3]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_5^*,\ 5T_5$	$10T_{42}^+$	14400	$[10,\ 5,\ 4^2,\ 3^2,\ 2,\ 1^3]$
$[5,\ 4,\ 1]$	$1T_1,\ 4T_5^*,\ 5T_5$	$10T_{43}$	28800	$[10,\ 5,\ 4^2,\ 3^2,\ 2^2,\ 1^2]$
$[9,\ 1]$	$1T_1,\ 9T_9^{+*}$	$10T_{26}^+$	360	$[10,\ 9,\ 4,\ 1^7]$
$[9,\ 1]$	$1T_1,\ 9T_{14}^{+*}$	$10T_{31}^+$	720	$[10,\ 9,\ 8,\ 1^7]$
$[9,\ 1]$	$1T_1,\ 9T_{15}^*$	$10T_{30}$	720	$[10,\ 9,\ 8,\ 1^7]$
$[9,\ 1]$	$1T_1,\ 9T_{16}^*$	$10T_{32}$	720	$[10,\ 9,\ 4,\ 2,\ 1^6]$
$[9,\ 1]$	$1T_1,\ 9T_{19}^*$	$10T_{35}$	1440	$[10,\ 9,\ 8,\ 2,\ 1^6]$
$[9,\ 1]$	$1T_1,\ 9T_{33}^+$	$10T_{44}^+$	$10!\,/\,2$	$[10,\ \ldots,\ 3,1^2]$
$[9,\ 1]$	$1T_1,\ 9T_{34}$	$10T_{45}$	$10!$	$[10,\ \ldots,\ 1]$

G : Groupes de Galois possibles, $D(G)$: degrés de rupture , $S(G)$: groupes de Galois des facteurs de rupture, $\mathcal{L}(G)$: degrés de rupture

Annexe B

Implantation de l'algorithme `Generateurs`

Cette annexe est consacrée l'implantation en MAGMA (version 2.10) du premier algorithme. L'algorithme `IsPurGaloisIdeal` calcule le groupe de décomposition d'un idéal triangulaire (Algorithme 4.2.12). Cette implantation a été réalisée en collaboration avec G. Renault.

Les entrée de la fonctions ci-dessous sont une permutation σ et l'ensemble des orbites d'un sous-groupe G de S_n noté `orbites`. Cette fonction retourne les orbites de $\{1, ..., n\}$ sous l'action du groupe $\langle G \cup \sigma \rangle$.

```
function NouvellesOrbites (orbites,sigma);
nvorbites := {};
while IsEmpty(orbites) eq false 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;



procedure TUPm(r,l,~sigma ,~S,~SP,~n,~sn);

 /* Cette procédure recherche une permutation sigma dans dec(I) de suffixe
l. Si elle est trouvée, le calcul s'achève. Lors de l'appel initial de tup,
sigma doit etre initialisée à la permutation identité (voir condition d'arrêt :
sigma not eq Id). Un prétest modulaire d'appartenance à l'idéal est utilisé.
*/

if r eq 0 then
     sigma:= sn ! l;
else
     ens:=Reverse(Sort(SetToSequence({1..n} diff Set(l))));
     for a in ens do
          if sigma eq Id(sn) then
              ll := [a] cat l;
              rho := SetToSequence({1..n} diff Set(ll)) cat ll;
              if NormalForm((SP[r])^(sn! rho ,SP)) eq 0 then
                  if NormalForm((S[r])^(sn! rho ,S)) eq 0 then
                     TUPm(r-1,ll ,~sigma ,~S,~SP,~n,~sn);
                  end if;
              end if;
          end if;
      end for;
end if;
end procedure;



procedure deh0ahnm(k,~G,~S,~SP,~n,~sn,~orbites);

 /* Cette procédure détermine un système de générateurs du fixateur de {k-1..n}
du groupe de décomposition D de l'idéal engendré par les polynôme de l'ensemble
S en fonction d'un système de générateurs du fixateur de {k-1..n} de D. Un
prétest modulaire d'appartenance à l'idéal est utilisé */

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
               sigma:= Id(sn);
               TUPm (k-1,[ak] cat [(k+1)..n],~sigma ,~S,~SP,~n,~sn);
               if not (sigma eq Id(sn)) then
                    G:=G cat [sigma];
                    orbites:=NouvellesOrbites(orbites,sigma);
                    elt:=elt meet {Max(o): o in orbites};
               end if;
          end if;
     end if;
end while;
end procedure;



Generateurs:=function(S);

 /* Cette fonction calcule un système de générateurs du groupe de décomposition
de l'idéal engendré par les polynômes de la liste S ; un prétest modulaire
d'appartenance à l'idéal y est ajouté */

n:=Rank(Parent (S[1]));
sn:=Sym(n);
G:=[];
orbites := {{i}: i in {1..n}} ;
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]];
for k:= 2 to n do
    deh0ahnm(k,~G,~S,~SP,~n,~sn,~orbites);
end for;
return PermutationGroup<n|G>;
end function;
```

Bibliographie

[1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *Appl. Algebra Engrg. Comm. Comput.*, 15(3-4) :279–294, 2004.

[2] A.-M. Ampère. Fonctions interpolaires. Annales de M. Gergonne, 1826.

[3] 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.

[4] H. Anai and K. Yokoyama. Radical representation of polynomial roots. *Sūrikaisekikenkyūsho Kōkyūroku*, (920) :9–24, 1995.

[5] J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118 :23–40, 1997. Algorithms for algebra (Eindhoven, 1996).

[6] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comput.*, 28(1-2) :105–124, 1999.

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

[8] 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.

[9] K. Belabas. A relative van Hoeij algorithm over number fields. *J. Symbolic Comput.*, 37(5) :641–668, 2004.

[10] E. H. Berwick. On soluble sextic equations. *Proc. London Math. Soc.*, 29 :1–28, 1929.

[11] 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).

[12] N. Bourbaki. *Algèbre Commutative. Chapitres 5 à 7.* Éléments de mathématiques. Masson, 1985.

[13] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, 4 :374–383, 1970.

[14] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. 72 :3–21, 1979.

[15] G. Butler. *Fundamental algorithms for permutation groups*, volume 559 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 1991.

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

[17] 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.

[18] 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.

[19] 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.

[20] L. Ducos. Construction de corps de décomposition grâce aux facteurs de résolvantes. *Comm. Algebra*, 28(2) :903–924, 2000.

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

[22] H. M. Edwards. Kronecker's views on the foundations of mathematics. In *The history of modern mathematics, Vol. I (Poughkeepsie, NY, 1989)*, pages 67–77. Academic Press, Boston, MA, 1989.

[23] J.-C. Faugére. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3) :61–88, 1999.

[24] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). pages 75–83 (electronic), 2002.

[25] H. O. Foulkes. The resolvents of an equation of seventh degree. *Quart. J. Math. Oxford Ser.*, 2 :9–19, 1931.

[26] K. Girstmair. On the computation of resolvents and Galois groups. *Manuscripta Math.*, 43(2-3) :289–307, 1983.

[27] Giulia. UMS MEDICIS. Intel - Pentium III 2 x 933 Mhz, 1024 Mo, Linux 2.4.1, http ://www.medicis.polytechnique.fr.

[28] Gómez Molleda, M. A. *Cálculo del Centro de un Grupo de Galois y Applicationes.* PhD thesis, Universidad de Cantabria, 2002.

[29] RENAULT Guénaël. *Calcul efficace de corps de décomposition.* PhD thesis, LIP6, Université Paris VI, 2005.

[30] 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.

[31] A. Hulpke. *Konstruction transitiver Permutationsgruppen.* PhD thesis, RWTH Aachen, 1996.

[32] 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.

[33] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4 :182–196 (electronic), 2001. http ://www.mathematik.uni-kassel.de/ klueners/minimum/.

[34] L. Kronecker. Ein fundamentalsatz der allgemeinen arithmetik. *Journal für die reine und angewandte Mathematik*, 100 :490–510, 1887.

[35] S. Landau. Polynomial time algorithms for Galois groups. In *EUROSAM 84 (Cambridge, 1984)*, volume 174 of *Lecture Notes in Comput. Sci.*, pages 225–236. Springer, Berlin, 1984.

[36] S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1) :184–195, 1985.

[37] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *J. Comput. System Sci.*, 30(2) :179–208, 1985.

[38] Susan Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1) :184–195, 1985.

[39] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symbolic Comput.*, 13(2) :117–131, 1992.

[40] D. Lazard. Solving quintics by radicals. In *The legacy of Niels Henrik Abel*, pages 207–225. Springer, Berlin, 2004.

[41] F. Lehobey. *Calcul et factorisation interactive de résolvantes de Lagrange en théorie de Galois effective.* PhD thesis, Université de Rennes 1, 1999.

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

[43] 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.

[44] F. Mertens. Ein beweis des galois'shen fundamentalsatzes. *Akad. Wiss. Wien Math.-Natur. Kl. Sitzungsber. IIa*, 111 :17–37, 1902.

[45] M. Noro and K. Yokoyama. Factoring polynomials over algebraic extension fields. *Josai Information Science Researches*, **9** :11–33, 1997.

[46] 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.

[47] S. Orange, G. Renault, and A. Valibouze. Note sur les relations entre les racines d'un polynôme réductible. *Theor. Inform. Appl.*, 39(4) :651–659, 2005.

[48] Aubry P. and Moreno Maza M. Triangular sets for solving polynomial systems : a comparative implementation of four methods. *J. Symb. Comput.*, 28(1-2) :125–154, 1999.

[49] PARI/GP. http ://www.parigp-home.de, 2002. Version 2.2.4.

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

[51] *Risa/Asir, version 2003/05/07.* http ://www.asir.org.

[52] X. F. Roblot. Polynomial factorization algorithms over number fields. *J. Symbolic Comput.*, 38(5) :1429–1443, 2004.

[53] Á. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2003.

[54] C. Sims. Computation with permutation groups. In *Proc. Second Symp. on Symbolic and Algebraic Manipulation*, pages 23–28. ACM Press, 1971.

[55] L. Soicher and J. McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3) :273–281, 1985.

[56] 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.

[57] R. Stauduhar. The determination of galois groups. *Math. Comp.*, 27 :981–996, 1973.

[58] A. Steel. Communication privée, jan 2003. Mail en réponse à une question sur la présence d'un bug dans la factorisation de polynôme à coefficients dans un corps de nombres.

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

[60] B. Trager. Algebraic factoring and rational functiun integration. In *Proceedings of SYMSAC'76*, pages 219–226, 1976.

[61] 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.

[62] 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.

[63] M. van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2) :167–189, 2002.

[64] D. Wang. Méthodes d'élimination et applications. *INPG*, 1999. Mémoire d'habilitation.

[65] 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).