Oh ! Venez après cela prêcher la paix ! Venez demander aux hommes qui souffrent d'avoir pitié de ce qui est ! Pitié, jamais ! Haine, voilà tout. Qui ne la ressent pas profondément, cette haine du présent, n'a pas vraiment l'amour de l'avenir. [...]

Il me manque, pour être un savant, de n'être que cela. Le cœur chez moi s'est révolté contre la tête ; je n'ajoute pas comme toi : «C'est bien dommage».

Évariste Galois.

Remerciements

Matérialiste convaincu, je mesure le profit que j'ai pu tirer des conditions de travail exceptionnelles dont Marc Giusti m'a fait bénéficier en m'acceptant au laboratoire GAGE, où j'ai pu apprécier l'importance des moyens qu'il a mis à la disposition des jeunes doctorants. Nicole Dubois y a ajouté sa bonne humeur et sa gentillesse constantes, et Joël Marchand s'est toujours rendu disponible pour me former aux outils informatiques du laboratoire dont il assurait en même temps la maintenance avec la compétence que chacun lui reconnaît.

Annick Valibouze m'a encadré avec un dévouement tout particulier ; les cachets de la poste de la rue du Louvre timbrés à 23h55 en font foi : ils correspondent à des dossiers que je lui ai fait signer à 23h. Le sujet sur lequel elle m'a fait travailler, bien déblayé par ses travaux communs avec Jean-Marie Arnaudiès, a été un très bon point de départ qui m'a permis de biffurquer vers la résolution de systèmes algébriques. Enfin, sans ménager son temps, elle m'a fait bénéficier de sa compétence en programmation dans les différents systèmes de calcul formel en m'apprenant à programmer.

Malgré ses lourdes tâches administratives, Marc Giusti a co-encadré cette thèse, s'est montré disponible pour me conseiller et m'a montré comment l'éclairage précieux d'une philosophie d'évaluation dévoile les possiblités d'un gain énorme de complexité.

J'ai été débloqué dans plusieurs situations critiques par mon camarade François Ollivier, aux contributions duquel je dois beaucoup et avec qui ce fut toujours un plaisir de discuter.

Daniel Lazard m'a fait l'honneur de participer à mon jury. Il a en outre collaboré à la résolution de systèmes avec symétries, et m'a montré un intéressant champ d'application en mécanique céleste qui débouche sur une collaboration fructueuse avec son élève Ilias Kotsireas.

Bernd Heinrich Matzat et Jean-François Mestre ont eu la patience de rapporter sur mon mémoire. Carlo Traverso m'a fait le grand honneur d'accepter de présider mon jury. Je tiens à les en remercier.

Une relecture rigoureuse de ma thèse a été effectué par Jean-Marie Arnaudiès qui l'a enrichie de ses corrections. Il a en outre, avec sa bonne humeur méridionale, répondu avec précision à mes questions algébriques.

Claude Quitte m'a fait bénéficier avec désintéressement de ses connaissances variées en mathématiques.

J'ai pu bénéficier de discussions mathématiques avec Marc Chardin, Vincent Cossart, Jean-Charles Faugère, Joos Heintz, Gregor Kemper, Ilias Kotsireas, Guillermo Moreno, Jean Moulin-Ollagnier, Luis-Miguel Pardo, Michel Petitot, Olivier Piltant, Jirung Albert Shih, Martin Sombra, Bernd Sturmfels et Jacques-Arthur Weil. Ma participation au Projet Galois du GDR MEDICIS m'a aussi permis de discuter avec ses membres, dont Ines Abdeljaouad, Lionel Ducos, Isabelle Gil-Delessalle, Frédéric Lehobey et Nicolas Rennert.

Ariane Germa-Peladan, Jirung Albert Shih et Jacques-Arthur Weil ont eu à supporter, en temps que compagnons de bureau, mes questions informatiques à mon arrivée au laboratoire.

Table des matières

Chapitre 1

Introduction

Il est fréquent qu'une même technique algébrique puisse être utilisée dans plusieurs domaines distincts. Le travail qui est présenté ici en est l'illustration. Il devait en effet se limiter initialement à l'étude du problème direct de la théorie de Galois effective : identifier le groupe de Galois d'un polynôme donné. Mais il s'est avéré que les outils de la théorie des invariants que nous avons développés dans ce but donnent aussi des résultats pour la résolution des systèmes d'équations algébriques invariantes par des symétries. Cela nous a conduit à développer notre travail dans cette direction.

La structure de ce volume, divisé en trois parties, suit cette évolution. Une première partie présente des outils de théorie des invariants que nous avons développés ; ils seront utilisés dans les deux autres parties. Suivent une seconde partie qui traite du problème direct de la théorie de Galois effective, et une troisième qui présente une méthode de résolution des systèmes d'équations algébriques avec symétries.

$\star$

La première partie concerne donc la théorie des invariants effective. Elle se propose de permettre une manipulation efficace des éléments de l'algèbre $k[\mathbf{X}]^H$, ou $k(\mathbf{X})^H$, des invariants sous l'action d'un sous-groupe fini H du groupe linéaire. Il s'agit d'être capable d'une part d'effectuer des calculs algébriques sur ces invariants sans avoir à manipuler les polynômes sous forme développée, d'autre part de permettre de spécialiser n'importe quel invariant de H à partir de la seule connaissance des valeurs spécialisées d'un petit nombre d'entre eux.

Un premier chapitre met en place les notations et rappelle quelques résultats généraux. Il est suivi (chapitre 2) d'une première approche linéaire du problème dans le cas où H est un groupe de permutations : on représente les invariants de H dans une base de k-espace vectoriel. Le problème qui apparaît est le calcul du produit de deux éléments de la base. Pour cela, nous généralisons (Prop. 2.1) un résultat d'A. Valibouze qui concerne le groupe symétrique. Nous généralisons aussi (Prop. 2.5) le test d'égalité, qui est nécessaire pour regrouper les termes après le calcul d'un produit ; dans le cas du groupe symétrique, ce test d'égalité se limitait à un simple algorithme de tri. Nous avons en outre implanté dans le langage de calcul formel AXIOM [37] cette représentation des invariants du groupe symétrique, sous forme d'un domaine, `PolynomesSymetriques`, ainsi que divers algorithmes permettant d'exprimer ces invariants dans diverses représentations, et de passer d'une représentation à une autre. La description des invariants au chapitre 2 permet donc les calculs algébriques sur les invariants.

Les chapitres 3 et 4 traitent le problème de la spécialisation. Ils mènent, de façon parallèle, des méthodes permettant d'exprimer les invariants de H en fonction des éléments d'une base de transcendance $(\Pi_1, \ldots, \Pi_n)$ et d'une base de module libre sur la partie transcendante. Pour cela, le chapitre 4 décrit $k[\mathbf{X}]^H$ et s'appuie sur une décomposition d'Hironaka (normalisation de Noether alliée à la propriété de

Cohen-Macaulay), c'est-à-dire de la forme

$$k[X_1, \ldots, X_n]^H = \bigoplus_{i=1}^{e} k[\Pi_1, \ldots, \Pi_n]\ \Sigma_i\ , \tag{1.1}$$

la somme directe portant sur des $k[\mathbf{\Pi}]$-modules, tandis que le chapitre 3 décrit $k(\mathbf{X})^H$ grâce à un élément primitif :

$$k(\mathbf{X})^H = \bigoplus_{i=0}^{e-1} k(\Pi_1, \ldots, \Pi_n)\ \Theta^i\ . \tag{1.2}$$

Marc Giusti et Joos Heintz ont montré dans une série de travaux, qui fut initiée par [30] pour aboutir à [31] (voir aussi un résumé de ces travaux dans la note au CRAS [33]) qu'une mise en position de Noether d'une variété — ce qui correspond algébriquement à une normalisation de Noether de l'anneau de fonctions associé — est d'une manière générale un bon cadre pour une évaluation avec une bonne complexité. Le travail présenté ici est ainsi, dans le cadre particulier de la théorie des invariants, auquel cas la normalisation de Noether peut d'ailleurs être calculée une fois pour toutes pour chaque groupe, une illustration de ce principe général, même si nous y présentons les choses dans une philosophie de réécriture et non d'évaluation comme dans [30] et [32]. C'est donc à la lumière des travaux de Marc Giusti et de Joos Heintz que nous avons pu comprendre avec du recul la raison de l'efficacité des algorithmes de cette thèse, dont la rédaction finale a bénéficié de cet éclairage qui manquait à nos premiers articles [17] et [19] sur le sujet.

Les théories utilisées sont donc bien connues : les travaux de Hochster, Eagon et Stanley [60] dans le cas polynomial, et la théorie des corps dans le cas fractionnaire. Dans les deux cas ($k(\mathbf{X})^H$ au chapitre 3 et $k[\mathbf{X}]^H$ au chapitre 4), la décomposition (extension transcendante de corps ou décomposition de Noether) est d'un type particulier : le fait qu'on a une algèbre d'invariants implique que l'on a un module libre sur la partie transcendante pure. Nous avons pu trouver des algorithmes efficaces d'algèbre linéaire pour effectuer en pratique cette décomposition. Cela permet d'une part d'effectuer facilement les opérations dans cette algèbre, en se limitant aux opérations sur les éléments de cette base. Mais cela permet surtout de spécialiser les invariants de H grâce à la connaissance des valeurs spécialisées de $\Pi_1, \ldots, \Pi_n$.

En effet, au chapitre 3, on obtient la valeur spécialisée θ de Θ — ou de l'un de ses conjugués — à partir des valeurs spécialisées de $\Pi_1, \ldots, \Pi_n$ en calculant et en spécialisant le polynôme minimal de Θ : alors, θ en sera une racine. Nous donnons alors un algorithme rapide (Prop. 3.10) pour exprimer un invariant de H (resp. sa valeur spécialisée) en fonction de $\Pi_1, \ldots, \Pi_n, \Theta$ (resp. leurs valeurs spécialisées) selon la décomposition (1.2). Il consiste à mettre une structure d'espace quadratique sur l'espace vectoriel $k(\mathbf{X})^H$ (voir Prop. 3.5).

En revanche, au chapitre 4, les choses sont un peu plus compliquées, bien que nous donnions aussi (Prop. 4.11) un algorithme pour calculer effectivement la décomposition (1.1) d'un invariant. On peut en effet, comme au chapitre 3, obtenir les valeurs spécialisées σ_i des Σ_i — ou d'un de leurs conjugués — en calculant, spécialisant, puis factorisant leur polynôme minimal. Le problème est qu'alors, il n'y a aucune raison pour que le conjugué de Σ_i dont σ_i est la valeur spécialisée soit conjugué par le même élément que le conjugué d'un Σ_j dont σ_j est la valeur spécialisée : on a en général $\sigma_i = \widetilde{\tau.\Sigma_i}$ et $\sigma_j = \widetilde{\tau'.\Sigma_j}$, où τ et τ' n'ont rien à voir l'un avec l'autre, ce qui fait que l'on ne peut rien en tirer. Mais nous montrons en fait (théorèmes 4.12 et 4.14) que si l'on impose non seulement aux σ_i d'être racine des polynômes minimaux mais en outre de satisfaire toutes les syzygies (spécialisées) entre les Σ_i, syzygies que l'on peut calculer à l'avance, alors cela assure la cohérence qui manquait : les σ_i viennent de Σ_i conjugués par un même élément.

Les deux chapitres 3 et 4 ont donc des applications algorithmiques, qui seront pleinement utilisées dans la seconde partie (théorie de Galois effective) et à la troisième partie (résolution des systèmes d'équations algébriques avec symétries).

Le chapitre 5 est indépendant et traite un problème soumis par B. Sturmfels : si un groupe linéaire satisfait au problème de Noether (c'est-à-dire si ses invariants forment une extension transcendante pure de k) pour une certaine action sur un anneau de polynômes à n indéterminées, alors il y satisfait encore quand il opère de façon diagonale sur np indéterminées. Ce résultat est connu depuis Mattuck et fut généralisé ensuite. Nous en donnons ici une preuve effective, qui a en outre l'avantage de fournir explicitement une base de transcendance pure pour l'action diagonale à partir d'une base pure pour l'action initiale.

$\star$

La seconde partie concerne la théorie de Galois effective, et plus particulièrement le problème direct (recherche du groupe de Galois d'un polynôme donné), quoique les calculs de résolvantes puissent aussi s'appliquer à certains aspects du problème inverse (réalisation effective d'un groupe en un degré donné par exemple).

Le problème direct, qui conduit à des calculs que Galois jugeait «impraticables» et qu'il ne «voudrait charger ni lui ni personne de faire», a cependant été abordé dès 1929 par Berwick, qui donne une méthode de résolution complète en degré 6 dans le cas transitif, et par Tchebotarev (1950), qui donne des méthodes modulaires qui permettent dans certains cas d'identifier le groupe de Galois. Mais c'est avec le développement de l'informatique, qui permet maintenant des calculs hors de portée au siècle de Galois, que se sont développées diverses méthodes, et plus particulièrement au cours des vingt-cinq dernières années : méthodes numériques à partir de Stauduhar (1973) et poursuivies Geyer (1993) et par Eichenlaub et Olivier (1995), méthodes p-adiques (Yokoyama, 1996), méthodes algébriques utilisant des résolvantes (voir Déf. 6.1) d'invariants linéaires — c'est-à-dire polynomiaux de degré un (Butler, McKay, Soicher, 1981). En 1993, Arnaudiès et Valibouze montrent [7] que les méthodes utilisant des résolvantes de Lagrange absolues, c'est-à-dire dont les coefficients sont des invariants du groupe symétrique $\mathfrak{S}_n$, sont déterministes et ils donnent un moyen d'obtenir le meilleur algorithme utilisant des résolvantes absolues ; puis Valibouze montre dans [70] qu'on peut accélérer ces méthodes en calculant les groupes de Galois de facteurs irréductibles de bas degré des résolvantes (contrairement à Berwick qui le faisait par manque de résolvantes en degré 6, Valibouze l'utilise pour optimiser une méthode déjà déterministe sans cela). Ils montrent aussi qu'on peut utiliser des résolvantes relatives (c'est-à-dire dont les coefficients appartiennent à $k[\mathbf{X}]^L$ où L est un sous-groupe de $\mathfrak{S}_n$), mais se pose alors le problème de la spécialisation de ces résolvantes.

Pour les résolvantes absolues, spécialiser des polynômes symétriques par les racines d'un polynôme f se faisait en les exprimant en fonction des polynômes symétriques élémentaires, puis en substituant à ces polynômes symétriques élémentaires les coefficients (au signe près) de f. Pour calculer les coefficients d'une résolvante relative à un groupe L, qui appartiennent bien à k quand L contient la représentation du groupe de Galois de f, on doit spécialiser les coefficients génériques de ces résolvantes qui sont des invariants du groupe $L \subset \mathfrak{S}_n$. Mais quand $L \neq \mathfrak{S}_n$, ces derniers ne peuvent pas s'exprimer génériquement en fonction des coefficients de f puisque ceux-ci sont des expressions symétriques en les racines. C'est pourquoi les résolvantes relatives sont restées longtemps le domaine réservé des numériciens, qui les calculent à partir d'approximations des racines de f.

Nous montrons dans les chapitres 8 et 9 qu'il est en fait possible de calculer ces résolvantes relatives par du calcul formel uniquement (donc sans calculer d'approximations des racines), et de manière efficace. Cela peut paraître contradictoire d'après ce qui vient d'être dit : «les coefficients des résolvantes relatives ne peuvent pas s'exprimer génériquement en fonction des coefficients de f». L'explication est que nous calculons une résolvante relative sans savoir précisément laquelle : elle est relative à un certain conjugué $\tau.L.\tau^{-1}$ de L, où τ est une permutation que l'on ne connaît pas ; mais nous montrons au chapitre 8 que cela n'a pas d'importance ; et c'est logique car de toute manière c'est seulement à conjugaison près que l'on cherche à identifier la représentation du groupe de Galois dans le groupe symétrique.

C'est à partir de cette idée, et en utilisant comme outils les chapitres 3 et 4, que nous avons développé l'algorithme du chapitre 8, combinant les résolvantes relatives et les méthodes formelles précédentes.

Le fait que nous calculions une résolvante relative sans savoir laquelle c'est, comme nous venons de l'expliquer, est en fait un grand avantage sur les méthodes numériques. En effet ces dernières, dans leurs étapes intermédiaires, obligent à identifier précisément des sous-groupes, au lieu de leur seule classe de conjugaison, et à tester des conjugaisons par des permutations d'un sous-groupe de $\mathfrak{S}_n$ (voir [21, Par. 2.1.4, Remarque]), ce qui est coûteux et artificiel, puisque le résultat final est en fait à conjugaison près par un élément de $\mathfrak{S}_n$.

Le chapitre 8 correspond à l'article [17] dont nous avons retiré certaines parties afin d'éviter des redites de résultats du chapitre 3. Nous y donnons un équivalent formel de la méthode numérique de Stauduhar, qui consiste à utiliser les résolvantes relatives pour tester si le groupe de Galois est inclus dans un certain groupe, puis par ce moyen, à parcourir le graphe des classes de conjugaison de sous-groupes de $\mathfrak{S}_n$ par inclusions successives en partant de $\mathfrak{S}_n$ jusqu'à trouver le groupe de Galois cherché (ou plutôt la classe de conjugaison de sa représentation dans $\mathfrak{S}_n$, ce qui est plus précis car cela contient une information sur l'action de ce groupe sur les racines de f).

Outre cette «Méthode de Stauduhar formelle», ou «méthode de descente directe», on trouve aussi au chapitre 8 (Prop. 8.5) une borne sur le nombre de transformations à effectuer pour rendre les résolvantes séparables.

Signalons que le chapitre 8 a été rédigé avant le Théorème 4.14, et c'est pourquoi il n'utilise que les outils du chapitre 3. Mais le Th. 4.14 montre que l'on peut tout aussi bien utiliser le point de vue polynomial du chapitre 4 : nous en donnons l'illustration dans l'Annexe A

Le chapitre 9 reprend l'article [18], qui généralise la méthode du chapitre 8. Alors qu'au chapitre 8, on n'utilisait que les facteurs linéaires des résolvantes (c'est-à-dire leurs racines dans k) pour spécialiser les invariants, la méthode du chapitre 9, qui s'appuie sur le Théorème 9.7, montre qu'on peut tirer parti des autres facteurs.

Par exemple, si une résolvante d'un invariant Θ d'un groupe H a un facteur irréductible h de degré 2 sur k, soit $h = T^2 + aT + b$, alors il existe des permutations τ_1 et τ_2 telles que h soit le spécialisé de $(T - \tau_1.\Theta)(T - \tau_2.\Theta)$, donc on connaît ainsi la valeur spécialisée (c'est $-a$) du polynôme $\tau_1.\Theta + \tau_2.\Theta$, qui est un invariant d'un certain groupe G (ici le stabilisateur de $\{\tau_1.H, \tau_2.H\}$). On peut ainsi spécialiser des invariants de G grâce au calcul d'une résolvante de H : c'est l'idée qui est exploitée au chapitre 9.

Cela améliore souvent la méthode de «descente directe» de façon considérable, quand G est un groupe de grand indice mais H de petit indice : on remplace ainsi le calcul et la factorisation d'une résolvante de degré l'indice de G par ceux d'une résolvante de degré l'indice de H. Nous avons baptisé cette méthode «descente diagonale» car on ne passe plus d'un groupe à un sous-groupe, on passe directement de H à G.

Nous avons étudié jusqu'au degré 10 les algorithmes de résolution du problème direct par cette méthode, et calculé le degré maximal des résolvantes à factoriser pour identifier le groupe de Galois dans tous les cas de figure. Ces bornes sur les degrés sont répertoriées dans les tableaux du § 9.4, où elles sont comparées aux degrés nécessaires avec la méthode de «descente directe» (Stauduhar formelle) et avec la méthode de factorisation de résolvantes absolues (utilisant les degrés et groupes de Galois des facteurs irréductibles).

Le chapitre 7 est indépendant. Après avoir rappelé le lien entre groupe de Galois et idéal des relations algébriques entre les racines d'un polynôme, nous montrons (Prop. 7.5) le résultat suivant: le groupe de Galois d'un produit fg de polynômes est produit direct de ses sous-groupes $\mathrm{Gal}_k(f)$ et $\mathrm{Gal}_k(g)$ si et seulement si les relations algébriques entre les racines de fg se décomposent en relations entre les racines de f d'une part, et entre les racines de g d'autre part. Cela implique par exemple que des extensions galoisiennes finies sont linéairement disjointes si et seulement si leur intersection est réduite au corps de base.

$\star$

La troisième partie présente une méthode nouvelle de résolution de systèmes d'équations algébriques invariantes par des symétries.

Les méthodes usuelles utilisées pour résoudre de tels systèmes brisent les symétries. C'est le cas d'un calcul de base standard de l'idéal engendré par les équations du système. Une implantation efficace des calculs de bases standard a été implantée dans GB par Faugère. Une telle base standard privilégie un ordre sur les indéterminées. Une version améliorée des bases standard transforme un système algébrique en système triangulaire, dont la dernière équation n'a plus qu'une inconnue. Ici encore, les symétries sont brisées.

Gatermann s'est intéressée [24] à l'utilisation des symétries dans le calcul des bases Standard. Elle peut ainsi dans certains cas réduire les calculs. Notre point de vue est différent : nous ne cherchons pas de base standard de l'idéal de départ, nous cassons l'extension de corps dans laquelle vivent les solutions en extensions de plus petit degrés grâce aux symétries.

Le chapitre 10 reprend l'article [19], à quelques différences près : le § 10.5 est nouveau ; deux exemples ont été ajoutés ; d'autres paragraphes ont au contraire été supprimés car ils recoupaient les chapitres 3 et 4.

Soit G un sous-groupe fini du groupe linéaire $\mathbf{GL}_n(k)$ qui laisse invariant les équations du système, où n est le nombre d'inconnues. L'idée de cette partie est de décomposer l'algèbre d'invariants $k[\mathbf{X}]^G$, (resp. le corps $k(\mathbf{X})^G$), en l'écrivant comme module libre sur $k[\mathbf{X}]^L$ (resp. espace vectoriel sur $k(\mathbf{X})^L$), où $L \subset \mathbf{GL}_n(k)$ est un groupe fini de réflexions (resp. satisfaisant le problème de Noether) et contenant G.

On peut alors exprimer les équations du système de départ en fonction de n invariants $\Pi_1, \ldots, \Pi_n$ de L et d'un petit nombre d'invariants $\Sigma_1, \ldots, \Sigma_e$ (resp. un seul invariant Θ et ses puissances) de G.

Cela conduit à remplacer le système initial par deux systèmes : un premier système en $\Pi_1, \ldots, \Pi_n$, et un second système paramétré par les solutions $\pi_1, \ldots, \pi_n$ du premier donne les solutions $(x_1, \ldots, x_n)$ du système initial.

Nous prouvons dans les théorèmes 10.6 et 10.10 que l'on obtient ainsi toutes les solutions du système de départ. Le premier de ces théorèmes est fondé sur les techniques du chapitre 3, et est donc valable en caractéristique quelconque. Le second théorème s'appuie sur celles du chapitre 4 (donc en caractéristique nulle) et résulte du Théorème 4.14 : les équations du second système sont en effet les syzygies entre $\Sigma_1, \ldots, \Sigma_n$.

Autrement dit, la méthode consiste à casser l'extension de corps $k(x_1, \ldots, x_n)$ en deux parties, en introduisant $k(\pi_1, \ldots, \pi_n)$ au milieu. On fait ainsi chuter les degrés des polynômes à factoriser. Cela peut permettre par exemple de résoudre par radicaux les systèmes, comme nous le montrons dans les exemples du § 10.7. Mais on peut aussi s'en servir pour une autre représentation des solutions.

Outre les exemples présentés au § 10.7, où nous résolvons à la main certains systèmes (par exemple le système aux racines cycliques sixièmes) dont la base standard requérait de très lourds calculs (même sur des ordinateurs performants), la méthode de cette partie est utilisée, en collaboration avec I. Kotsireas, pour résoudre des équations de la mécanique céleste (problème aux 4 corps avec symétries).

$\star$

L'Annexe A est un exemple illustratif de la méthode du chapitre 8 («descente directe»), utilisée pour résoudre le problème direct en degré 5 : nous y donnons un nouvel algorithme, qui n'utilise que du calcul formel (pas de calcul approché des racines) et des factorisations de polynômes de degré au plus 6.

L'Annexe B illustre la méthode de «descente diagonale» du chapitre 9, sur l'exemple du problème direct en degré 6.

Première partie

Invariants de groupes finis

Chapitre 1

Généralités

Dans toute la suite de ce volume, k désigne un corps commutatif, n un entier naturel non nul et $X_1, \ldots, X_n$ des indéterminées algébriquement indépendantes sur k. La lettre grasse $\mathbf{X}$ désignera la famille $(X_1, \ldots, X_n)$; par exemple, $k[\mathbf{X}]$ est l'anneau de polynômes $k[X_1, \ldots, X_n]$.

De manière générale, k sera supposé, dans toute la suite, de caractéristique quelconque dans les chapitres ou paragraphes traitant des corps d'invariants fractionnaires $k(\mathbf{X})^G$, et de caractéristique nulle dans ceux portant sur des algèbres d'invariants polynomiaux $k[\mathbf{X}]^G$ — mais nous le repréciserons à chaque fois.

1.1 Action de groupes. Représentation de groupes.

Dans ce paragraphe, nous rappelons les définitions d'action (ou opération) à gauche d'un groupe sur un ensemble, et de représentation linéaire d'un groupe fini. On y désigne par G un groupe, dont la loi est notée multiplicativement, et par E un ensemble.

Action à gauche d'un groupe sur un ensemble

On appelle *action* (ou *opération*) du groupe G sur l'ensemble E toute application $\left| \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g.x \end{array} \right.$ telle que

i. $\forall x \in E, 1.x = x$

ii. $\forall (g_1, g_2) \in G,\ \forall x \in E,\ (g_1 g_2).x = g_1.(g_2.x)$.

Soit $x \in E$. On appelle *orbite* de x sous l'action de G et on note $\mathcal{O}rb_G(x)$ ou $G.x$ l'ensemble $\mathcal{O}rb_G(x) = G.x = \{g.x \ / \ g \in G\}$. On appelle *stabilisateur* (ou *sous-groupe d'isotropie*) de x dans G et on note $\mathcal{S}tab_G(x)$ le sous-groupe de G suivant : $\mathcal{S}tab_G(x) = \{g \in G \ / \ g.x = x\}$. On appelle *stabilisateur* d'une partie A de E et on note $\mathcal{S}tab_G(A)$ le sous-groupe de G suivant : $\mathcal{S}tab_G(A) = \{g \in G \ / \ g.A = A\}$. Les orbites sous l'action de G des éléments de E constituent une partition de E. On dit que l'action . est *transitive* si et seulement s'il n'y a qu'une orbite (alors égale à E). On dit que l'action . est *fidèle* si et seulement si $\bigcap_{x \in E} \mathcal{S}tab_G(x) = \{1\}$.

Représentation par permutations d'un groupe

À l'action . de G sur E on peut associer le morphisme de groupes ρ de G vers le groupe $\mathrm{Perm}(E)$ des permutations de E défini de la façon suivante : pour tout $g \in G$, on définit $\rho(g) \left| \begin{array}{ccc} E & \to & E \\ x & \mapsto & \rho(g)(x) = g.x \end{array} \right.$.

On dit que le morphisme ρ est une *représentation par permutations* du groupe G. Il est injectif si et seulement si l'action . est fidèle. Réciproquement, à tout morphisme ρ de G vers $\mathrm{Perm}(E)$, on peut associer une unique action . du groupe G dont ρ dérive.
EXEMPLE : Si G est un groupe fini d'ordre n, il opère fidèlement sur lui-même par multiplication à gauche, et ρ définit donc alors un isomorphisme de G sur un sous-groupe de $\mathfrak{S}_n$ (c'est le «Théorème de Cayley»).

Action d'un groupe sur un espace vectoriel

On appelle *action à gauche* du groupe G sur un k-espace vectoriel V toute action à gauche . de G sur l'ensemble support de V telle que pour tout $g \in G$, l'application $\rho_g : \left| \begin{array}{c} V \longrightarrow V \\ v \mapsto g.v \end{array} \right.$ soit linéaire ; ρ_g est alors un automorphisme de V, dont l'automorphisme réciproque est ρ_g^{-1}. En outre, l'application $g \mapsto \rho_g$ est un morphisme de G dans $\mathbf{GL}(V)$, ce qui donne une équivalence entre la notion d'action sur un espace vectoriel et la notion de représentation linéaire (cf. le paragraphe qui vient).

Représentation linéaire d'un groupe

Soit V un k-espace vectoriel. On appelle *représentation linéaire de G dans V* tout morphisme de G dans le groupe $\mathbf{GL}(V)$ des automorphismes de V. Une telle représentation ρ définit bien sûr une unique action . de G sur l'espace vectoriel V par : $\forall (g,v) \in G \times V,\ g.v = (\rho(g))(v)$.

À une opération . de G sur un ensemble E, on peut associer la représentation linéaire de G dans l'espace vectoriel $V = k^E$ définie sur les vecteurs de base (donc par linéarité sur tout V) de la façon suivante : $\forall g \in G, \forall x \in E,\ (\rho(g))(e_x) = e_{g.x}$, où $(e_x)_{x \in E}$ désigne la base canonique de k^E. Ainsi, toute action d'un groupe sur un ensemble peut être vue comme une représentation linéaire.
EXEMPLE : Le groupe symétrique $\mathfrak{S}_n$ opère sur $\mathbb{N}_n^* = \{1, \ldots, n\}$ en posant $\tau.i = \tau(i)$. Soit ρ la représentation linéaire de $\mathfrak{S}_n$ dans $V = k^n$ associée à cette action. Alors pour tout $\tau \in \mathfrak{S}_n$, la matrice de $\rho(\tau)$ dans la base canonique de k^n est $A_\tau = (\delta_{i,\tau(j)})_{(i,j) \in (\mathbb{N}^*}$, où δ désigne le symbole de Kronecker. Par exemple, pour $n = 3$, soit $\tau = (1\ 2\ 3)$. Alors $A_\tau = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Aussi, dans toute la suite de ce volume, les représentations de groupes par permutations seront traitées comme des cas particuliers de représentations linéaires.

Représentation dans l'algèbre symétrique $k[V] = \mathbf{S}(V^*)$

Soit ρ une représentation linéaire d'un groupe G dans un espace vectoriel V. Soit V^* le dual de V. Soit $\mathbf{S}(V^*) = \bigoplus_{k=0}^{\infty} S^k(V^*)$ l'algèbre symétrique de V, où $S^0(V^*) = k$, $S^1(V^*) = V^*$, $S^2(V^*) = V^* \circledS V^*$, *etc.* (voir une définition dans [13, A III.67] par exemple). Nous noterons $k[V] = \mathbf{S}(V^*)$; cette notation est justifiée ci-dessous.

Soit alors $\tilde{\rho}$ la représentation de G dans $k[V]$ produit symétrique de la représentation contragrédiente de ρ. Elle est définie à partir de ρ de la façon suivante :

$$\forall g \in G, \forall p \in k[V], \forall v \in V,\ ((\tilde{\rho}(g))(p))(v) = p((\rho(g^{-1}))(v))$$

Si V admet une base $\mathbf{v} = (v_i)_{i \in I}$, soit $\mathbf{v}^* = (v_i^*)_{i \in I}$ sa base duale. Alors, $k[V]$ est l'anneau de polynômes $k[v_i^*]_{i \in I}$, dont le produit est le produit symétrique $\circledS$: les éléments de $k[V]$ peuvent être vus comme des expressions polynomiales à coefficients dans k en les formes linéaires v_i^*, de la même façon que les fonctions polynomiales sur k^n, k étant supposé infini, peuvent être vues comme des polynômes en les formes linéaires associées aux indéterminées $X_1, \ldots, X_n$. D'où la notation $k[V]$, par analogie avec $k[\mathbf{X}]$.

Notons que l'application qui associe $k[V]$ à V et $\tilde{\rho}(g)$ à $\rho(g)$ est un foncteur covariant (le g^{-1} de la définition a été mis exprès pour le rendre covariant, c'est-à-dire pour que $\tilde{\rho}$ soit bien un morphisme).

Représentation dans un anneau de polynômes

La définition découle de celle du paragraphe précédent, qui en est la version canonique.

Plus précisément : soit $\rho : G \longrightarrow \mathbf{GL}_n(k)$ une représentation linéaire de G dans k^n. Pour tout $g \in G$, notons $A_g = \rho(g)$ la matrice de $\mathbf{GL}_n(k)$ correspondant à g. Alors la représentation $\tilde{\rho}$ de G dans $k[\mathbf{X}] = k[X_1, \ldots, X_n]$ associée à ρ est définie par :

$$\begin{aligned} \forall g \in G, \forall p \in k[\mathbf{X}], (\rho(g))(p) &= p(\mathbf{X}.B^t) \qquad \text{où } B = A_g^{-1} \\ &= p(b_{1,1}X_1 + \ldots + b_{1,n}X_n, \ldots, b_{n,1}X_1 + \ldots + b_{n,n}X_n) \\ &\quad \text{où } B = (b_{i,j})_{i,j \in \mathbb{N}_n^*}. \end{aligned}$$

La contravariance de la définition par rapport à un changement linéaire des indéterminées $X_1, \ldots, X_n$ est claire si l'on se réfère au paragraphe précédent, mais est ici masquée par le fait qu'on a identifié, par sa base canonique, k^n à son dual.

Dans la suite, on notera en général $g.p$ pour $(\tilde{\rho}(g))(p)$, en utilisant l'action . associée à la représentation $\tilde{\rho}$.

EXEMPLE : Reprenons l'exemple d'une opération à gauche d'un groupe G sur un ensemble fini, considérée comme cas particulier d'une représentation linéaire (cf. *supra*). Alors on voit facilement que $\tau.p = A_\tau.p = p(\mathbf{X}.(A_\tau^{-1})^t)$ est égal à $p(X_{\tau(1)}, \ldots, X_{\tau(n)})$. Vérifions-le pour l'exemple précédent, $n = 3$ et $\tau = (1\ 2\ 3)$: on a bien $\tau.p = p(X_2, X_3, X_1)$.

Action d'un groupe sur une k-algèbre. Représentation galoisienne d'un groupe

On appelle *action à gauche* du groupe G sur une k-algèbre A toute action à gauche . de G sur le k-espace vectoriel support de A telle que pour tout $g \in G$ et tout $(x, y) \in A^2$ on ait $g.(xy) = (g.x)(g.y)$.

De même que pour les actions sur un ensemble ou sur un espace vectoriel, la donnée d'une action à gauche de G sur une k-algèbre A équivaut ici à la donnée d'un morphisme ρ du groupe G vers le groupe $\mathrm{Aut}_k(A)$ des automorphismes de la k-algèbre A.

Dans le cas où A est un corps commutatif K, l'action à gauche . définit donc un morphisme du groupe ρ de G dans le groupe de Galois $\mathrm{Gal}(K : k)$ de l'extension de corps $K : k$ (c'est-à-dire le groupe des automorphismes de k-algèbre de K), et le groupe $G/\ker(\rho)$ est donc isomorphe à un sous-groupe de $\mathrm{Gal}(K : k)$. Donc si l'action est fidèle, alors $\mathrm{Gal}(K : k)$ a un sous-groupe isomorphe à G.

1.2 Invariants d'un groupe

1.2.1 Définitions

Soit k un corps commutatif et G un groupe.

Définition 1.1 *Soit $\rho : G \longrightarrow \mathbf{GL}_n(k)$ une représentation du groupe G dans k^n. On dit qu'un polynôme $p \in k[\mathbf{X}]$ (resp. une fraction $p \in k(\mathbf{X})$) est* un invariant de G, *ou encore un* G-invariant, *si et seulement si pour tout $g \in G$ on a $g.p = p$ (où $g.p = \tilde{\rho}(g)(p)$). On note $k[\mathbf{X}]^G$ (resp. $k(\mathbf{X})^G$) l'algèbre des invariants polynomiaux (resp. fractionnaires) de G.*
Si L est un sous-groupe de $\mathbf{GL}_n(k)$ contenant G, p est appelé un invariant primitif de G relatif à L, *ou encore un* G-invariant L-relatif, *si et seulement si $\mathcal{S}tab_L(P) = G$ (voir Prop. 3.1 pour une explication à cette terminologie).*

On notera souvent implicitement $k[\mathbf{X}]^G$ au lieu de $k[\mathbf{X}]^\rho$ quand la représentation ρ du groupe G sera évidente dans le contexte ; par exemple quand G est un sous-groupe de $\mathbf{GL}_n(k)$, ou encore quand

c'est un sous-groupe du groupe symétrique $\mathfrak{S}_n$ (auquel cas ρ est la représentation linéaire associée à la représentation par permutations, cf. le paragraphe 1.1).

Exemple 1.2 *Soit* $\mathbf{E} = (E_1, \ldots, E_n)$, *où* $E_i = \sum_{1 \leq j_1 < \ldots < j_i \leq n} \prod_{l=1}^{i} X_{j_l}$ *pour tout* $i \in \mathbb{N}_n^*$ *(polynômes symétriques élémentaires). Alors,* $k[\mathbf{X}]^{\mathfrak{S}_n} = k[\mathbf{E}]$ *et* $k(\mathbf{X})^{\mathfrak{S}_n} = k(\mathbf{E})$. *Plus généralement, si* L *est un produit* $\mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}$ *de groupes symétriques, avec* $\sum_{j=1}^{s} n_j = n$ *et chaque* $\mathfrak{S}_{n_j}$ *agissant sur les indéterminées* $X_{n_1+\ldots+n_{j-1}+k}$, $1 \leq k \leq n_j$, *alors* $k[\mathbf{X}]^L = k[\mathbf{E^{(1)}}, \ldots, \mathbf{E^{(s)}}]$ *et* $k(\mathbf{X})^L = k(\mathbf{E^{(1)}}, \ldots, \mathbf{E^{(s)}})$ *où pour tout* $j \in \mathbb{N}_s^*$, *on a noté* $\mathbf{E^{(j)}}$ *la famille* $(E_1^{(j)}, \ldots, E_{n_j}^{(j)})$ *des polynômes symétriques élémentaires en les variables* $X_{n_1+\ldots+n_{j-1}+k}$, $1 \leq k \leq n_j$ *(voir une preuve dans [34]).*

On verra une réciproque de l'Exemple 1.2 au Corollaire 4.3.

1.2.2 Propriétés

Proposition 1.3 *Pour tout sous-groupe fini* G *de* $\mathbf{GL}_n(k)$, $k(\mathbf{X})^G$ *est de degré de transcendance* n *sur* k, *et donc* $k[\mathbf{X}]^G$ *est dimension de Krull* n *sur* k.

Preuve – Cette proposition est bien connue, voir [62, Prop. 2.1.1] par exemple. □

Rappelons le résultat suivant, dont la première partie est due à Hilbert et la seconde à E. Noether :

Théorème 1.4 (Hilbert-Noether) *On suppose* $\mathrm{caract}(k) = 0$. *Pour tout sous-groupe réductif (ou en particulier fini)* G *de* $\mathbf{GL}_n(k)$, $k[\mathbf{X}]^G$ *est une* k*-algèbre finie. Si* G *est fini, elle est même engendrée par les* $\binom{n+|G|}{n}$ *polynômes* $\sum_{\sigma \in G} \sigma.m$ *où* m *décrit l'ensemble des monômes de degré inférieur ou égal à* $|G|$ *(borne de Noether).*

Proof – voir [62] par exemple. □

En caractéristique non-nulle, contentons-nous de citer [35] qui montre que le résultat reste valable dans ce cas en remplaçant la borne de Noether $|G|$ par $\max\{n, \frac{n(n-1)}{2}\}$, à condition que G soit un groupe de permutations. Signalons aussi une conjecture de G. Kemper, qui veut que la borne de Noether soit encore valable quand $\mathrm{caract}(k)$ est inférieur à $|G|$ et ne divise pas $|G|$ (pour le moment, ce n'est prouvé que quand G est un groupe résoluble).

$k[\mathbf{X}]^G$ est une k-algèbre graduée, dont les dimensions des composantes homogènes peuvent être calculées très facilement grâce au théorème suivant :

Théorème 1.5 (Molien) *Supposons* $\mathrm{caract}(k) = 0$. *Soit* G *un sous-groupe fini de* $\mathbf{GL}_n(k)$. *La série de Hilbert* $\mathcal{H}_G(z) = \sum_{d=0}^{+\infty} \dim k[\mathbf{X}]_d^G z^d \in \mathbb{Z}[[z]]$, *dont le coefficient d'indice* d *est la dimension sur* k *de la composante homogène de degré* d *de* $k[\mathbf{X}]^G$, *est le développement de la fraction rationnelle suivante :*

$$\mathcal{H}_G(z) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(Id - z\sigma)}$$

Preuve – voir [54]. □

Les chapitres 3 et 4 étudieront les structures des algèbres d'invariants $k(\mathbf{X})^G$ et $k[\mathbf{X}]^G$ respectivement, en mettant en valeur le parallèle entre les deux.

Chapitre 2

Expression des invariants dans une base de k-module

Ici, il suffit que k soit un anneau intègre commutatif de caractéristique nulle. L'objet de ce paragraphe est d'écrire les invariants d'un groupe fini $L \subset \mathfrak{S}_n$ en fonction des éléments d'une base du k-module $k[\mathbf{X}]^L$, et de permettre les calculs algébriques sur les invariants dans cette base.

Plus précisément, le groupe $L \subset \mathfrak{S}_n$ opère à gauche sur $\mathbb{N}^n$ par permutation des éléments des n-uplet. Soit $\Omega \subset \mathbb{N}^n$ une transversale pour cette action, c'est-à-dire une partie de $\mathbb{N}^n$ qui contient un et un seul élément de chaque orbite, et $\mathcal{P}_\Omega$ la projection de $\mathbb{N}^n$ sur Ω qui a tout n-uplet α associe l'élément de Ω qui appartient à la même orbite que α. Nous définissons pour tout n-uplet $\alpha = (\alpha_1, \ldots, \alpha_n)$ les polynômes suivants :

– La *forme monomiale associée à α relativement à L* :

$$M_\alpha^L = \sum_{\gamma \in L.\alpha} \mathbf{X}^\gamma$$

– La *forme monomiale augmentée associée à α relativement à L*

$$A_\alpha^L = \sum_{\sigma \in L} \mathbf{X}^{\sigma.\alpha} \quad .$$

On a donc la relation suivante entre ces deux objets :

$$A_\alpha^L = |\mathcal{S}tab_L(\alpha)|.M_\alpha^L \quad .$$

Il est alors clair que $(M_\alpha^L)_{\alpha \in \Omega}$ est une k-base de $k[\mathbf{X}]^L$. Notons que le nombre de polynômes M_α^L d'un degré d peut être calculé par la formule de Molien (Théorème 1.5).

On veut être capable d'effectuer les opérations de la k-algèbre $k[\mathbf{X}]^L$, ses éléments étant décomposés dans cette base.

Le premier problème est le test d'égalité. Il est résolu si l'on est capable de tester si $M_\alpha^L = M_{\alpha'}^L$ pour deux n-uplets α et α' donnés. Cela équivaut à $\mathcal{P}_\Omega(\alpha) = \mathcal{P}_\Omega(\alpha')$ donc le problème est résolu si l'on sait évaluer la projection $\mathcal{P}_\Omega$ efficacement. On sait alors effectuer facilement les opérations de la structure de k-espace vectoriel de $k[\mathbf{X}]^L$. Reste la multiplication, qui se ramène par linéarité au produit de deux éléments de la base et fait l'objet du paragraphe 2.1.

Une première partie traite donc du problème de la multiplication de deux éléments de la base $(M_\alpha^L)_{\alpha \in \Omega}$. Suit le cas particulier des polynômes symétriques qui est particulièrement agréable, puis son implantation

en AXIOM (domaine `PolynomesSymetriques`). Nous n'avons pas encore implanté le cas général car il nécessite des calculs sur les groupes (pour calculer Ω, $E(\alpha,\beta)$ et $\mathcal{P}_\Omega$) que ne permet pas AXIOM ; et pour le moment les passerelles entre AXIOM et les langages adaptés aux groupes comme GAP, qui permettraient d'appeler les fonctions d'un langage depuis l'autre, sont inexistantes.

2.1 Produit de deux éléments de la base

Soit α et β deux n-uplets d'entiers positifs ou nuls. Calculons le produit des formes monomiales augmentées associées :

$$\begin{aligned} A^L_\alpha.A^L_\beta &= (\sum_{\sigma\in L}\mathbf{X}^{\sigma.\alpha}).(\sum_{\tau\in L}\mathbf{X}^{\sigma.\beta}) \\ &= \sum_{\sigma,\tau\in L}\mathbf{X}^{\sigma.\alpha+\tau.\beta} \\ &= \sum_{\sigma\in L}(\sum_{\tau\in L}\mathbf{X}^{\sigma.(\alpha+\sigma^{-1}.\tau.\beta)}) \\ &= \sum_{\sigma\in L}(\sum_{\tau'\in L}\mathbf{X}^{\sigma.(\alpha+\tau'.\beta)}) \\ &= \sum_{\tau\in L}A^L_{\alpha+\tau.\beta} \end{aligned}$$

donc pour les formes monomiales on a, en se plaçant dans le corps des fractions de k :

$$\begin{aligned} M^L_\alpha.M^L_\beta &= \frac{1}{|\mathcal{S}tab_L(\alpha)|.|\mathcal{S}tab_L(\beta)|}.\sum_{\tau\in L}|\mathcal{S}tab_L(\alpha+\tau.\beta)|.M^L_{\alpha+\tau.\beta} \\ &= \frac{1}{|\mathcal{S}tab_L(\alpha)|}.\sum_{\gamma\in L.\beta}|\mathcal{S}tab_L(\alpha+\gamma)|.M^L_{\alpha+\gamma} \quad . \end{aligned}$$

L'inconvénient de cette formule est qu'elle fait intervenir des calculs sur les rationnels, car $|\mathcal{S}tab_L(\alpha)|$ ne divise pas en général $|\mathcal{S}tab_L(\alpha+\gamma)|$. On va donc regrouper les termes afin de se ramener à des manipulations d'entiers.

Faisons opérer le groupe $\mathcal{S}tab_L(\alpha)$ sur l'ensemble $L.\beta$ par restriction. Le stabilisateur d'un élément γ s'écrit :

$$\mathcal{S}tab_{\mathcal{S}tab_L(\alpha)}(\gamma) = \mathcal{S}tab_L(\alpha)\cap\mathcal{S}tab_L(\gamma) = \mathcal{S}tab_L(\alpha\times\gamma)$$

où $\alpha\times\gamma$ désigne le n-uplet $((\alpha_1,\gamma_1),\ldots,(\alpha_n,\gamma_n))\in(\mathbb{N}^2)^n$. L'orbite de γ sous l'action de $\mathcal{S}tab_L(\alpha)$ a donc pour cardinal

$$|\mathcal{O}rb_{\mathcal{S}tab_L(\alpha)}(\gamma)| = \frac{|\mathcal{S}tab_L(\alpha)|}{|\mathcal{S}tab_L(\alpha\times\gamma)|} \quad .$$

Or les éléments γ' de l'orbite de γ sous l'action de $\mathcal{S}tab_L(\alpha)$ vérifient $M^L_{\alpha+\gamma} = M^L_{\alpha+\gamma'}$, donc on peut réécrire la formule du produit sous la forme suivante, en regroupant les termes selon la partition $\{P_1,\ldots,P_u\}$ de $L.\beta$ donnée par les orbites sous l'action du groupe $\mathcal{S}tab_L(\alpha)$:

$$M^L_\alpha.M^L_\beta = \sum_{\gamma\in E(\alpha,\beta)}\frac{|\mathcal{S}tab_L(\alpha+\gamma)|}{|\mathcal{S}tab_L(\alpha\times\gamma)|}.M^L_{\alpha+\gamma} \quad ,$$

où $E(\alpha,\beta)$ désigne un sous-ensemble de $L.\beta$ obtenu en gardant un seul élément par orbite P_i pour tout $i\in\{1,\ldots,u\}$;

Remarquons enfin que le cardinal de $\mathcal{S}tab_L(\alpha+\gamma)$ est divisible par celui de son sous-groupe $\mathcal{S}tab_L(\alpha \times \gamma)$. On a donc montré la proposition suivante, qui généralise [66, paragraphe 4.1.1] :

Proposition 2.1 *Si α et β sont deux n-uplets, on a la formule suivante permettant d'exprimer le produit des formes monomiales M^L_α et M^L_β comme combinaison linéaire à coefficients entiers de formes monomiales :*

$$M^L_\alpha . M^L_\beta = \sum_{\gamma \in E(\alpha,\beta)} \frac{|\mathcal{S}tab_L(\alpha+\gamma)|}{|\mathcal{S}tab_L(\alpha \times \gamma)|} . M^L_{\alpha+\gamma},$$

où $E(\alpha,\beta)$ désigne un sous-ensemble de $L.\beta$ transverse à l'action de $\mathcal{S}tab_L(\alpha)$ (c'est-à-dire contenant un et un seul élément de chaque orbite sous l'action de $\mathcal{S}tab_L(\alpha)$).

Remarque 2.2 *Pour obtenir une formule faisant intervenir des coefficients entiers, on a regroupé certains termes tels que $M^L_{\alpha+\gamma} = M^L_{\alpha+\gamma'}$, mais pas tous ; par exemple pour $n = 4$, $L = \mathfrak{S}_4$, $\alpha = (3,3,2,1)$, $\gamma = (2,2,1,3)$ et $\gamma' = (2,1,3,2)$, les n-uplets $\alpha+\gamma = (5,5,3,4)$ et $\alpha+\gamma' = (5,4,5,3)$ définissent la même forme monomiale, et pourtant ils ne sont pas regroupés ensemble, puisque γ' s'écrit $\sigma.\gamma$ avec un $\sigma \in \mathfrak{S}_n \setminus \mathcal{S}tab_{\mathfrak{S}_n}(\alpha)$.*

2.2 Cas particulier $L = \mathfrak{S}_n$ (polynômes symétriques)

Dans ce cas, il est facile de reconnaître si deux n-uplets α et α' définissent la même forme monomiale (*i.e.* appartiennent à la même orbite sous L) : il suffit de réordonner chacun de ces n-uplets dans l'ordre décroissant par exemple, puis de tester l'égalité. Pour Ω, on peut choisir l'ensemble des n-uplets décroissants d'entiers naturels. La projection $\mathcal{P}_\Omega$ est alors donnée par un simple algorithme de tri, donc de complexité $O(n\mathrm{Log}\, n)$.

On peut alors, dans la Proposition 2.1, si $(\alpha,\beta) \in \Omega^2$, prendre $E(\alpha,\beta)$ égal à l'ensemble des $\gamma \in L.\beta$ tels que $\alpha \times \gamma$ soit une suite décroissante pour l'ordre lexicographique : en effet, si l'on note k_1,...,k_r (avec $k_1 + \ldots + k_r = n$) les entiers définis par

$$\alpha_1 = \alpha_2 = \ldots = \alpha_{k_1} > \alpha_{k_1+1} = \ldots = \alpha_{k_1+k_2} > \ldots > \alpha_{k_1+\ldots+k_{r-1}+1} = \ldots = \alpha_n$$

alors $\mathcal{S}tab_L(\alpha) = \mathfrak{S}_{k_1} \times \ldots \times \mathfrak{S}_{k_r}$, et $E(\alpha,\beta)$ est l'ensemble des $\gamma \in L.\beta$ tels que $\forall i \in \{1,\ldots,r-1\}, \gamma_{k_1+\ldots+k_i+1} \geq \cdots \geq \gamma_{k_1+\ldots+k_{i+1}}$. Il y a donc bien un et un seul élément par orbite sous l'action de $\mathfrak{S}_{k_1} \times \ldots \times \mathfrak{S}_{k_r}$

Remarquons que si Ω et les ensembles $E(\alpha,\beta)$ sont choisis comme ci-dessus alors, dans la Proposition 2.1, pour tout $(\alpha,\beta) \in \Omega^2$ et $\gamma \in E(\alpha,\beta)$, $\alpha+\gamma$ appartient encore à Ω donc il n'est pas nécessaire d'appliquer la projection $\mathcal{P}_\Omega$ (c'est-à-dire l'algorithme de tri) à $\alpha+\gamma$.

Remarque 2.3 *Le cas $L = \mathfrak{S}_n$ se généralise aisément au cas où L est un produit $L = \mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_r}$ de groupes symétriques : on se ramène alors à un algorithme de tri séparément sur chaque paquet d'indéterminées.*

Ce cas a été implanté par A. Valibouze dans le module SYM [67] qu'elle a créé, et qui est maintenant intégré aux bibliothèques du langage MACSYMA.

2.3 Implantation du domaine `PolynomesSymetriques`

Nous présentons dans ce paragraphe l'implantation en AXIOM du cas $L = \mathfrak{S}_n$, dans un domaine appelé `PolynomesSymetriques`. Nous rappelons qu'AXIOM distingue trois niveaux de structuration :

- le niveau *paquetage*, ou sont simplement implantées des fonctions faisant intervenir des types prédéfinis (par exemple le type `Polynomial(Fraction Integer)` : polynômes à coefficients dans $\mathbb{Q}$).

- le niveau *domaine*, qui permet de définir de nouveaux types. `PolynomesSymetriques` est un domaine, donc permettra de construire de nouveaux types, par exemple `PolynomesSymetriques(4, Complex Integer, 0, [], [X1,X2,X3,X4])` sera le domaine des polynômes symétriques sur 4 indéterminées et à coefficients dans les entiers de Gauss. Un domaine permet de définir la représentation en machine du type.

- le niveau *catégorie*, qui permet de grouper des domaines ayant des propriétés communes. Par exemple, l'élévation à une puissance m d'une grandeur mathématique pourrait être implantée une fois pour toutes dans la catégorie `Ring`, à partir d'une multiplication qui est elle-même implantée de façon différentes dans les différents domaines qui héritent de la catégorie `Ring`. L'algorithme est en effet le même pour élever un entier ou un polynôme ou une matrice à une puissance m, une fois qu'on sait effectuer les multiplications d'entiers, de polynômes ou de matrices.

Nous avons donc choisi de faire de `PolynomesSymetriques` un domaine. Nous allons préciser la représentation interne des polynômes en machine qu'il utilise.

On adopte la base $(M_\alpha)_{\alpha\in\Omega}$ de $k[\mathbf{X}]^{\mathfrak{S}_n}$, où Ω est l'ensemble des suites décroissantes d'entiers naturels et où $M_\alpha = M_\alpha^{\mathfrak{S}_n}$. On représente l'élément M_α par $\mathcal{P}_\Omega$, où la projection $\mathcal{P}_\Omega$ est un algorithme de tri. Nous représentons en machine `PolynomesSymetriques` comme le module libre (domaine `FreeModule`, qui existe déjà en AXIOM) construit sur le domaine `Partition` (c'est-à-dire l'ensemble des suites décroissantes d'entiers naturels, qui existe aussi déjà en AXIOM), qui hérite lui-même de la catégorie `Monoid` (Monoïde). `PolynomesSymetriques` est donc défini comme le module libre sur le monoïde Ω.

Les tests d'égalité de deux éléments M_α et $M_{\alpha'}$ reviennent donc simplement à tester l'égalité des deux n-uplets $\mathcal{P}_\Omega(\alpha)$ et $\mathcal{P}_\Omega(\alpha')$. L'implantation de la structure de k-module de $k[\mathbf{X}]^{\mathfrak{S}_n}$ est déjà prédéfinie par la représentation machine utilisée (module libre sur Ω), et pour la multiplication on utilise la Proposition 2.1 avec les ensembles $E(\alpha,\beta)$ du paragraphe 2.2.

`PolynomesSymetriques` prend en argument l'entier n, l'anneau k, deux arguments que nous explicitons *infra* , puis la liste $\mathbf{X} = (X_1, \ldots, X_n)$ des indéterminées.

Voici un exemple d'application, avec $n = 3$ et $k = \mathbb{Z}$.

```
(1) ->d := PolynomesSymetriques(3,Integer,0,[],[X1,X2,X3])
   (1)  PolynomesSymetriques(3,Integer,0,[],[X1,X2,X3])
                                                        Type: Domain

(2) ->a := makeMonom([3,2,1])$d
   (2)  (3 2 1)
       Type: PolynomesSymetriques(3,Integer,0,[],[X1,X2,X3])

(3) ->b := makeMonom([7,3,1])$d
   (3)  (7 3 1)
       Type: PolynomesSymetriques(3,Integer,0,[],[X1,X2,X3])

(4) ->a*b
                                          2
   (4)  (10 5 2) + (10 4 3) + (9 6 2) + 2(9 4 ) + (8 6 3) + (8 5 4)
       Type: PolynomesSymetriques(3,Integer,0,[],[X1,X2,X3])
                          Time: 0.02 (IN) + 0.02 (EV) + 0.05 (OT) = 0.08 sec
```

Sur cet exemple, on a fait le produit des deux polynômes $a = M_{(3,2,1)} = X_1^3X_2^2X_3 + \ldots$ (5 autres termes obtenus en permutant les indéterminées) et $b = M_{(7,3,1)}$, et on a obtenu pour résultat $ab = M_{(10,5,2)} + M_{(10,4,3)} + M_{(9,6,2)} + 2M_{(9,4,4)} + M_{(8,6,3)} + M_{(8,5,4)}$.

Autres fonctions du domaine `PolynomesSymetriques:` On sait que la k-algèbre $k[\mathbf{X}]^{\mathfrak{S}_n}$ est engendré par les polynômes symétriques élémentaires $E_1, \ldots, E_n$, ou aussi, si les entiers non nuls sont inversibles dans k, par les n premiers polynômes de Newton $P_i = M_{(i,0,\ldots,0)} = \sum_{j=1}^{n} X_j^i$, $1 \leq i \leq n$. Nous avons implanté dans le domaine `PolynomesSymetriques` trois algorithmes différents permettant d'exprimer un polynôme symétrique p dans l'une ou l'autre de ces bases de transcendance pure de k-algèbre.

L'un de ces algorithmes utilise un résultat du type formule d'inversion Moebius, mais concernant des polynômes (voir [47, 5]), qui permet d'exprimer un polynôme symétrique en fonction des puissances de Newton.

Nous présentons ci-après celui de ces trois algorithmes qui est le plus efficace en moyenne: il est dû à A. Valibouze (voir [66, Paragraphe 5.2.1] et [67] pour son implantation) et implanté en AXIOM par nos soins, marche sous l'hypothèse que les entiers non nuls de k soient inversibles, et consiste dans un premier temps à exprimer le polynôme $p \in k[\mathbf{X}]^{\mathfrak{S}_n}$ en fonction des polynômes de Newton en nombre plus élevé que n (borné seulement par le degré de p), puis dans un second temps à utiliser les formules de Newton pour se ramener aux n premiers polynômes de Newton ou aux n polynômes symétriques élémentaires.

L'algorithme est fondé sur la proposition suivante :

Proposition 2.4 (Valibouze) *Soit α un n-uplet décroissant d'entiers naturels et $\beta = (\alpha_2, \ldots, \alpha_n, 0)$. Soit μ le nombre d'éléments de α qui sont égaux à α_1. Soit r le nombre de valeurs distinctes et non nulles parmi les éléments de β, et soit $(l_1, \ldots, l_r)$ la famille définie par: $l_1 = 2$ (si $r \geq 1$) et*

$$\alpha_{l_1} = \alpha_{l_1+1} = \ldots = \alpha_{l_2-1} > \alpha_{l_2} = \ldots > \ldots = \alpha_{l_j-1} > \alpha_{l_j} = \ldots > \ldots = \alpha_{l_r-1} > \alpha_{l_r} > 0.$$

Alors

$$\mu M_\alpha = P_{\alpha_1} M_\beta - \sum_{j=1}^{r} M_{(\alpha_1+\alpha_{l_j}, \alpha_2, \ldots, \alpha_{l_j-1}, \alpha_{l_j+1}, \ldots, \alpha_n, 0)}.$$

Preuve – Cela résulte de l'application de la formule du produit (Proposition 2.1) en prenant, avec les notations de cette proposition, pour n-uplet α le n-uplet β d'ici et pour n-uplet β le n-uplet $(\alpha_1, 0, \ldots, 0)$ d'ici. □

L'application de la Proposition 2.4 par récurrence décroissante sur le nombre d'éléments non nuls dans le n-uplet α permet d'exprimer un polynôme $p \in k[\mathbf{X}]^n$ en fonction des polynômes de Newton P_i, i variant de 1 au degré de p.

Voici un exemple d'application avec $n = 3$, $k = \mathbb{Q}$:

```
(1) ->d := PolynomesSymetriques(3,Integer,14,[E1,E2,E3],[X1,X2,X3])
   (1)  PolynomesSymetriques(3,Fraction Integer,14,[E1,E2,E3],[X1,X2,X3])
                                                          Type: Domain

(2) ->a := (makeMonom([3,3,1])$d)^2
          2          2
   (2)  (6 2) + 2(6 4 )
      Type: PolynomesSymetriques(3,Fraction Integer,14,[E1,E2,E3],[X1,X2,X3])

(3) ->symToElem(a)$d
           4  2      3  2       2  4
   (3)  4E3 E1  - 4E3 E2 E1 + E3 E2
                    Type: MultivariatePolynomial([E1,E2,E3],Fraction Integer)
```

Les troisième et quatrième arguments du domaine `PolynomesSymetriques` sont respectivement le degré maximal des polynômes p (on se le donne afin de précalculer les formules de Newton jusqu'à ce degré),

ici 14, et la liste des variables représentant les polynômes symétriques élémentaires, ici $[E1, E2, E3]$. On appliqué la fonction `symToElem` sur le polynôme $(M_{(3,3,1)})^2 = (X_1^3X_2^3X_3 + X_1^3X_3^3X_2 + X_2^3X_3^3X_1)^2 = M_{(6,6,2)} + 2M_{(6,4,4)}$ et on a obtenu : $(M_{(3,3,1)})^2 = 4E_3^4E_1^2 - 4E_3^3E_2^2E_1 + E_3^2E_2^4$, où $E_1 = X_1 + X_2 + X_3$, $E_2 = X_1X_2 + X_2X_3 + X_3X_2$ et $E_3 = X_1X_2X_3$.

On peut aussi bien sûr appliquer cet algorithme pour spécialiser le polynôme p connaissant les valeurs spécialisées par exemple des polynômes symétriques élémentaires. On utilise alors le même algorithme mais en l'appliquant à des valeurs numériques au lieu de l'appliquer à des indéterminées. Voici sur exemple l'exemple précédent :

```
(4) ->specialiseParElem(a,[3,-1,2])$d
   (4)  484
                                                    Type: Fraction Integer
```

On a remplacé (E_1, E_2, E_3) par $(3, -1, 2)$ et calculé la valeur que prend a pour cette spécialisation. Bien évidemment, on a spécialisé d'abord et effectué les calculs ensuite ; par exemple les formules de Newton (à un ordre majoré par $14 = \deg(a)$) ont été calculées directement sur les valeurs $(3, -1, 2)$ et non génériquement ; et la Proposition 2.4 elle-même a été appliquée (plusieurs fois, par récurrence) directement sur les valeurs spécialisées.

Une autre fonction, `specialiseParPui`, permet aussi de spécialiser p en se donnant la spécialisation de (P_1, P_2, P_3) au lieu de celle de (E_1, E_2, E_3).

Le domaine `PolynomesSymetriques` contient nombreuses autres fonctions : formules de Newton, conversions dans tous les sens possibles entre polynômes symétrique développé, ou exprimé dans la base $(M_\alpha)_{\alpha\in\Omega}$, ou en fonction des polynômes symétriques élémentaires ou des polynômes de Newton, projection de Reynolds de $k[\mathbf{X}]$ sur $k[\mathbf{X}]^{\mathfrak{S}_n}$, etc. Il est disponible sur demande par courrier électronique à

`colin@gage.polytechnique.fr`

ou directement par ftp à l'adresse

`ftp://medicis.polytechnique.fr/pub/publications/colin/axiom`

2.4 Remarque sur l'implantation dans le cas général

Comme nous l'avons fait remarquer plus haut, l'implantation du cas général (L sous-groupe quelconque de $\mathfrak{S}_n$) butte sur le calcul effectif de Ω, $E(\alpha, \beta)$ et $\mathcal{P}_\Omega$, que ne permet pas facilement AXIOM pour le moment. On peut cependant, en attendant, contourner le problème en testant l'égalité $M_\alpha = M_{\alpha'}$ non directement par l'appartenance de α et α' à la même orbite sous L, mais indirectement grâce à la proposition suivante :

Proposition 2.5 *Soit $(I_1, \ldots, I_r)$ une famille génératrice fixée de la k-algèbre $k[\mathbf{X}]^L$. Soit deux n-uplets d'entiers naturels $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ et $\alpha' = (\alpha'_1, \ldots, \alpha'_n) \in \mathbb{N}^n$. Alors α' appartient à l'orbite $L.\alpha$ si et seulement si $I_i(\alpha) = I_i(\alpha')$ (évaluations de I_i en α et α') pour tout i tel que $1 \leq i \leq r$.*

Preuve – Si $I_i(\alpha) = I_i(\alpha')$ pour tout i tel que $1 \leq i \leq r$, alors le polynôme

$$p = \prod_{\sigma\in L} \sum_{i=1}^{n} (X_i - \alpha_{\sigma(i)})^2$$

appartient à $k[\mathbf{X}]^L$ donc s'exprime en fonction de $I_1, \ldots, I_r$, d'où $p(\alpha') = p(\alpha)$. Or, $p(\alpha) = 0$, donc $p(\alpha') = 0$ et il existe donc $\sigma \in L$ tel que $\alpha' = \sigma.\alpha$. La réciproque est triviale. □

Le test d'égalité entre M_α et $M_{\alpha'}$ est donc ramené aux r tests d'égalité $I_i(\alpha) = I_i(\alpha')$, $1 \leq i \leq r$. Notons qu'une telle famille génératrice finie existe toujours (Th. 1.4), et qu'une famille assez réduite est donnée par la propriété de Cohen-Macaulay (voir Th. 4.4).

Chapitre 3

Théorie des corps et invariants fractionnaires

Dans tout ce chapitre, k est un corps commutatif quelconque (pas d'hypothèse sur sa caractéristique). Ce chapitre établit une description des invariants qui est parallèle à celle du chapitre 4. Ici, nous engendrons l'algèbre des invariants $k(\mathbf{X})^H$, où H est un sous-groupe finie de $\mathbf{GL}_n(k)$, tandis qu'au chapitre 4 nous engendrons l'algèbre $k[\mathbf{X}]^H$. Dans les deux cas, la famille génératrice est constituée d'une base de transcendance et d'une base de module libre sur la partie transcendante. L'outil est la théorie des corps dans ce chapitre et la propriété de Cohen-Macaulay dans le chapitre 4. Et dans les deux cas, nous nous intéressons aux algorithmes permettant d'une part de trouver une telle famille génératrice, d'autre part d'exprimer ensuite un invariant donné en fonction des éléments de cette famille.

3.1 Un invariant primitif est un élément primitif

Le résultat suivant est bien connu, en tout cas pour les groupes de permutations (voir [68]) :

Théorème 3.1 *Ici, k est un corps commutatif quelconque. Soit H et L deux sous-groupes finis du groupe linéaire $\mathbf{GL}_n(k)$, tels que $H \subset L$. Soit Θ un invariant primitif de H relativement à L (cf. Définition 1.1). Alors, on a $k(\mathbf{X})^H = k(\mathbf{X})^L[\Theta]$, et $(1, \Theta, \ldots, \Theta^{e-1})$ est une base du $k(\mathbf{X})^L$-espace vectoriel $k(\mathbf{X})^H$, où $e = [L : H]$.*

Preuve – D'après [13, A V.64 Théorème 3.a], comme L est fini et opère sur $k(\mathbf{X})$ fidèlement et par automorphismes de corps, $k(\mathbf{X}) : k(\mathbf{X})^L$ est une extension galoisienne et a pour groupe de Galois L. La sous-extension $k(\mathbf{X}) : k(\mathbf{X})^L[\Theta]$ est donc aussi galoisienne, et son groupe de Galois est constitué des automorphismes de $k(\mathbf{X})$ qui laissent invariants non seulement tous les points de $k(\mathbf{X})^L$ mais aussi Θ. Ce groupe est donc $\mathcal{S}tab_L(\Theta)$, qui est H par hypothèse, et qui est aussi le groupe de Galois de l'extension $k(\mathbf{X}) : k(\mathbf{X})^H$. D'après le théorème de dualité de Galois, on en déduit que $k(\mathbf{X})^L[\Theta] = k(\mathbf{X})^H$. Le résultat sur la base en résulte, car Θ est alors un élément primitif de l'extension $k(\mathbf{X})^H : k(\mathbf{X})^L$, qui est de degré $[L : H]$. □

Exemple 3.2 *Soit $n = 3$, $\Theta = X_1 + X_2 \in k[X_1, X_2, X_3]$ et $\Psi = X_1X_2 \in k[X_1, X_2, X_3]$. On constate que $\mathcal{S}tab_{\mathfrak{S}_3}(\Theta) = \mathcal{S}tab_{\mathfrak{S}_3}(\Psi) = \{Id, (1\ 2)\} \simeq \mathfrak{S}_2$. D'après le Théorème 3.1, on en conclut que Ψ appartient à $k(\mathbf{X})^{\mathfrak{S}_3}[\Theta]$ et que Θ appartient à $k(\mathbf{X})^{\mathfrak{S}_3}[\Psi]$. Et en effet, on peut vérifier que $\Psi = \Theta^2 - E_1\Theta + E_2$ et que $\Theta = \frac{\Psi(E_2 - \Psi)}{E_3}$, où E_1, E_2 et E_3 désignent les polynômes symétriques élémentaires en X_1, X_2, X_3.*

Le but de ce chapitre est de donner une version effective du théorème 3.1, c'est-à-dire de fournir des algorithmes permettant d'exprimer effectivement un invariant en fonction d'un élément primitif, comme dans l'exemple ci-dessus.

Remarquons qu'un H-invariant primitif L-relatif existe toujours car $k(\mathbf{X})^H : k(\mathbf{X})^L$ est séparable comme sous-extension de l'extension galoisienne $k(\mathbf{X}) : k(\mathbf{X})^L$. De plus, quand $L \subset \mathfrak{S}_n$, un H-invariant primitif L-relatif Θ simple peut être calculé, grâce à un algorithme de K. Girstmair (voir [29]), qui a été implanté en AXIOM (voir [37]) par I. Abdeljaouad.

$\star$

Remarquons que lorsque $k(\mathbf{X})^L$ est une extension pure de k, c'est-à-dire quand on peut écrire $k(\mathbf{X})^L = k(\Pi_1, \ldots, \Pi_n)$, on a alors une décomposition analogue à la décomposition de Hironaka du chapitre 4 :

$$k(\mathbf{X})^H = \bigoplus_{i=0}^{e-1} k(\Pi_1, \ldots, \Pi_n)\Theta^i \ . \tag{3.1}$$

Problème de Noether : Étant donné un sous-groupe fini L de $\mathbf{GL}_n(k)$, la question «le corps des invariants $k(\mathbf{X})^L$ est-il une extension transcendante pure de k» est connue sous le nom de *problème de Noether*. C'est à partir du problème inverse de la théorie de Galois qu'Emmy Noether s'est posée le problème auquel son nom est resté attaché. En effet, un groupe de permutations qui satisfait le problème de Noether peut s'écrire d'une infinité de manières comme groupe de Galois d'un polynôme sur $\mathbb{Q}$, et même de façon paramétrisable (c'est le *critère de Noether*, voir [51, page 5]).

Le problème de Noether a été étudié récemment dans [38]. Nous revenons sur un cas particulier de ce problème dans le chapitre 5.

On ne connaît pas de condition simple au problème de Noether qui soit analogue au théorème de Chevalley pour les invariants polynomiaux (voir Théorème 4.2 et [16]). Bien sûr, les conditions du théorème de Chevalley impliquent une réponse affirmative au problème de Noether, mais la réciproque est très loin d'être vrai. Les contrexemples ne manquent pas ; en voici un :

Proposition 3.3 *On a $k(X_1, X_2, X_3, X_4)^{\mathfrak{D}_4} = k(E_1, E_3, E_4, I)$, où $\mathfrak{D}_4$ désigne le sous-groupe diédral de $\mathfrak{S}_4$ engendré par (1 2) et (1 3 2 4), où $I = X_1X_2 + X_3X_4$ et où $E_1, \ldots, E_4$ désignent les polynômes symétriques élémentaires en $X_1, \ldots, X_4$.*

Preuve – D'après le Théorème 3.1, $k(\mathbf{X})^{\mathcal{D}_4} = k(\mathbf{X})^{\mathfrak{S}_4}(I) = k(E_1, E_2, E_3, E_4)(I)$. Il suffit donc de prouver que $E_2 \in k(E_1, E_3, E_4, I)$. Or, si l'on calcule le polynôme minimal de I sur $k(\mathbf{X})^{\mathfrak{S}_4}$, on obtient $I^3 - E_2I^2 + (E_1E_3 - 4E_4)I + 4E_2E_4 - E_3^2 - E_1^2E_4 = 0$, d'où $E_2 = I + \frac{IE_1E_3 - E_3^2 - E_1^2E_4}{I^2 - 4E_4}$. Une autre base pure de $k(\mathbf{X})^{\mathcal{D}_4}$ est donnée aussi dans [38, Paragraphe 2.4.2]. □

Ainsi, $k(\mathbf{X})^{\mathfrak{D}_4}$ est engendré par 4 polynômes homogènes algébriquement indépendants mais ce n'est pas le cas de $k[\mathbf{X}]^{\mathfrak{D}_4}$, car $\mathfrak{D}_4$ ne satisfait pas les hypothèses du Théorème 4.2.

3.2 Un résultat de Lagrange

Le résultat suivant est dû à Lagrange, qui le démontra dans [44], et fut repris et formalisé comme suit dans [7, Théorème 4.3]. Il précise le théorème 3.1 dans le cas où $L = \mathfrak{S}_n$. Nous en donnons une preuve plus simple et dans un cadre plus général à la Remarque 3.11.

Théorème 3.4 (de Lagrange) *Soit H un sous-groupe de $\mathfrak{S}_n$, $\Theta \in k[\mathbf{X}]^H$ un invariant primitif de H, et $\Theta_1 = \sigma_1.\Theta = \Theta, \Theta_2 = \sigma_2.\Theta, \ldots, \Theta_e = \sigma_e.\Theta$ où $(\sigma_1 = Id, \sigma_2, \ldots, \sigma_e)$ est une transversale de H dans*

$\mathfrak{S}_n$ et $e = [\mathfrak{S}_n : H]$ (c'est-à-dire que $\{\Theta_1, \Theta_2, \ldots, \Theta_e\}$ est l'orbite $\mathfrak{S}_n.\Theta$ de Θ sous l'action de $\mathfrak{S}_n$). Alors on a :

$$k[\mathbf{X}]^H \subset \frac{1}{\Delta_\Theta} k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta]$$

où $\Delta_\Theta = \prod_{1 \leq i < j \leq e} (\Theta_i - \Theta_j)^2 \in k[\mathbf{X}]^{\mathfrak{S}_n}$.

Remarquons que Δ_Θ est le discriminant de la résolvante de Lagrange $\mathcal{L}_\Theta$ (voir Définition 6.1).

Preuve – (d'après [44] et [7]). Soit $P \in k[\mathbf{X}]^H$, et $P_i = \sigma_i.P_i$ pour $1 \leq i \leq e$ ($P_1 = P$). Alors pour tout $i \in \{0, \ldots, e-1\}$, le polynôme $Q_i = \sum_{j=1}^{e} P_j \Theta_j^i$ appartient à $k[\mathbf{X}]^{\mathfrak{S}_n}$, et $(P_1, \ldots, P_e)$ est solution du système linéaire suivant (sur le corps $k(\mathbf{X})$) :

$$\forall i \in \{0, \ldots, e-1\},\ \Theta_1^i P_1 + \ldots + \Theta_e^i P_e = Q_i$$

qui est un système de Cramer car son déterminant est $\delta_\Theta = \prod_{1 \leq i < j \leq e} (\Theta_i - \Theta_j)$ (déterminant de Vandermonde), non nul. Comme $\Delta_\Theta = \delta_\Theta^2$, on a donc $P = \frac{\delta_\psi \mathcal{D}}{\Delta_\Theta}$, où

$$\mathcal{D} = \begin{vmatrix} Q_0 & 1 & \ldots & 1 \\ Q_1 & \Theta_2 & \ldots & \Theta_e \\ \vdots & \vdots & & \vdots \\ Q_{e-1} & \Theta_2^{e-1} & \ldots & \Theta_e^{e-1} \end{vmatrix}$$

On remarque que $\delta_\Theta \mathcal{D}$ peut s'écrire $R(\Theta_2, \ldots, \Theta_e)$ avec $R \in (k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta])[T_2, \ldots, T_e]^{\mathfrak{S}_{e-1}}$. Or, les polynômes symétriques élémentaires en $\Theta_2, \ldots, \Theta_e$ appartiennent tous à $k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta]$: en effet, ce sont au signe près les coefficients du polynôme $\prod_{i=2}^{e} (T - \Theta_i)$, qui est le quotient pour la division euclidienne dans l'anneau $(k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta])[T]$ de $\mathcal{L}_\Theta = \prod_{i=1}^{e} (T - \Theta_i) \in k[\mathbf{X}]^{\mathfrak{S}_n}$ par $T - \Theta$. Or, d'après le théorème fondamental sur les polynômes symétriques, $R(\Theta_2, \ldots, \Theta_e)$ s'exprime comme polynôme à coefficients dans $k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta]$ en ces polynômes symétriques élémentaires, donc appartient lui-même à $k[\mathbf{X}]^{\mathfrak{S}_n}[\Theta]$, d'où le résultat. □

L'inconvénient de la preuve de Lagrange — qui est cependant constructive — est qu'elle permet relativement difficilement d'exprimer en pratique un invariant P de H en fonction de Θ. De plus, si l'on veut spécialiser les polynômes symétriques qui apparaissent, on est obligé de calculer d'abord l'expression générique

$$P = \frac{C_0 + C_1 \Theta + \ldots + C_{e-1} \Theta^{e-1}}{\Delta_\Theta}$$

puis de spécialiser après coup seulement les polynômes symétriques Δ_Θ et C_i qui apparaissent.

Nous allons voir dans le paragraphe suivant une méthode permettant d'éviter ces lourds calculs génériques.

3.3 Une version effective des théorèmes 3.1 et 3.4

Nous voulons calculer les coordonnées d'un invariant $P \in k(\mathbf{X})^H$ dans une $k(\mathbf{X})^L$-base $(1, \Theta, \ldots, \Theta^{e-1})$ formée des puissances d'un élément primitif Θ. Pour cela, l'idée consiste à mettre une structure de $k(\mathbf{X})^L$-espace quadratique sur $k(\mathbf{X})^H$.

3.3.1 Structure d'espace quadratique sur $k(\mathbf{X})^H$

Proposition 3.5 *Ici, k est un corps commutatif quelconque. Si L et H sont deux sous-groupes finis de $\mathbf{GL}_n(k)$ tels que $H \subset L$, alors la $k(\mathbf{X})^L$-forme bilinéaire symétrique $< .,. >$ définie sur $k(\mathbf{X})^H$ par:*

$$\begin{aligned} \forall\, (P,Q) \in (k(\mathbf{X})^H)^2, \qquad < P,Q > &= \sum_{\sigma \in (L//H)_g} \sigma.(PQ) \\ &= \frac{1}{|H|} \sum_{\sigma \in L} \sigma.(PQ) \text{ si caract}(k) \text{ ne divise pas } |H| \end{aligned}$$

est non-dégénérée.

Nous donnons de ce résultat une preuve effective, dans le cas particulier où L est un groupe de permutations, et une preuve non effective dans le cas général.

Première preuve (*Cas où $L \subset \mathfrak{S}_n$*) – Cette preuve relativement technique consiste, une fraction $F \in k(\mathbf{X})^H$ étant donnée, à trouver un n-uplet $\beta \in \mathbb{N}^n$ tel que le polynôme $\mu = \sum_{\tau \in H} \mathbf{X}^{\tau.\beta} \in k[\mathbf{X}]^H$ ne soit pas orthogonal à F.

Pour commencer, nous réduisons le cas général $F \in k(\mathbf{X})^H$ au cas d'un polynôme $P \in k[\mathbf{X}]^H$. Écrivons $F = P_1/P_2$ sous la forme d'une fraction irréductible. Nous voyons alors facilement que P_1 et P_2 doivent appartenir à $k[\mathbf{X}]^H$; le polynôme $Q = \prod_{\sigma \in (L//H)_g} \sigma.P_2$ appartient donc à $k[\mathbf{X}]^L$, et $P = QP_1/P_2$ appartient à $k[\mathbf{X}]^H$. Aussi, si nous supposons le résultat vérifié pour les polynômes nous pouvons trouver un n-uplet $\beta \in \mathbb{N}^n$ tel que $< P, \mu > \neq 0$. Et on aura alors $< F, \mu >= (1/Q) < P, \mu > \neq 0$.

Prouvons maintenant le résultat quand F est un polynôme $P \in k[\mathbf{X}]^H$. Nous utiliserons les notations et conventions suivantes :

- L'ordre sur $\mathbb{N}^n$ sera par défaut l'ordre lexicographique, noté $<$.
- Si $\alpha \in \mathbb{N}^n$, $\alpha^\star \in \mathbb{N}^n$ désigne le plus grand élément de l'orbite $L.\alpha$ de α sous l'action de L. Par exemple, si $L = \mathfrak{S}_n$, $\alpha^\star$ est calculé en rangeant les éléments de α dans l'ordre décroissant.
- Si $g = a.X_1^{\alpha_1}.X_2^{\alpha_2} \ldots X_n^{\alpha_n}$ est un monôme non nul, on note $\phi(g) = \alpha$.

Soit $\alpha = (\alpha_1, \ldots, \alpha_n)$ le plus grand $\phi(g)^\star$ quand g décrit l'ensemble des monômes de P, et m un monôme correspondant à $\phi(g)^\star$. À une renumérotation près des indéterminées $X_1, \ldots, X_n$, on peut supposer que $m = a.\mathbf{X}^\alpha$ pour un certain scalaire non nul $a \in k$. On peut alors écrire :

$$P = \sum_{\sigma \in E} a_\sigma X_1^{\alpha_{\sigma(1)}} \ldots X_n^{\alpha_{\sigma(n)}} + \sum_{i \in I} m_i$$

où E est un système de représentants des classes à gauche de $\mathcal{S}tab_L(\alpha)$ dans L tel que $Id \in E$, où les a_σ appartiennent à k ($a_{Id} = a$), et où les m_i ($i \in I$) sont des monômes tels que $\phi(m_i)^\star < \phi(m)^\star = \alpha$.

Soit $\beta \in \mathbb{N}^n$, et $\mu = \sum_{\tau \in H} \mathbf{X}^\beta$. Alors $< P, \mu >$ est la somme des polynômes $s.(P\mu)$ pour $s \in (L//H)_g$, où

$$P\mu = \sum_{\sigma \in E, \tau \in H} a_\sigma \mathbf{X}^{\sigma.\alpha + \tau.\beta} + \sum_{i \in I, \tau \in H} m_i \mathbf{X}^{\tau.\beta} \quad .$$

Soit d le degré total de P. Nous supposons que $\forall i \in \mathbb{N}^*_{n-1}, \beta_{i+1} > \beta_i + d$. Nous allons montrer que c'est une condition suffisante pour que $m\mathbf{X}^\beta = a\mathbf{X}^{\alpha+\beta}$ ne soit pas détruit par les autres monôme quand on additionne tous les $s.(P\mu)$. Cela prouvera bien que $< P, \mu > \neq 0$.

- Commençons par les monômes $m_i \mathbf{X}^{\tau.\beta}$. Soit $i \in I$ et $\tau \in H$. Soit $\gamma = \phi(m_i)$. Comme $\alpha > \gamma^\star = (\tau^{-1}.\gamma)^\star$ et $\beta^\star = \beta$, on $\alpha + \beta > (\tau^{-1}.\gamma)^\star + \beta^\star \geq (\tau^{-1}.\gamma + \beta)^\star = (\gamma + \tau.\beta)^\star$, *i.e.* $\phi(m\mathbf{X}^\beta)^\star > \phi(m_i \mathbf{X}^{\tau.\beta})^\star$. Aussi, aucun des $s.(m_i \mathbf{X}^{\tau.\beta})$ ($i \in I$, $\tau \in H$, $s \in (L//H)_g$) n'a le même multidegré que $m\mathbf{X}^\beta$.

- Traitons maintenant le cas des monômes $a_\sigma \mathbf{X}^{\sigma.\alpha+\tau.\beta}$. Soit $(\sigma, \tau) \in E \times H$. Nous avons $(\sigma.\alpha + \tau.\beta)^\star = (\beta + (\tau^{-1}\sigma).\alpha)^\star$. De deux choses l'une : soit $\tau^{-1}\sigma \notin \mathcal{S}tab_L(\alpha)$, et alors $\alpha + \beta > (\sigma.\alpha + \tau.\beta)^\star$ (car

$\beta_{i+1} > \beta_i + d$), si bien qu'alors aucun des $s.(a_\sigma \mathbf{X}^{\sigma.\alpha+\tau.\beta})$ $(s \in L)$ n'a le même multidegré que $m\mathbf{X}^\beta$; soit $\tau^{-1}\sigma \in \mathcal{S}tab_L(\alpha)$. Dans ce dernier cas, le seul $s.(a_\sigma \mathbf{X}^{\sigma.\alpha+\tau.\beta})$ $(s \in L)$ qui ait pour multidegré $\alpha + \beta$ est $a_\sigma \mathbf{X}^{(\tau^{-1}\sigma).\alpha+\beta}$. Mais comme $\tau^{-1}\sigma \in E \cap \mathcal{S}tab_L(\alpha) = \{Id\}$, on a alors $\sigma = \tau \in H$. Par conséquent, $a_\sigma = a$, car $P \in k[\mathbf{X}]^H$.

Nous avons prouvé que les seuls monômes de multidegré $\alpha+\beta$ qui apparaissent dans le développement de $< P, \mu >$ ont pour coefficient a, et qu'il y a au moins un tel monôme: $m\mathbf{X}^\beta$; leur somme est donc non nulle. Par suite, $< P, \mu > \neq 0$. □

Autre preuve (*Cas général*) – L'extension $k(\mathbf{X}) : k(\mathbf{X})^L$ est galoisienne (voir la démonstration du Théorème 3.1) donc sa sous-extension $k(\mathbf{X})^H : k(\mathbf{X})^L$ est séparable. La forme bilinéaire trace associée à cette extension, qui n'est autre que $< ., . >$, est donc non-dégénérée d'après [13, A V.47 Proposition 1.c)]. □

Remarque 3.6 *Quand la caractéristique de k est zéro ou ne divise pas $|L|$, l'application de $k[\mathbf{X}]$ sur $k[\mathbf{X}]^L$ définie par $P \mapsto \frac{1}{|L|}\sum_{\sigma\in L} \sigma.P$ est parfois appelée le projecteur de Reynolds $\mathcal{R}ey_L$. Alors, $< P, Q >$ est égal à $[L : H].\mathcal{R}ey_L(PQ)$.*

Remarque 3.7 *La forme $< ., . >$ est non-dégénérée mais par contre, elle n'est pas en général définie. Par exemple, pour $n = 4$, $L = \mathfrak{S}_4$, $H = \{Id\}$ et $P = (X_1 - X_2) + i(X_3 - X_4)$, on a $< P, P >= \sum_{\sigma\in\mathfrak{S}_4} \sigma.((X_1 - X_2)^2 - (X_3 - X_4)^2 + 2i(X_1 - X_2)(X_3 - X_4)) = 0$.*

Sous des hypothèses supplémentaires, la forme $< ., . >$ est cependant définie :

Proposition 3.8 *Si k est un sous-corps de $\mathbb{C}$ invariant par conjugaison ($\bar{k} = k$; ce n'est pas automatique : penser à $\mathbb{Q}(\pi + i)$), et L un sous-groupe fini de $\mathbf{GL}_n(k)$, alors la $k(\mathbf{X})^L$-forme sesquilinéaire à symétrie hermitienne $(.,.)$ définie sur $k(\mathbf{X})$ par :*

$$\forall\, (P, Q) \in k(\mathbf{X})^2,\ \ (P, Q) \ = < P, \bar{Q} > = \ \sum_{\sigma\in L} \sigma.(P\bar{Q})$$

est définie positive. Elle induit donc, pour tout sous-groupe H de L, une forme définie positive sur $k(\mathbf{X})^H$.

Preuve – Soit $P \in k(\mathbf{X})$ tel que $(P, P) = 0$. Soit W l'hypersurface algébrique de $(k \cap \mathbb{R})^n$ définie par le dénominateur de $\prod_{\sigma\in L} \sigma.(P\bar{P})$. Alors pour tout α appartenant à $(k \cap \mathbb{R})^n \setminus W$, $(P, P)(\alpha) = \sum_{\sigma\in L}(\sigma.(P.\bar{P}))(\alpha) = \sum_{\sigma\in L} |(\sigma.P)(\alpha)|^2$ appartient à $\mathbb{R}$ et $|P(\alpha)|^2 \leq (P, P)(\alpha) = 0$; donc $P.\bar{P}(\alpha) = 0$. Or, $P\bar{P}$ appartient à $(k \cap \mathbb{R})(\mathbf{X})$ (car $\bar{k} = k$) et $k \cap \mathbb{R}$, comme sous-corps de $\mathbb{R}$, doit contenir $\mathbb{Q}$ et être infini. Par conséquent, d'après le théorème de prolongement des identités algébriques (voir [13, A IV.17]), $P.\bar{P} = 0$; et donc $P = 0$. □

Corollaire 3.9 *Si $k \subset \mathbb{R}$, alors la forme bilinéaire symétrique $< ., . >$ définie dans la Proposition 3.5 est définie.*

3.3.2 Application

Nous appliquons maintenant le résultat précédent au problème que nous nous étions fixés au début : exprimer $P \in k(\mathbf{X})^H$ comme polynôme en Θ à coefficients dans $k(\mathbf{X})^L$.

Nous apprenons que Jean-Marie Arnaudiès avait déjà utilisé cette méthode, que nous avons publiée dans [17], pour exprimer des invariants les uns en fonction d'autres, dans le cadre de la recherche du groupe de Galois d'un polynôme de degré 5 (voir [4]).

Proposition 3.10 *Ici encore, k est un corps commutatif quelconque. Soit H et L deux sous-groupes finis de $\mathbf{GL}_n(k)$ tels que $H \subset L$. Soit Θ un invariant primitif de H relatif à L, et $P \in k(\mathbf{X})^H$. Soit $< .,. >$ la $k(\mathbf{X})^L$-forme bilinéaire symétrique sur $k(\mathbf{X})^H$ définie dans la Proposition 3.5. Alors les coordonnées $(A_0, \ldots, A_{e-1})$ de P dans la $k(\mathbf{X})^L$-base $(1, \Theta, \ldots, \Theta^{e-1})$ de $k(\mathbf{X})^H$ sont l'unique solution du système de Cramer sur le corps $k(\mathbf{X})^L$ suivant:*

$$\forall i \in \{0, \ldots, e-1\},\ < \Theta^i, 1 > A_0 + < \Theta^i, \Theta > A_1 + \ldots + < \Theta^i, \Theta^{e-1} > A_{e-1} \ = < \Theta^i, P > \qquad (3.2)$$

Preuve – En effet, $(A_0, A_1, \ldots, A_{e-1})$ doit satisfaire $P = \sum_{j=0}^{e-1} A_j \Theta^j$, donc pour tout $i \in \{1, \ldots, e-1\}$, en projetant par $< .,. >$ sur Θ^i, on obtient : $< \Theta^i, P >= \sum_{j=0}^{e-1} A_j < \Theta^i, \Theta^j >$. Le système (3.2) est alors de Cramer car $(1, \Theta, \ldots, \Theta^{e-1})$ est une $k(\mathbf{X})^L$-base de l'espace $k(\mathbf{X})^H$, sur lequel $< .,. >$ est non-dégénérée d'après la Proposition 3.5. □

Cette proposition donne donc un algorithme pour exprimer $P \in k(\mathbf{X})^H$ en fonction des puissances d'un invariant primitif Θ. Toutefois, quand on a plusieurs polynômes P à exprimer de la sorte, plutôt que de résoudre à chaque fois un système linéaire, on a intérêt à orthogonaliser une fois pour toutes la base $(1, \Theta, \ldots, \Theta^{e-1})$ en une base $(U_0, \ldots, U_{e-1})$, par l'algorithme de Gram-Schmidt par exemple. On obtient alors la décomposition de P simplement par la formule suivante :

$$P = \sum_{i=0}^{e-1} \frac{< P, U_i >}{< U_i, U_i >} . U_i$$

et il ne reste plus qu'à réexprimer P dans la base $(1, \Theta, \ldots, \Theta^{e-1})$. Notons que l'hypothèse requise sur $< .,. >$ pour orthogonaliser $(1, \Theta, \ldots, \Theta^{e-1})$ par l'algorithme de Gram-Schmidt (que ses restrictions à chacun des sous-espaces $\bigoplus_{j=0}^{i} k(\mathbf{X})^L . \Theta^j$, pour $0 \leq i \leq e-1$, soient non-dégénérées) est plus forte que celle de la Proposition 3.10. Elle est vérifié par exemple sous les hypothèses de la Proposition 3.8.

Le gros avantage de la Proposition 3.10 est qu'elle permet, contrairement à la preuve de Lagrange, de spécialiser au fur et à mesure des calculs (voir le paragraphe 3.5).

Remarque 3.11 *La Proposition 3.10 nous donne une seconde preuve du Théorème 3.4, plus simple et sous des hypothèses plus faibles, c'est-à-dire en remplaçant $\mathfrak{S}_n$ par un sous-groupe fini quelconque L de $\mathbf{GL}_n(k)$. Plus précisément, si $H \subset L$ sont deux sous-groupes finis de $\mathbf{GL}_n(k)$ et Θ un invariant primitif de H relatif à L alors*

$$k[\mathbf{X}]^H \subset \frac{1}{\Delta_\Theta} k[\mathbf{X}]^L[\Theta], \qquad \text{où} \quad \Delta_\Theta = \prod_{(\Theta', \Theta'') \in (L.\Theta)^2, \Theta' \neq \Theta''} (\Theta' - \Theta'') \ .$$

Preuve – Le système (3.2) montre que les coordonnées A_i d'un $P \in k[\mathbf{X}]^H$ dans la base $(1, \Theta, \ldots, \Theta^{e-1})$ peuvent s'écrire $A_i = B_i / C$ avec $B_i \in k[\mathbf{X}]^L$ et $C = \det(M_\Theta) \in k[\mathbf{X}]^L$, où

$$M_\Theta = \begin{pmatrix} < 1, 1 > & < 1, \Theta > & \ldots & < 1, \Theta^{e-1} > \\ < \Theta, 1 > & < \Theta, \Theta > & \ldots & < \Theta, \Theta^{e-1} > \\ \vdots & \vdots & & \vdots \\ < \Theta^{e-1}, 1 > & < \Theta^{e-1}, \Theta > & \ldots & < \Theta^{e-1}, \Theta^{e-1} > \end{pmatrix}$$

Or, on remarque que $M_\Theta = V(\Theta_1, \ldots, \Theta_e)^t V(\Theta_1, \ldots, \Theta_e)$ où $V(\Theta_1, \ldots, \Theta_e)$ désigne la matrice de Vandermonde de $(\Theta_1, \ldots, \Theta_e)$. Par conséquent, $C = \det(M_\Theta) = \det(V(\Theta_1, \ldots, \Theta_e))^2$ est égal à Δ_Θ, d'où le résultat. □

3.4 Implantation

Nous avons implanté l'algorithme de la Proposition 3.10, ainsi que sa variante qui remplace la résolution d'un système linéaire par une orthogonalisation une fois pour toutes de la base $(1, \Theta, \ldots, \Theta^{e-1})$, en AXIOM, dans le cas où L est un groupe de permutations (mais ce n'est pas plus compliqué quand L est un groupe fini de matrices). Le paquetage a pour nom `ElementPrimitif`. Nous nous limiterons à présenter le cas $L = \mathfrak{S}_n$, où nous pouvons exprimer les éléments de $k[\mathbf{X}]^{\mathfrak{S}_n}$ en fonction des polynômes symétriques élémentaires.

La forme bilinéaire symétrique $< ., . >$ définie à la Proposition 3.5 est extrêmement simple à implanter et rapide à évaluer : en effet, si l'on utilise la représentation des polynômes symétriques du chapitre 2, alors $< P, Q >$ s'obtient en remplaçant chaque monôme $\mathbf{X}^\alpha$ du produit PQ par la forme monomiale M_α multipliée par l'entier $|\mathcal{S}tab_{\mathfrak{S}_n}(\alpha)|$. Il n'y a donc rien à calculer, hormis $|\mathcal{S}tab_{\mathfrak{S}_n}(\alpha)|$, mais seulement à changer le type des objets (α ne représente plus $\mathbf{X}^\alpha$ mais M_α).

Voici un exemple d'application, avec $n = 4$, $k = \mathbb{Q}$, $L = \mathfrak{S}_4$, $H =< (1\ 3\ 2\ 4), (1\ 2) >\simeq \mathfrak{D}_4$, $e = [L : H] = 3$, $\Theta = X_1X_2 + X_3X_4$, et différents polynômes $P \in k[\mathbf{X}]^H$.

```
(1) ->prim := ElementPrimitif(4,Fraction Integer,[E1,E2,E3,E4],[X1,X2,X3,X4])
   (1)  ElementPrimitif(4,Fraction Integer,[E1,E2,E3,E4],[X1,X2,X3,X4])
                                                              Type: Domain

(2) ->theta := X1 * X2 + X3 * X4
   (2)  X2 X1 + X4 X3
                Type: MultivariatePolynomial([X1,X2,X3,X4],Fraction Integer)

(3) ->psi := X1**2 * X3 + X3**2 * X2 + X2**2 * X4 + X4**2 * X1
             2     2          2     2
   (3)  X3 X1  + X4 X1 + X4 X2  + X3 X2
                Type: MultivariatePolynomial([X1,X2,X3,X4],Fraction Integer)

(4) ->psiprime : mp := X1**2 * X4 + X3**2 * X1 + X2**2 * X3 + X4**2 * X2
              2     2          2     2
   (4)  X4 X1  + X3 X1 + X3 X2  + X4 X2
                Type: MultivariatePolynomial([X1,X2,X3,X4],Fraction Integer)

(5) ->systemeGeneriqueElem(theta,psi+psiprime,2)$prim
   (5)  [E2 E1 - 2E3,- E1,0]
   Type: List Fraction MultivariatePolynomial([E1,E2,E3,E4],Fraction Integer)

(6) ->systemeGeneriqueElem(theta,psi*psiprime,2)$prim
   (6)
         3        2                 3               2
   [E3 E1  - E4 E1  - 5E3 E2 E1 + E2  + 4E4 E2 + 4E3 ,
           2             2          2
    - E2 E1  + 2E3 E1 + E2  - 4E4, E1  - 2E2]
   Type: List Fraction MultivariatePolynomial([E1,E2,E3,E4],Fraction Integer)
```

La fonction `systemeGeneriqueElem` appliquée aux arguments `theta, psi+psiprime, 2` (ce dernier argument étant le degré $e-1$ du polynôme en Θ qui permet d'exprimer P) a permis d'exprimer $\Psi + \Psi'$ et $\Psi\Psi'$ en fonction de $\Theta = X_1X_2 + X_3X_4$ et des polynômes symétriques élémentaires, où $\Psi = X_1^2X_2 +$

$X_2^2X_3 + X_3^2X_4 + X_4^2X_1$ et $\Psi' = X_1^2X_4 + X_2^2X_1 + X_3^2X_2 + X_4^2X_3$. Le résultat obtenu signifie que :

$$\Psi + \Psi' = E_2E_1 - 2E_3 - E_1\Theta \quad \text{et}$$

$$\Psi\Psi' = E_3E_1^3 - E_4E_1^2 - 5E_3E_2E_1 + E_2^3 + 4E_4E_2 + 4E_3^2 + (-E_2E_1^2 + 2E_3E_1 + E_2^2)\Theta + (E_1^2 - 2E_2)\Theta^2 \ .$$

Comme $\mathcal{S}tab_{\mathfrak{S}_4}(\Psi) \simeq \mathfrak{C}_4$ est inclus dans $\mathcal{S}tab_{\mathfrak{S}_4}(\Theta) \simeq \mathfrak{D}_4$, on pourrait à l'inverse exprimer Θ en fonction de Ψ :

```
(7) ->systemeGeneriqueElem(psi,theta,2)$prim
```

mais nous n'écrivons pas le résultat, qui prendrait une page entière.

3.5 Application à la spécialisation des invariants

Nous allons appliquer ce qui précède au problème suivant :

Problème : Soit L et H deux sous-groupes finis de $\mathbf{GL}_n(k)$ tels que $H \subset L$. On spécialise les indéterminées $X_1, \ldots, X_n$ en des valeurs $x_1, \ldots, x_n$ respectivement, qui appartiennent à une extension algébrique $\hat{k}$ de k, et qui sont inconnues. Par contre on dispose d'un moyen de connaître les valeurs prises lors de cette spécialisation par les éléments de $k[\mathbf{X}]^L$, ainsi que le spécialisé θ d'un invariant primitif Θ de H relatif à L. On cherche alors à spécialiser un élément quelconque de $k(\mathbf{X})^H$.

Remarque 3.12 *Remarquons que Θ est racine du polynôme $\prod \tau \in (L//H)_g(T - \tau.\Theta) \in k[\mathbf{X}]^L[T]$, polynôme dont on sait spécialiser les coefficients car ils appartiennent à $k[\mathbf{X}]^L$. Si $p \in \hat{k}[T]$ est le spécialisé de ce polynôme, alors $p(\theta) = 0$, donc θ est l'une des $[L : H]$ racines de p. Si l'on se «trompe» de racine, on aura simplement spécialisé un conjugué $\tau.\Theta$ de Θ, qui est un invariant primitif de $\tau.H.\tau^{-1}$ relatif à L.*

Voici une situation concrète où ce problème se pose :
Exemple : Soit $L = \mathfrak{S}_n$ et H un sous-groupe de $\mathfrak{S}_n$. On considère un polynôme $f \in k[T]$, unitaire de degré n, qui s'écrit $f = T^n + \sum_{i=1}^n (-1)^i e_i T^{n-i}$. Soit $(x_1, \ldots, x_n)$ ses racines dans une clôture algébrique $\hat{k}$ de k. On ne connaît pas ces racines, mais on sait par contre spécialiser les polynômes symétriques élémentaires E_i en ces racines : E_i se spécialise en e_i ; et donc, par le théorème fondamental sur les polynômes symétriques, on sait spécialiser tous les éléments de $k[\mathbf{X}]^{\mathfrak{S}_n}$. Supposons qu'on connaisse la spécialisation $\theta = \Theta(x_1, \ldots, x_n)$ d'un invariant primitif Θ de H (on peut par exemple connaître θ par la factorisation de la résolvante $\mathcal{L}_{\Theta,\mathbf{x}}$, voir le Paragraphe 6.2). On cherche à utiliser Θ pour spécialiser un élément quelconque de $k[\mathbf{X}]^H$.

Revenons au problème général. Soit donc $P \in k(\mathbf{X})^H$ que l'on cherche à spécialiser. On notera $\widetilde{A}$ le spécialisé $A(\mathbf{x})$ d'un élément A de $k[\mathbf{X}]^L$ en $\mathbf{x}$, $\theta = \Theta(\mathbf{x})$ le spécialisé de Θ.

Première méthode : D'après la Proposition 3.10 et la remarque qui suit, on sait que l'on peut écrire d'une manière unique

$$P = \frac{C_0 + C_1\Theta + \ldots + C_{e-1}\Theta^{e-1}}{\Delta_\Theta} \quad \text{avec} \quad C_i \in k[\mathbf{X}]^L, \quad \text{pour} \quad 0 \leq i \leq e-1$$

et que $(\frac{C_0}{\Delta_\Theta}, \ldots, \frac{C_{e-1}}{\Delta_\Theta})$ est solution du système linéaire (3.2). En spécialisant ce système, on obtient donc le système linéaire suivant :

$$\forall i \in \{0, \ldots, e-1\},\ \widetilde{<\Theta^i, 1>} a_0 + \widetilde{<\Theta^i, \Theta>} a_1 + \ldots + \widetilde{<\Theta^i, \Theta^{e-1}>} a_{e-1} \ = \ \widetilde{<\Theta^i, P>} \qquad (3.3)$$

On sait calculer les coefficients de ce système car par hypothèse on sait spécialiser les éléments de $k[\mathbf{X}]^L$. Le déterminant de ce système est $\widetilde{\Delta_\Theta}$. S'il est non nul, alors sa solution $(a_0, \ldots, a_{e-1})$ vérifie

$$\widetilde{P} = a_0 + a_1\theta + \ldots + a_{e-1}\theta^{e-1}$$

et l'on saura donc spécialiser P.

Seconde méthode: On suppose cette fois non seulement que $\widetilde{\Delta_\Theta}$ est non nul, mais qu'en outre pour tout $k \in \{0, \ldots, e-1\}$, le déterminant $\widetilde{\Delta_{k,\Theta}}$ de la matrice $(\widetilde{<\Theta^i, \Theta^j>})_{0 \le i \le k, 0 \le j \le k}$ est non nul. On peut alors appliquer l'algorithme d'orthogonalisation de Gram-Schmidt après spécialisation, c'est-à-dire que l'on définit les familles $(U_0, \ldots, U_{e-1})$ et $(\widetilde{U_0}, \ldots, \widetilde{U_{e-1}})$ par récurrence de la manière suivante :

$$\forall\, i \in \{0, \ldots, e-1\},\ U_i = \Theta^i - \sum_{j=0}^{i-1} \frac{\widetilde{<\Theta^i, U_j>}}{\widetilde{<U_j, U_j>}} U_j \ \text{ et } \ \widetilde{U_i} = \theta^i - \sum_{j=0}^{i-1} \frac{\widetilde{<\Theta^i, U_j>}}{\widetilde{<U_j, U_j>}} \widetilde{U_j}.$$

Cela permet ensuite de calculer

$$\widetilde{P} = \sum_{j=0}^{e-1} \frac{\widetilde{<P, U_j>}}{\widetilde{<U_j, U_j>}} \widetilde{U_j} \qquad .$$

Remarquons que l'on n'a pas eu besoin de réexprimer P dans la base $(1, \Theta, \ldots, \Theta^{e-1})$, on a directement calculé les $\widetilde{U_i}$ en appliquant l'algorithme de Gram-Schmidt avec valeurs spécialisées parallèlement à son application aux valeurs génériques.

Remarque 3.13 (Dégénérescence par spécialisation) *Au cas où le déterminant Δ_Θ s'annulerait par spécialisation (cas de la première méthode) ou bien où l'un des $\widetilde{\Delta_{k,\Theta}}$ serait nul (cas de la seconde méthode), le système linéaire, ou la normalisation de Gram-Schmidt, dégénère. Dans les applications aux seconde et troisième parties, on règle ce problème respectivement grâce à la Proposition 8.4 et à la méthode indiquée dans le Paragraphe 10.7.4.*

Implantation Ces deux méthodes sont implantées en AXIOM, dans le cas où $L = \mathfrak{S}_n$. La spécialisation des éléments de $k[\mathbf{X}]^{\mathfrak{S}_n}$ connaissant les valeurs spécialisées des polynômes symétriques élémentaires utilise alors le domaine `PolynomesSymetriques` présenté au chapitre 2.

Montrons le résultat obtenu sur l'exemple précédent : $n = 4$, $k = \mathbb{Q}$, $L = \mathfrak{S}_4$, $H =< (1\ 3\ 2\ 4), (1\ 2) > \simeq \mathfrak{D}_4$, $\Theta = X_1X_2 + X_3X_4$. On cherche à spécialiser en les valeurs $x_1 = \frac{-1-i}{\sqrt{2}}$, $x_2 = \frac{1-i}{\sqrt{2}}$, $x_3 = \frac{-1+i}{\sqrt{2}}$, $x_4 = \frac{1+i}{\sqrt{2}}$, que l'on n'est pas supposé connaître, sinon par le fait qu'elles sont racines du polynôme $T^4 + 1$ et que $\theta = \Theta(x_1, x_2, x_3, x_4) = -2$ (la valeur de θ peut être calculée par exemple en factorisant $\mathcal{L}_{\Theta, T^4+1} = T(T-2)(T+2)$, voir le Paragraphe 6.2). On sait donc spécialiser les polynômes symétriques élémentaires $E_1, \ldots, E_4$, respectivement en $0, 0, 0$ et 1, et Θ, en θ. Nous allons en déduire les valeurs spécialisées de $\Psi + \Psi'$ et de $\Psi\Psi'$, où $\Psi = X_1^2X_2 + X_2^2X_3 + X_3^2X_4 + X_4^2X_1$ et $\Psi' = X_1^2X_4 + X_2^2X_1 + X_3^2X_2 + X_4^2X_3$:

```
(8) ->specialise(theta,psi+psiprime,[0,0,0,1],-2,2)$prim
   (8)  0
                                                    Type: Fraction Integer
```

```
(9) ->specialise(theta,psi*psiprime,[0,0,0,1],-2,2)$prim
   (9)  8
                                                    Type: Fraction Integer
```

donc $\widetilde{\Psi+\Psi'}=0$ et $\widetilde{\Psi\Psi'}=8$. C'est la première méthode qui a été utilisée ici. Les arguments de la fonction `specialise` sont respectivement Θ, P, $(\widetilde{E_1},\widetilde{E_2},\widetilde{E_3},\widetilde{E_4})$, θ et $e-1=[\mathfrak{S}_n:H]-1$.

Chapitre 4

Algèbres de Cohen-Macaulay et invariants polynomiaux

Dans tout ce chapitre, k est un corps commutatif de caractéristique nulle.

4.1 Le théorème de Chevalley

Rappelons la définition d'un groupe de réflexions et le théorème de Chevalley.

Définition 4.1 *Une matrice $A \in \mathbf{GL}_n(k)$ est appelée une* réflexion *si et seulement si elle est diagonalisable et une et une seule de ses n valeurs propres n'est pas égale à 1. Un sous-groupe fini H de $\mathbf{GL}_n(k)$ est appelé un* groupe de réflexions *si et seulement s'il est engendré par des réflexions.*

Remarque.– Le fait d'être un groupe de réflexions n'est pas une propriété du groupe abstrait sous-tendant H. Cela dépend de sa représentation fidèle $H \subset \mathbf{GL}_n(k)$.

Théorème 4.2 (Chevalley) *L'anneau $k[\mathbf{X}]^H$ des invariants d'un groupe fini $H \subset \mathbf{GL}_n(k)$ est engendré par n invariants homogènes et algébriquement indépendants si et seulement si H est un groupe de réflexions.*

Preuve – Voir [16] pour la partie directe, et [62, Th. 2.4.1] pour la réciproque. □

Corollaire 4.3 *L'anneau $k[\mathbf{X}]^H$ des invariants d'un groupe fini de permutations $H \subset \mathfrak{S}_n$ est engendré par n invariants homogènes algébriquement indépendants si et seulement si H est un produit $\mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}$ de groupes symétriques avec $\sum_{j=1}^{s} n_j = n$ et agit sur $k[\mathbf{X}]$ de sorte que chaque $\mathfrak{S}_{n_j}$ agisse par permutations sur un ensemble de n_j indéterminées, ces ensemble étant deux à deux disjoints.*

Preuve – Pour la partie «si», voir Exemple 1.2 ou [34]. Pour la partie «seulement si», nous remarquons tout d'abord que la matrice A_τ associée à une permutation $\tau \in \mathfrak{S}_n$ est toujours diagonalisable, et que son polynôme caractéristique est $\prod_{j=1}^{r}(1 - z^{l_j})$ où $l(\tau) = (l_1, \ldots, l_r)$ est la famille des longueurs des cycles de τ. (cela se voit facilement à partir de la décomposition par blocs de A_τ associée à la décomposition en cycles de τ). Aussi, une telle permutation τ agit comme une réflexion si et seulement si $l(\tau) = (1, \ldots, 1, 2)$, ou en d'autres termes, si et seulement si τ est une transposition. D'après le Théorème 4.2, H est alors engendré par des transpositions. C'est donc un produit de groupes symétriques agissant comme indiqué dans l'énoncé. □

4.2 La propriété de Cohen-Macaulay

La propriété de Cohen-Macaulay permet d'obtenir, de manière effective, une normalisation de Noether d'une algèbre d'invariants. Marc Giusti et Joos Heintz ont montré dans des travaux initiés par [30] et résumés dans [33] que d'une manière générale (hors du cadre de la théorie des invariants), une telle décomposition fournit une bonne structure de données pour une représentation par programmes d'évaluations. Nous verrons aux chapitres 9 et 10 et aux annexes A, B et C, bien que nous nous situions au long de cette thèse dans une *philosophie classique de réécriture* et non dans une *philosophie d'évaluation* (voir [30] pour ces notions), que l'utilisation de cette normalisation de Noether simplifie considérablement les calculs. De plus, dans ce cadre particulier de théorie des invariants, la normalisation de Noether ne dépend que d'une action de groupe, et peut donc être calculée une fois pour toutes pour chacune des actions utilisées, et être réutilisée pour tous les problèmes invariants sous la même action de groupe. Ce genre de situation — précalcul coûteux permettant des calculs ultérieurs très rapides — est classique dans le cadre des méthodes d'évaluation (voir [30]).

Théorème 4.4 (Hochster-Eagon) *Soit H un sous-groupe fini de $\mathbf{GL}_n(k)$ (k étant supposé de caractéristique nulle). Alors $k[\mathbf{X}]^H$ est une algèbre de Cohen-Macaulay sur k, de dimension de Krull n. Cela signifie que l'on peut trouver une famille $(\Pi_1, \ldots, \Pi_n) \in (k[\mathbf{X}]^H)^n$ de polynômes homogènes telle que $k[\mathbf{X}]^H$ soit un module de type fini sur $k[\Pi_1, \ldots, \Pi_n]$; et que pour n'importe quel tel choix $(\Pi_1, \ldots, \Pi_n)$, $k[\mathbf{X}]^H$ est un module libre sur $k[\Pi_1, \ldots, \Pi_n]$. Sa dimension est alors $(\prod_{i=1}^n \deg(\Pi_i))/|H|$. De plus, on peut trouver une $k[\mathbf{\Pi}]$-base de ce module formée de polynômes homogènes, dont l'un d'entre eux est 1.*

Preuve – L'existence d'une famille $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$ telle que $k[\mathbf{X}]^H$ soit de type fini sur $k[\Pi_1, \ldots, \Pi_n]$ résulte du théorème de normalisation de Noether et ne dépend donc pas du fait qu'on ait une algèbre d'invariants. Pour le reste, voir [60], ou [62, Th. 2.3.1 and 2.3.5]. □

Les polynômes Π_i sont appelés *invariants primaires* de H. Une base $(\Sigma_1, \ldots, \Sigma_e)$ de $k[\mathbf{X}]^H$ comme module sur $k[\Pi_1, \ldots, \Pi_n]$ est appelée famille d'*invariants secondaires* de H. On dit qu'ils forment ensemble un famille d'*invariants fondamentaux* de H. En pratique, on choisit en général les invariants secondaires Σ_i homogènes et $\Sigma_1 = 1$.

On peut donc écrire :

$$k[\mathbf{X}]^H = \bigoplus_{i=1}^{e} k[\Pi_1, \ldots, \Pi_n]\Sigma_i$$

où les Σ_i sont linéairement indépendants sur $k[\Pi_1, \ldots, \Pi_n]$ et les Π_i sont algébriquement indépendants sur k : c'est la description de $k[\mathbf{X}]^H$ la plus précise dont on pouvait rêver ! On l'appelle *décomposition d'Hironaka* de $k[\mathbf{X}]^H$. Signalons le résultat suivant, qui caractérise les familles d'invariants primaires :

Proposition 4.5 *Soit $(\Pi_1, \ldots, \Pi_n)$ une famille d'invariants homogènes du sous-groupe fini $H \subset \mathbf{GL}_n(k)$. Le $k[\Pi_1, \ldots, \Pi_n]$-module $k[\mathbf{X}]^H$ est de type fini (et donc alors libre d'après le Théorème 4.4) si et seulement si la sous-variété affine de k^n définie par ces polynômes est réduite au singleton $\{\mathbf{0}\}$ (c'est-à-dire si et seulement si la variété projective est vide).*

Preuve – Voir [40]. □

Remarque 4.6 *Le fait que $(\Pi_1, \ldots, \Pi_n)$ soit une base de transcendance pure de $k(\mathbf{X})^H$ n'implique pas qu'elle soit une famille d'invariants primaires de H. Par exemple, malgré le résultat de la Proposition 3.3, $k[\mathbf{X}]^{\mathcal{D}_4}$ n'est pas un module de type fini sur l'anneau $R = k[E_1, E_3, E_4, I]$, où $I = X_1X_2 + X_3X_4$.*

Preuve – En effet, R est un anneau de polynômes (car d'après les Prop. 3.3 et 1.3, les éléments E_1, E_3, E_4, I sont algébriquement indépendants sur k). Donc R est intégralement clos. Or, E_2 n'appartient pas à R, car R_2 (partie homogène de degré 2 de R) est de dimension 2 d'après sa série de Hilbert $\frac{1}{(1-z)(1-z^2)(1-z^3)(1-z^4)}$ et admet donc la famille libre (I, E_1^2) pour k-base ; et E_2 n'est pas combinaison linéaire de I et E_1^2. Mais on a vu à la Prop. 3.3 qu'il appartient à son corps des fractions $k(E_1, E_3, E_4, I)$. Donc E_2 n'est pas entier sur R ; et $R[E_2]$ n'est donc pas de type fini sur R. Or, $R[E_2] \subset k[\mathbf{X}]^{\mathcal{D}_4}$, et R est noethérien ; par conséquent, $k[\mathbf{X}]^{\mathcal{D}_4}$ n'est pas non plus de type fini sur R. □

La proposition qui suit permet de relier le Théorème 4.4 au point de vue de théorie des corps du chapitre 3.

Proposition 4.7 *Si $L \subset \mathbf{GL}_n(k)$ est un groupe fini de réflexions, alors pour tout sous-groupe H de L, $k[\mathbf{X}]^H$ est un module libre sur $k[\mathbf{X}]^L$, de dimension $[L : H]$.*

Preuve – L'anneau $k[\mathbf{X}]^H$ est entier sur $k[\mathbf{X}]^L$ car tout $P \in k[\mathbf{X}]^H$ est racine du polynôme unitaire $\prod_{Q \in L.P}(T - Q) \in k[\mathbf{X}]^L[T]$; et $k[\mathbf{X}]^H$ est une $k[\mathbf{X}]^L$-algèbre finie. Elle est donc de type fini comme $k[\mathbf{X}]^L$-module. Or, d'après le Théorème 4.2, $k[\mathbf{X}]^L$ est engendré comme k-algèbre par n polynômes homogènes algébriquement indépendants. Par conséquent, d'après le Théorème 4.4, $k[\mathbf{X}]^H$ est un $k[\mathbf{X}]^L$-module libre. Sa dimension est celle de $k(\mathbf{X})^H$ sur $k(\mathbf{X})^L$, c'est-à-dire $[L : H]$ d'après le Théorème 3.1. □

Sous les hypothèses de la Proposition 4.7, nous pouvons donc, d'après le Théorème 4.2, trouver une famille $(\Pi_1, \ldots, \Pi_n, \Sigma_1, \ldots, \Sigma_e)$ d'invariants fondamentaux telle que

$$k[\mathbf{X}]^L = k[\Pi_1, \ldots, \Pi_n] \quad \text{et} \quad k[\mathbf{X}]^H = \bigoplus_{i=1}^{e} k[\mathbf{X}]^L \Sigma_i,$$

décomposition à comparer avec (3.1), qui est donnée par le Théorème 3.1 dans le cas où H satisfait le problème de Noether.

Voici quelques exemples qui nous seront utiles par la suite :

Exemple 4.8 *On sait (voir par exemple [13, A IV.58 Théorème 1]) que*

$$k[\mathbf{X}] = \bigoplus_{\forall j \in \{1,\ldots,n\}, 0 \leq i_j \leq j-1} k[\mathbf{X}]^{\mathfrak{S}_n} X_1^{i_1} \ldots X_n^{i_n}$$

c'est-à-dire que $k[\mathbf{X}]$ est un $k[\mathbf{X}]^{\mathfrak{S}_n}$-module libre de dimension $n!$, et admet pour base la famille des $\prod_{j=1}^n X_j^{i_j}$ tels que pour tout j, $0 \leq i_j \leq i - 1$.

Exemple 4.9 *Si $H \subset \mathfrak{S}_n$, alors d'après la Proposition 4.7 et le Corollaire 4.3, nous pouvons choisir $\Pi_i = E_i$ pour tout $i \in \{1, \ldots, n\}$ (polynômes symétriques élémentaires) ; et $k[\mathbf{X}]^H$ est alors un module libre sur $k[\mathbf{X}]^{\mathfrak{S}_n} = k[\mathbf{E}]$, de dimension $e = [\mathfrak{S}_n : H]$.*

Exemple 4.10 *Pour les mêmes raisons, si $H \subset \mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}$, alors $k[\mathbf{X}]^H$ est un module libre sur $k[\mathbf{X}]^{\mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}} = k[\mathbf{E}^{(1)}, \ldots, \mathbf{E}^{(s)}]$ (notations de l'Exemple 1.2) de dimension $\prod_{j=1}^s n_j!/|H|$.*

4.3 Version effective

Nous n'expliquerons pas dans le détail comment peuvent être calculées des familles d'invariants fondamentaux. Signalons les travaux de G. Kemper, (voir [40]) qui permettent de trouver des invariants

primaires qui minimisent «souvent» le nombre d'invariants secondaires. Cet algorithme est implanté en Maple (voir [39]) et en MAGMA [1].

La formule de Molien (Théorème 1.5) permet d'avoir une idée *a priori* des degrés possibles des invariants primaires: en effet, la série de Hilbert, que l'on peut connaître à l'avance par cette formule, devra être le développement de la fraction rationnelle

$$\frac{z^{s_1} + \ldots + z^{s_e}}{(1 - z^{p_1}) \ldots (1 - z^{p_n})}$$

où les s_i (resp. les p_j) sont les degrés des invariants secondaires Σ_i (respectivement des invariants primaires Π_j). De plus, le nombre d'invariants secondaires est

$$e = \frac{p_1 p_2 \ldots p_n}{|H|}$$

donc il est utile de minimiser le produit des degrés des invariants primaires. On peut aussi vouloir minimiser la somme de ces degrés, dont dépend le degré maximal des invariants secondaires (puisque la différence des deux est le degré de la série de Hilbert vue comme fraction rationnelle, qui est fixé).

C'est possible algorithmiquement: en effet, la condition sur les coefficients des polynômes Π_i pour que $(\Pi_1, \ldots, \Pi_n)$ soit une famille d'invariants primaires est Zariski-ouverte d'après la Proposition 4.5 (car les Π_i conviennent si et seulement si leurs coefficients n'annulent pas le n-résultant des Π_i ; sur les résultants, on pourra consulter [26]), et trouver un point hors d'une variété de degré d en dimension m est algorithmique: cela coûte au plus d^m essais. On peut alors chercher les familles d'invariants primaires possibles en partant de ceux dont le produit des degrés est le plus bas (parmi les valeurs permises par la série de Hilbert), et monter de degré en degré jusqu'à trouver une famille qui convienne. De cette manière c'est très coûteux, mais cela prouve que l'on peut toujours trouver en un nombre fini d'étapes une famille d'invariants primaires qui minimise le nombre d'invariants secondaires. Les algorithmes implantés actuellement en Maple et MAGMA sont plus rapides, et minimisent dans la plupart des cas le nombre d'invariants secondaires. De plus, [41] présente maintenant une méthode qui permet d'allier l'idée déterministe (mais impraticable en pratique) que nous avons exprimée ci-dessus (le fait que la condition qui caractérise des invariants primaires est Zariski-ouverte) à un critère efficace (voir [41, Théorème 2]) pour obtenir un algorithme à la fois rapide (au moins autant que [39]) et qui donne à coup sûr la meilleure famille d'invariants primaires, pour le critère que l'on choisit, par exemple minimiser le produit de leurs degrés.

$\star$

Une fois les invariants fondamentaux calculés, on peut exprimer un invariant P donné en fonction d'eux par des calculs de bases standard. Ces calculs sont coûteux, et surtout ne permettent pas de spécialiser *a priori*: on est obligé de calculer complètement l'expression générique de P en fonction des invariants fondamentaux, et on ne peut spécialiser qu'après.

Dans le cas de figure de la Proposition 4.7, nous montrons que l'on a un algorithme d'algèbre linéaire, donc simple, qui permet en outre de spécialiser *avant* les calculs:

Proposition 4.11 (Décomposition d'Hironaka effective) *Avec les hypothèses de la Prop. 4.7 et les notations précédents, les coordonnées $(A_1, \ldots, A_e) \in (k[\mathbf{X}])L)^e$ d'un invariant $P \in k[\mathbf{X}]^H$ dans la base $(\Sigma_1, \ldots, \Sigma_e)$ de $k[\mathbf{X}]^L$-module sont la solution du système linéaire de Cramer suivant:*

$$\forall i \in \{1, \ldots, e\},\ < \Sigma_i, \Sigma_1 > A_0 + < \Sigma_i, \Sigma_2 > A_1 + \ldots + < \Sigma_i, \Sigma_{e-1} > A_{e-1} \ = < \Sigma_i, P > \qquad (4.1)$$

dont les coefficients appartiennent à $k[\mathbf{X}]^L$, où $< ., . >$ est la forme bilinéaire définie à la Proposition 3.5.

Preuve – On cherche la famille $(A_1, \ldots, A_e) \in (k[\mathbf{X}]^L)^e$ qui vérifie $P = \sum_{j=1}^e A_j \Sigma_j$. Par bilinéarité de $< ., . >$, elle doit vérifier aussi : $\forall i \in \mathbb{N}_e^*, < \Sigma_i, P >= \sum_{j=1}^e A_j < \Sigma_i, \Sigma_j >$. Ce système est de Cramer pour les mêmes raisons qu'à la Proposition 3.10 (on plonge les algèbres $k[\mathbf{X}]^H$ et $k[\mathbf{X}]^L$ dans leur corps des fractions ; $(\Sigma_1, \ldots, \Sigma_e)$ est alors une base de $k(\mathbf{X})^H$ comme $k(\mathbf{X})^L$-espace vectoriel). Par conséquent, $(A_1, \ldots, A_e)$ est la seule solution de ce système. □

Dans le cas général, l'algorithme qui permet d'exprimer un invariant en fonction d'une famille d'invariants fondamentaux utilise des bases standard au lieu de l'algèbre linéaire, ce qui est beaucoup plus coûteux du point de vue de la complexité.

Notons que sous l'hypothèse $k[\mathbf{X}] \cap k(\mathbf{\Pi}) = k[\mathbf{\Pi}]$, il résulte de [56, p. 50, Prop. 1] qu'il suffit de calculer une base standard de l'idéal $(\Pi_i(\mathbf{X}) - \Pi_i(\mathbf{Y}))_{1 \leq i \leq e}$ pour un ordre éliminant en $\mathbf{X}$, où $\mathbf{Y} = (Y_1, \ldots, Y_n)$. En réduisant un invariant $P \in k[\mathbf{X}]^H$ dans cette base standard, on obtiendra alors à la fois une famille $\mathbf{\Sigma}$ d'invariants secondaires Σ_i et la décomposition de P dans $\mathbf{\Sigma}$.

4.4 Spécialisation

4.4.1 Caractérisation par les syzygies

Nous prouvons maintenant les deux résultats suivants qui montrent, l'un en générique et l'autre sur les spécialisations, dans le cas de figure agréable où $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$, L étant un groupe de réflexions, que les invariants secondaires sont, à l'action près du groupe L, déterminés par leurs relations syzygies.

Ces deux résultats seront utiles pour permettre la spécialisation : voir le paragraphe 4.4.2.

Théorème 4.12 *Soit $L \subset \mathbf{GL}_n(k)$ un groupe fini de réflexions et H un sous-groupe de L. Soit $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n) \in (k[\mathbf{X}]^L)^e$ une famille de polynômes homogènes telle que $k[\mathbf{X}]^L = k[\mathbf{\Pi}]$ (donnée par le Théorème 4.2) et $(\Sigma_1, \ldots, \Sigma_e) \in k[\mathbf{X}]^H$ une famille d'invariants secondaires, c'est-à-dire telle que $k[\mathbf{X}]^H = \bigoplus_{i=0}^e k[\mathbf{X}]^L \Sigma_i$. Soit $\mathfrak{I} \subset k[\mathbf{\Pi}][Y_1, \ldots, Y_e]$, où les Y_i sont des indéterminées sur $k[\mathbf{X}]$, l'idéal des relations algébriques (syzygies) sur l'anneau $k[\mathbf{\Pi}]$ entre $\Sigma_1, \ldots, \Sigma_e$. Soit*

$$V(\mathfrak{I}) = \{(P_1, \ldots, P_e) \in (k[\mathbf{X}]^H)^e \ / \ \forall S \in \mathfrak{I}, S(P_1, \ldots, P_e) = 0\}$$

la variété définie par l'idéal $k[\mathbf{X}]^H \otimes_{k[\mathbf{X}]^L} \mathfrak{I}$ dans $(k[\mathbf{X}]^H)^e$. Alors $V(\mathfrak{I})$ est égal à :

$$V' = \{(\tau.\Sigma_1, \ldots, \tau.\Sigma_e) \ / \ \tau \in L\} \ .$$

Preuve – Il est clair que $V(\mathfrak{I})$ contient V', car il contient le point $(\Sigma_1, \ldots, \Sigma_n)$ par définition de $\mathfrak{I}$ et les éléments de $\mathfrak{I}$ sont invariants sous l'action de L. Réciproquement, soit $(P_1, \ldots, P_e) \in V(\mathfrak{I})$. Tout d'abord, pour tout $i \in \{1, \ldots, e\}$, le polynôme $\prod_{\tau \in (L//H)_g} (Y_i - \tau.\Sigma_i)$ appartient à $\mathfrak{I}$, ce qui prouve que Σ_i est entier sur $k[\mathbf{X}]^L$ et surtout, comme $(P_1, \ldots, P_e)$ appartient à $V(\mathfrak{I})$, qu'il existe $\tau_i \in L$ tel que $P_i = \tau_i.\Sigma_i$. Il reste à montrer que les τ_i peuvent être choisis tous égaux. Soit alors $U_1, \ldots, U_e$ des indéterminées sur $k[\mathbf{X}, \mathbf{Y}]$. Le polynôme $\prod_{\tau \in (L//H)_g} ((Y_1 - \tau.\Sigma_1)U_1 + \ldots + (Y_e - \tau.\Sigma_e)U_e))$ appartient à $k[\mathbf{\Pi}][\mathbf{U}] \otimes_{k[\mathbf{\Pi}]} \mathfrak{I}$ (en effet, il s'annule sur $\mathbf{\Sigma} = (\Sigma_1, \ldots, \Sigma_e)$ et ses coefficients en $\mathbf{U}, \mathbf{Y}$ appartiennent à $k[\mathbf{X}]^L$). Ce polynôme s'annule donc sur $(P_1, \ldots, P_e)$. Cela prouve qu'il existe $\tau \in L$ tel que $\sum_{i=1}^e (P_i - \tau.\Sigma_i)U_i = 0$. Donc, pour tout $i \in \{1, \ldots, e\}$, $P_i = \tau.\Sigma_i$. □

Nous allons maintenant définir quelques générateurs de l'idéal $\mathfrak{I}$ des syzygies entre les Σ_i.

Le lemme qui suit est valable sans l'hypothèse $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$ (donc $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$ est ici une famille quelconque d'invariants primaires de H).

François Ollivier, que je tiens à remercier ici pour sa contribution, a eu l'idée d'utiliser ce lemme pour démontrer le Théorème 4.14 : il semble en effet que, bien que l'énoncé de ce théorème ne suppose pas la

spécification d'un ordre sur les indéterminées, on simplifie grandement sa démonstration (à supposer qu'il y en eût une autre) en utilisant des bases standard, qui spécifient un ordre particulier ; telle est l'idée que F. Ollivier m'a communiquée.

Pour tout $(i,j) \in \{1,\ldots,e\}^2$, $\Sigma_i\Sigma_j$ appartient à $k[\mathbf{X}]^H$ donc il existe $(A_1^{i,j},\ldots,A_e^{i,j}) \in (k[\mathbf{\Pi}])^e$ tel que $\Sigma_i\Sigma_j = \sum_{k=1}^e A_k^{i,j}\Sigma_k$; nous définissons alors $S_{i,j} = Y_iY_j - \sum_{k=1}^e A_k^{i,j}Y_k \in k[\mathbf{\Pi}][\mathbf{Y}]$. De même, il existe $(B_1,\ldots,B_e) \in (k[\mathbf{X}]^L)^e$ tel que $1 = \sum_{k=1}^e B_k\Sigma_k$, et nous posons $S_0 = \sum_{k=1}^e B_kY_k - 1$ (remarquons qu'en pratique, on choisit souvent les Σ_i homogènes et $\Sigma_1 = 1$, donc $S_0 = Y_1 - 1$).

Lemme 4.13 *La famille $\mathcal{B}$ constituée des $1 + \frac{e(e+1)}{2}$ polynômes S_0 et $S_{i,j}$, $1 \le i \le j \le e$ forme une base standard de $\mathfrak{I}$, considéré comme idéal de l'anneau de polynômes $k[\mathbf{\Pi}][\mathbf{Y}]$ sur l'anneau de base $k[\mathbf{\Pi}]$, pour n'importe quel ordre admissible sur les monômes en $Y_1,\ldots,Y_n$ qui compare les degrés totaux d'abord.*

Preuve – Sur les bases standard, nous nous référons à [20, chap. 2] et aux travaux de Buchberger et d'Hironaka.

Déjà, les éléments de $\mathcal{B}$ engendrent $\mathfrak{I}$: en effet, ils appartiennent tous à $\mathfrak{I}$ par définition, et si l'on appelle $\mathfrak{J} \subset \mathfrak{I}$ l'idéal qu'ils engendrent alors tout polynôme $S \in \mathfrak{I}$ est congru modulo $\mathfrak{J}$ à un polynôme de degré 1 (c'est évident par récurrence puisqu'on peut réduire à des termes linéaires tous les produits Y_iY_j). Il existe donc $S' \in \mathfrak{I}$ de degré 1 tel que $S - S' \in \mathfrak{J}$. Mais alors $S' + CS_0 \in \mathfrak{I}$, où $C \in k[\mathbf{\Pi}]$ désigne le terme constant de S', est une relation linéaire sur $k[\mathbf{\Pi}]$ entre les Σ_i qui forment une famille libre sur $k[\mathbf{\Pi}]$, donc $S' + CS_0 = 0$, d'où $S' \in \mathfrak{J}$ et $S \in \mathfrak{J}$. On a donc montré que $\mathfrak{I} = \mathfrak{J}$, donc les S_0 et $S_{i,j}$, $1 \le i \le j \le e$ engendrent bien $\mathfrak{I}$.

On rappelle (voir [20]) que pour montrer qu'ils en forment une base standard, il suffit de montrer que tous les **S**-polynômes des paires d'éléments de $\mathcal{B}$ dont les monômes dominants ne sont pas étrangers sont réduits à zéro par division par les éléments de $\mathcal{B}$ rangés dans un ordre quelconque. Le monôme dominant d'un $S_{i,j}$ est Y_iY_j, donc le **S**-polynôme d'un $S_{i,j}$ et d'un $S_{i,k}$ (avec $k \neq j$) est $Y_kS_{i,j} - Y_jS_{i,k} = -\sum_{l=1}^e (A_l^{i,j}Y_kY_l - A_l^{i,k}Y_jY_l)$, et la division d'un tel polynôme par la famille $\mathcal{B}$ donne un polynôme de degré 1 qui appartient à $\mathfrak{J}$. Par le même raisonnement que plus haut, ce polynôme est alors de la forme $-CS_0$, où $C \in k[\mathbf{\Pi}]$ désigne son terme constant, et il est donc réduit à zéro par division par S_0. En ce qui concerne le **S**-polynôme de deux polynômes S_0 et $S_{i,j}$ avec $i \neq k_0 \neq j$, où $B_{k_0}Y_{k_0}$ est le monôme dominant de S_0, il s'écrit $Y_iY_jS_0 - B_{k_0}Y_{k_0}S_{i,j}$ et se réduit aussi à 0 par division par $\mathcal{B}$ pour la même raison. On a donc montré que $\mathcal{B}$ constitue une base standard de $\mathfrak{I}$. □

Théorème 4.14 *Avec les hypothèses du Théorème 4.12 (en particulier $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$, soit $\hat{k}$ une clôture algébrique de k et $\mathbf{x} = (x_1,\ldots,x_n) \in \hat{k}^n$. On note $\widetilde{A} = A(x_1,\ldots,x_n)$ la spécialisation en $\mathbf{x}$ d'un élément $A \in k[\mathbf{X}]$, et si $S \in k[\mathbf{X}][Y_1,\ldots,Y_n]$, on note $\widetilde{S}$ le polynôme de $\hat{k}[\mathbf{Y}]$ dont les coefficients sont les spécialisés $\widetilde{A}$ des coefficients A de S. Soit $\widetilde{\mathfrak{I}} \subset \hat{k}[\mathbf{Y}]$ l'idéal $\{\widetilde{S} \;/\; S \in \hat{k} \otimes_k \mathfrak{I}\}$ de $\hat{k}[\mathbf{Y}]$. Alors la variété*

$$V(\widetilde{\mathfrak{I}}) = \{(p_1,\ldots,p_e) \in \hat{k}^e \;\;/\;\; \forall s \in \widetilde{\mathfrak{I}},\; s(p_1,\ldots,p_e) = 0\} \subset \hat{k}^e$$

définie dans $\hat{k}^e$ par l'idéal $\widetilde{\mathfrak{I}}$ est égale à

$$\widetilde{V'} = \{(\widetilde{\tau.\Sigma_1},\ldots,\widetilde{\tau.\Sigma_n}) \;\;/\;\; \tau \in L\}\ .$$

Preuve – Montrons déjà qu'on peut se ramener au cas où les invariants secondaires Σ_i sont homogènes et $\Sigma_1 = 1$. En effet, on sait (Théorème 4.4) qu'il existe une base $(\Sigma'_1,\ldots,\Sigma'_n)$ du $k[\mathbf{\Pi}]$-module $k[\mathbf{X}]^H$ telle que les Σ'_i soient homogènes et $\Sigma'_1 = 1$. Soit $M \in \mathcal{M}(n,k[\mathbf{\Pi}])$ la matrice de passage de la base $(\Sigma_1,\ldots,\Sigma_n)$ à la base $(\Sigma'_1,\ldots,\Sigma'_n)$. Elle est inversible, donc son déterminant, *a priori* dans $k[\mathbf{\Pi}]$, appartient en fait à $k \setminus \{0\}$. Donc, la matrice $\widetilde{M} \in \mathcal{M}(n,\hat{k})$ obtenue en spécialisant les coefficients de M a le même déterminant, et est elle aussi inversible. Or, l'idéal $\mathfrak{I}'$ des syzygies sur $k[\mathbf{\Pi}]$ entre les Σ'_i se déduit de $\mathfrak{I}$

par l'automorphisme de $k[\mathbf{\Pi}][\mathbf{Y}]$ défini par l'action à gauche de la matrice M. Comme $\widetilde{M}$ est inversible, son action à gauche sur $\hat{k}[\mathbf{Y}]$ défini aussi un automorphisme, qui envoie $\widetilde{\mathfrak{I}}$ sur $\widetilde{\mathfrak{I}'}$; donc si le résultat est vrai pour $(\Sigma'_1, \ldots, \Sigma'_n)$ alors il l'est encore pour $(\Sigma_1, \ldots, \Sigma_n)$.

Nous pouvons donc supposer que les Σ_i sont homogènes et que $\Sigma_1 = 1$. Choisissons alors un ordre monomial admissible sur les monômes en les Y_i qui compare les degrés totaux d'abord. On sait d'après le Lemme 4.13 que $\mathcal{B}$ est une base standard de $\mathfrak{I}$ pour un tel ordre. Or, les monômes dominants des polynômes $S_{i,j}$ et S_0 sont tous unitaires (car $S_0 = Y_1 - 1$ et $S_{i,j} = Y_iY_j +$ termes linéaires). Donc par spécialisation, aucun des monômes dominants des éléments de $\mathcal{B}$ ne s'annule. Par conséquent, $\widetilde{\mathcal{B}} = \{\widetilde{S_0}\} \cup \{\widetilde{S_{i,j}} \ / \ 1 \leq i \leq j \leq e\}$ est aussi une base standard de $\widetilde{\mathfrak{I}}$ sur $\hat{k}$. Par suite, les points de $V(\widetilde{\mathfrak{I}})$ dans $\hat{k}^e$ sont exactement les spécialisés des points de $V(\mathfrak{I})$ dans $(k[\mathbf{\Pi}])^e$, d'où $V(\widetilde{\mathfrak{I}}) = \widetilde{V'}$ □

Remarquons que dans le théorème précédent, $\widetilde{V'}$ peut avoir des points multiples, si par exemple $(\tau_1.\Sigma_1, \ldots, \tau_1.\Sigma_e)$ et $(\tau_2.\Sigma_1, \ldots, \tau_2.\Sigma_e)$ se spécialisent en le même point de $\hat{k}^e$.

Remarquons aussi que l'on a donné au passage une base standard $\widetilde{\mathcal{B}}$ de $\widetilde{\mathfrak{I}}$, qui nous sera utile par la suite.

4.4.2 Conséquences pratiques

Supposons que l'on soit dans la situation

$$k[\mathbf{X}]^H = \bigoplus_{i=1}^{e} k[\mathbf{\Pi}]\Sigma_i \quad \text{avec} \quad k[\mathbf{\Pi}] = k[\mathbf{X}]^L$$

où $H \subset L \subset \mathbf{GL}_n(k)$ et L est un groupe fini de réflexions. Nous nous proposons de résoudre un problème analogue à celui du Paragraphe 3.5 : on cherche à spécialiser les éléments de $k[\mathbf{X}]^H$ à partir de la donnée des valeurs spécialisées des éléments de $k[\mathbf{X}]^L = k[\mathbf{\Pi}]$ (donc les valeurs spécialisées des Π_i suffisent) et ici, au lieu d'un élément primitif comme au Par. 3.5, on se donne aussi les valeurs spécialisées de tous les invariants secondaires Σ_i. La Proposition 4.11 permet alors, par la résolution d'un système linéaire de Cramer, d'exprimer l'invariant à spécialiser en fonction des Π_i et Σ_i, et donc de le spécialiser aussi. On peut même, quand le déterminant du système en question ne s'annule pas par spécialisation, résoudre ce système après la spécialisation : c'est moins coûteux. Jusqu'ici, les théorèmes 4.12 et 4.14 n'ont pas servi.

Mais c'est à la détermination des valeurs spécialisées des invariants secondaires Σ_i que vont servir les théorèmes 4.12 et 4.14. En effet, dans le cadre du Paragraphe 3.5, où l'on utilisait un élément primitif Θ de $k(\mathbf{X})^H$ sur $k(\mathbf{X})^L$, les choses étaient simples (voir la Remarque 3.12) : on pouvait calculer le spécialisé de Θ, ou de l'un de ses conjugués $\tau.\Theta$ (auquel cas on spécialisait les éléments de $k(\mathbf{X})^{\tau.H.\tau^{-1}}$ au lieu de ceux de $k(\mathbf{X})^H$).

Ici, on peut aussi calculer le polynôme minimal $\prod_{\tau \in (L//H)_g}(T - \tau.\Sigma_i)$ de chaque Σ_i, le spécialiser (puisque tous ses coefficients appartiennent à $k[\mathbf{\Pi}]$), et calculer ses racines qui seront les valeurs spécialisées des conjugués de $\tau_i.\Sigma_i$ de Σ_i. Le problème est que pour s'en servir ensuite pour spécialiser les éléments d'un $k[\mathbf{X}]^{\tau.H.\tau^{-1}}$, il faut respecter une certaine cohérence : il faut que les Σ_i soient tous modifiés par un même $\tau \in L$. En effet, si $P \in k[\mathbf{X}]^{\tau.H.\tau^{-1}}$ s'écrit $P = A_1\tau.\Sigma_1 + \ldots + A_e\tau_e.\Sigma_e$, il est vrai que $\widetilde{P} = \widetilde{A_1}\widetilde{\tau.\Sigma_1} + \ldots + \widetilde{A_e}\widetilde{\tau.\Sigma_e}$ mais on ne pourra rien tirer de la connaissance des $\widetilde{\tau_i.\Sigma_i}$ avec des $\tau_i \in L$ quelconques sans lien entre eux.

Le Théorème 4.14 nous permet d'assurer cette cohérence : il montre que si l'on utilise non seulement les polynômes minimaux de chacun des Σ_i, mais aussi toutes les syzygies entre eux, alors on est assuré que les valeurs spécialisées $\sigma_1, \ldots, \sigma_e$ que l'on obtient s'écrivent toutes $\sigma_i = \widetilde{\tau.\Sigma_i}$ avec le même $\tau \in L$.

Pour cette raison, le Théorème 4.14 sera essentiel pour l'application des résultats de théorie des invariants de ce chapitre aux seconde et troisième parties.

Remarque 4.15 *En pratique, résoudre les systèmes des syzygies est très simple : on calcule d'abord le polynôme minimal de chaque Σ_i (c'est une syzygie), on le spécialise et on détermine ses e racines. Cela donne donc e^e solutions potentielles pour $(\widetilde{\Sigma_1}, \ldots, \widetilde{\Sigma_e})$. On teste alors pour chacune d'entre elles si elle annule les polynômes $\widetilde{S_{i,j}}$ définis dans la démonstration du Théorème 4.14, et l'on sait que seules les e vraies solutions résisteront à ce test.*

Chapitre 5

Une preuve constructive d'un théorème de Mattuck

Dans ce chapitre, k est un corps commutatif de caractéristique quelconque. Nous nous proposons d'apporter une contribution au problème de Noether, à savoir (voir [38]) :

Problème de Noether : *Un sous-groupe fini G du groupe linéaire $\mathbf{GL}_n(k)$ étant donné, le corps $k(X_1, \ldots, X_n)^G$ des invariants fractionnaires de G est-il une extension pure de k.*

Cette contribution consiste en la donnée d'une preuve très élémentaire et constructive au résultat bien connu suivant : la réponse au problème de Noether pour un groupe de permutations $G \subset \mathfrak{S}_n$ agissant diagonalement sur p paquets de n indéterminées est affirmative dès lors qu'elle est affirmative quand le même groupe G agit simplement sur n indéterminées. Ce qui est nouveau ici est que la preuve que nous donnons fournit explicitement une base de transcendance pure et résout donc constructivement le problème de Noether.

$\star$

Soit np indéterminées indépendantes $(X_{i,j})_{1\leq i\leq p, 1\leq j\leq n}$ sur un corps commutatif k. Soit $G \subset \mathfrak{S}_n$ un sous-groupe du groupe symétrique $\mathfrak{S}_n$. On le munit de son action à gauche naturelle sur $K = k(X_{1,1}, \ldots, X_{1,n})$ définie par $g.X_{1,i} = X_{1,g(i)}, g \in G, 1 \leq i \leq n$ et par sa compatibilité avec les structures de corps et de k-algèbre de K. Nous notons K^G l'algèbre des invariants de G dans K pour cette action. On définit aussi l'action par blocs de G sur $L = k((X_{i,j})_{1\leq i\leq p, 1\leq j\leq n})$ par $\forall g \in G, \forall i, \forall j, g.X_{i,j} = X_{i,g(j)}$ et par sa compatibilité avec les structures de corps et de k-algèbre de L. On note L^G l'algèbre des invariants de G dans L pour cette action (on parle parfois dans la littérature d'*invariants vectoriels* en désignant les invariants pour cette action par blocs de G).

Le théorème qui suit a d'abord été prouvé par A. Mattuck dans [50] dans le cas où G est le groupe symétrique $\mathfrak{S}_n$ tout entier. Dans le cas général, ce théorème est une conséquence d'un théorème de Miyata (voir [53] ou [38, p. 68, Proposition 3.18]).

Théorème 5.1 *Si K^G est une extension transcendante pure de k, alors L^G aussi.*

Le but de ce chapitre est de donner une preuve constructive du Théorème 5.1, en exhibant une base de transcendance pure de L^G en fonction des éléments d'une base de transcendance pure de K^G.

$\star$

Soit T une indéterminée sur L. Nous définissons pour tout $i \in \{2, \ldots, p\}$ le polynôme suivant :

$$P_i = \sum_{j=1}^{n} X_{ij} \prod_{k \neq j} \frac{T - X_{1,k}}{X_{1,j} - X_{1,k}} \in L^G[T] \qquad \text{(polynôme interpolateur de Lagrange).}$$

Il satisfait $P_i(X_{1,j}) = X_{i,j}$ pour tout $i \in \{2, \ldots, p\}$ et tout $j \in \{1, \ldots, n\}$.

Soit $(\Theta_{1,1}, \ldots, \Theta_{1,n})$ une base de transcendance pure de K^L sur k. Nous définissons alors la famille $(\Theta_{i,j})_{2 \leq i \leq p, 1 \leq j \leq n} \in (L^G)^{n(p-1)}$ de la façon suivante :

$$P_i = \sum_{j=1}^{n} \Theta_{i,j} T^{j-1}, \qquad \text{pour } 2 \leq i \leq p.$$

Alors on a :

Théorème 5.2 *$(\Theta_{i,j})_{1 \leq i \leq p, 1 \leq j \leq n}$ est une base de transcendance pure de L^G sur le corps k.*

Proof – En effet, les polynômes $\Theta_{i,j}$ appartiennent à L^G, et si f appartient à L^G, alors grâce aux égalités $X_{i,j} = P_i(X_{1,j})$ pour $2 \leq i \leq p$ et $1 \leq j \leq n$, nous pouvons trouver un polynôme g tel que $f = g(X_{1,1}, \ldots, X_{1,n})$, avec $g \in F(Y_1, \ldots, Y_n)^G$ où $F = k((\Theta_{i,j})_{2 \leq i \leq p, 1 \leq j \leq n})$. Or, on a $F(X_{1,1}, \ldots, X_{1,n})^G = F \otimes_k k(X_{1,1}, \ldots, X_{1,n})^G = F \otimes_k k(\Theta_{1,1}, \ldots, \Theta_{1,n}) = F(\Theta_{1,1}, \ldots, \Theta_{1,n})$. Par suite, le corps L^G est égal à $k((\Theta_{i,j})_{1 \leq i \leq p, 1 \leq j \leq n})$. Mais comme G est fini, le degré de transcendance de L^G sur k est précisément np d'après la Proposition 1.3, c'est-à-dire le cardinal de la famille $(\Theta_{i,j})_{1 \leq i \leq p, 1 \leq j \leq n}$. Cette famille forme donc une base pure de L^G sur k. □

Remarque : La preuve du Théorème 5.2 donnée ci-dessus fournit même un algorithme permettant d'exprimer un élément donné de $f \in L^G$ comme fraction rationnelle à coefficients dans k en les éléments $\Theta_{i,j}$ de la base pure de L^G, pour peu que l'on ait déjà un algorithme permettant d'exprimer les éléments de K^G en fonction de sa base pure $(\Theta_{1,1}, \ldots, \Theta_{1,n})$.

Exemple : Soit $n = 4$ et $p = 2$. Le groupe diédral $G =< (12), (1324) > \simeq \mathfrak{D}_4$, $G \subset \mathfrak{S}_4$, agit naturellement sur $k(\mathbf{X}) = k(X_1, X_2, X_3, X_4)$ et agit diagonalement sur $k(\mathbf{X}, \mathbf{Y}) = k(X_1, X_2, X_3, X_4, Y_1, Y_2, Y_3, Y_4)$ en permutant les colonnes de la matrice

$$\begin{pmatrix} X_1 & X_2 & X_3 & X_4 \\ Y_1 & Y_2 & Y_3 & Y_4 \end{pmatrix}.$$

On sait (voir la Prop. 3.3) que $k(\mathbf{X})^G = k(\Theta_1, \Theta_2, \Theta_3, \Theta_4)$ avec $\Theta_1 = X_1 + X_2 + X_3 + X_4$, $\Theta_2 = X_1X_2 + X_3X_4$, $\Theta_3 = X_1(X_2(X_3 + X_4) + X_3X_4) + X_2X_3X_4$ et $\Theta_4 = X_1X_2X_3X_4$. Alors le résultat du Théorème 5.2 prouve que $k(\mathbf{X}, \mathbf{Y})^G = k(\Theta_1, \Theta_2, \Theta_3, \Theta_4, \Psi_1, \Psi_2, \Psi_3, \Psi_4)$ avec

$\Delta_i = \prod_{k \neq i}(X_i - X_k)$, et $\quad \Psi_1 = \frac{Y_1}{\Delta_1} + \frac{Y_2}{\Delta_2} + \frac{Y_3}{\Delta_3} + \frac{Y_4}{\Delta_4}$,

$\Psi_2 = \frac{Y_1(X_2+X_3+X_4)}{\Delta_1} + \frac{Y_2(X_3+X_4+X_1)}{\Delta_2} + \frac{Y_3(X_4+X_1+X_2)}{\Delta_3} + \frac{Y_4(X_1+X_2+X_3)}{\Delta_4}$,

$\Psi_3 = \frac{Y_1(X_2X_3+X_3X_4+X_4X_2)}{\Delta_1} + \frac{Y_2(X_3X_4+X_4X_1+X_1X_3)}{\Delta_2} + \frac{Y_3(X_4X_1+X_1X_2+X_2X_4)}{\Delta_3} + \frac{Y_4(X_1X_2+X_2X_3+X_3X_1)}{\Delta_4}$,

$\Psi_4 = \frac{Y_1X_2X_3X_4}{\Delta_1} + \frac{Y_2X_3X_4X_1}{\Delta_2} + \frac{Y_3X_4X_1X_2}{\Delta_3} + \frac{Y_4X_1X_2X_3}{\Delta_4}$.

Remerciements.- Je tiens particulièrement à remercier B. Sturmfels, qui m'a appris entre autres choses l'existence du théorème de Mattuck, et G. Kemper qui m'a indiqué le théorème de Miyata.

Deuxième partie

Le problème direct de la théorie de Galois

Chapitre 6

Généralités

Nous nous proposons d'étudier dans cette partie le problème direct de la théorie de Galois, c'est-à-dire la détermination du groupe de Galois d'un polynôme $f \in k[T]$ et de la façon dont ce groupe opère sur l'ensemble des racines de f.

Dans toute cette partie, k sera un corps commutatif effectif (c'est-à-dire qu'on peut effectuer algorithmiquement les calculs algébriques et les tests de nullité sur k), et tel qu'il existe des algorithmes de factorisation pour les polynômes à une indéterminée à coefficients dans k.

Par exemple, $\mathbb{Q}$, $\mathbb{F}_{p^\alpha}$, $\mathbb{Q}(U)$, $\mathbb{Q}(U)/(P)$ où $P \in k[U]$ est irréductible sur $\mathbb{Q}$, $\mathbb{F}_{p^\alpha}(U_1, \ldots, U_m)$ sont de tels corps.

Le présent chapitre donne une vue générale des méthodes existant pour déterminer le groupe de Galois d'un polynôme, ainsi que les résultats qu'elles utilisent, en insistant sur ceux dont nous aurons besoin par la suite. Les propositions présentées dans ce chapitre sont donc déjà connues pour l'essentiel, même si elles sont parfois reformulées.

6.1 Représentation par permutations du groupe de Galois

Soit $f \in k[T]$ un polynôme unitaire et séparable, n son degré, $\mathbf{x} = (x_1, \ldots, x_n)$ la famille de ses racines dans une extension algébriquement close $\dot{k}$ de k (cela suppose la donnée d'une numérotation particulière des racines), de sorte que $f = \prod_{i=1}^{n}(T - x_i)$.

Rappelons que le *groupe de Galois* de f sur le corps k, noté $\mathrm{Gal}_k(f)$, est par définition le groupe des automorphismes de la k-algèbre $k(\mathbf{x})$, ou encore le groupe des automorphismes du corps $k(\mathbf{x})$ qui laissent invariants tous les points de k. Rappelons aussi que les éléments de $\mathrm{Gal}_k(f)$ laissent globalement invariant l'ensemble de racines de f (puisqu'ils laissent invariantes les expressions polynomiales symétriques en ces racines car elles appartiennent à k), et qu'il opère fidèlement sur l'ensemble de ces racines (en effet, un élément de $\mathrm{Gal}_k(f)$ qui fixe chaque racine x_i laisse $k(\mathbf{x})$ invariant point par point et est donc l'identité).

La numérotation particulière $\mathbf{x} = (x_1, \ldots, x_n)$ définit donc une opération fidèle de $\mathrm{Gal}_k(f)$ sur l'ensemble $\{1, \ldots, n\}$ des indices des racines. En d'autres termes, $\mathrm{Gal}_k(f)$ est isomorphe à un sous-groupe Γ de $\mathfrak{S}_n$, où l'isomorphisme $\varphi : \mathrm{Gal}_k(f) \longrightarrow \Gamma$ vérifie

$$\forall i \in \{1, \ldots, n\}, \forall g \in \mathrm{Gal}_k(f), \varphi(g)(i) = g(x_i).$$

Le groupe Γ et l'isomorphisme φ ne sont absolument pas canoniques, ils dépendent de la numérotation $\mathbf{x}$ des racines.

Par contre, la classe d'équivalence de Γ dans $\mathfrak{S}_n$, que nous noterons $[\Gamma]$, est canonique : en effet, une autre numérotation des racines de f conduit à un sous-groupe $\Gamma' \subset \mathfrak{S}_n$ conjugué de Γ dans $\mathfrak{S}_n$.

De façon générale, nous noterons $[H]_L$ la classe de conjugaison dans L d'un sous-groupe H de $L \subset \mathfrak{S}_n$, et nous omettrons l'indice quand $L = \mathfrak{S}_n$.

C'est donc cette classe de conjugaison $[\Gamma]$ que nous nous proposons d'identifier, à partir de la connaissance des coefficients de f. C'est bien sûr plus précis que déterminer $\mathrm{Gal}_k(f)$ à isomorphisme près. La donnée de la classe de conjugaison $[\Gamma]$ renseigne en effet non seulement sur le groupe abstrait (ce qui est suffisant pour savoir s'il est résoluble par exemple) mais aussi, et de manière canonique, sur la façon dont ce groupe opère sur l'ensemble $\{x_1, \ldots, x_n\}$ des racines de f.

6.2 Résolvantes de Lagrange

Les résolvantes furent introduites par Lagrange (voir [44], [45],[46]) dans le but de calculer les relations entre les racines d'un polynôme et d'étudier (dans le langage du XVIII$^{\mathrm{e}}$ siècle) l'extension de corps engendrée par ces racines. Cela permit à Lagrange d'unifier les méthodes (Cardan, Ferrari) qui étaient utilisées pour résoudre les équations algébriques de degré inférieur ou égal à 4. Cela lui permit même de présentir, en attendant que Galois le montre rigoureusement, qu'il ne pouvait exister de solution par radicaux de l'équation générique de degré 5 ou qu'en tout cas des méthodes du type de celles utilisées pour les degrés inférieurs ne pouvaient plus s'appliquer : en effet, jusqu'au degré 4, on pouvait trouver des résolvantes de degré inférieur à celui du polynôme de départ : résolvante de degré 2 pour le degré 3 (méthode de Cardan) et résolvante de degré 3 pour le degré 4 (méthode de Ferrari), et on pouvait procéder par étapes, c'est-à-dire calculer les racines de la résolvante (par radicaux) et en déduire celles de l'équation. Pour un degré $n \geq 5$ au contraire, les résolvantes intéressantes sont toutes de degré supérieur à n, et elles ramènent donc à un problème plus compliqué que le problème de départ.

Pour nous, les résolvantes seront un outil pour la détermination du groupe de Galois : Nous ne traiterons pas ici le problème de la résolution par radicaux.

Les notations que nous utilisons sont celles de [7], introduites par Arnaudiès et Valibouze.

Définition 6.1 *Soit L un sous-groupe de $\mathfrak{S}_n$ et H un sous-groupe de L. Soit Ψ un invariant primitif de H relatif à L (voir la Définition 1.1). On appelle* résolvante générique de Ψ relative à L *le polynôme*

$$\mathcal{L}_\Psi^L = \prod_{\sigma \in (L//H)_g} (T - (\sigma.\Psi)(X_1, \ldots, X_n)) \in k[\mathbf{X}]^L[T] \ ,$$

où $(L//H)_g$ désigne un ensemble de représentants des classes à gauche de H dans L.

Quand $L = \mathfrak{S}_n$, on parle de résolvante absolue *au lieu de résolvante relative, et on note $\mathcal{L}_\Psi$ pour $\mathcal{L}_\Psi^{\mathfrak{S}_n}$.*

Proposition 6.2 *Sous les hypothèses qui précèdent, $\mathcal{L}_\Psi^L$ est le polynôme minimal de Ψ sur le corps $k(\mathbf{X})^L$.*

Preuve – Par définition, $\mathcal{L}_\Psi^L$ appartient à $k(\mathbf{X})^L$, est unitaire et admet Ψ pour racine. En outre, son degré est aussi d'après le Théorème 3.1 le degré de l'extension $k(\mathbf{X})^H : k(\mathbf{X})^L$; d'où le résultat. □

$\star$

Soit f un polynôme comme au paragraphe 6.1, et Γ la représentation de son groupe de Galois dans $\mathfrak{S}_n$ définie par la numérotation $\mathbf{x} = (x_1, \ldots, x_n)$ des racines de f.

Si L contient Γ, alors tout coefficient P de $\mathcal{L}_\Psi^L$, qui est par définition un invariant de L, appartient à $k[\mathbf{X}]^\Gamma$. Donc $P(\mathbf{x}) = P(x_1, \ldots, x_n)$ appartient à $k(\mathbf{x})$ et est invariant sous l'action de $\mathrm{Gal}_k(f) = \mathrm{Gal}(k(\mathbf{x}) : k)$ donc appartient à k.

On peut donc poser la définition suivante :

Définition 6.3 *Si $\Gamma \subset L$, alors on définit la* résolvante de Ψ relative à L spécialisée en la famille $\mathbf{x} = (x_1, \ldots, x_n)$ des racines de f *comme étant :*

$$\mathcal{L}^L_{\Psi,\mathbf{x}} = \prod_{\sigma \in (L//H)_g} (T - (\sigma.\Psi)(x_1, \ldots, x_n)) \in k[T]$$

c'est-à-dire l'évaluation de $\mathcal{L}^L_\Psi$ sur $\mathbf{x} = (x_1, \ldots, x_n)$. Elle appartient bien à $k[T]$ d'après ce qui précède.

Quand $L = \mathfrak{S}_n$, on parle de résolvante absolue *au lieu de résolvante relative, et on note $\mathcal{L}_{\Psi,\mathbf{x}}$ pour $\mathcal{L}^{\mathfrak{S}_n}_{\Psi,\mathbf{x}}$.*

Remarque 6.4 *Remarquons que $\mathcal{L}^L_{\Psi,\mathbf{x}}$ dépend explicitement de la numérotation $\mathbf{x}$ choisie pour les racines de f, sauf quand $L = \mathfrak{S}_n$ (résolvante absolue) car alors les coefficients de $\mathcal{L}_\Psi$ appartiennent à $k[\mathbf{X}]^{\mathfrak{S}_n}$. Pour les résolvantes absolues uniquement, on pourra donc noter $\mathcal{L}_{\Psi,f}$ au lieu de $\mathcal{L}_{\Psi,\mathbf{x}}$.*

Exemple 6.5 (Méthode de Cardan) *Pour $n = 3$ et $k = \mathbb{Q}(j)$, où $j = e^{\frac{2i\pi}{3}}$, le polynôme $\Psi = (X_1 + jX_2 + j^2X_3)^3$ est un invariant primitif du groupe alterné $\mathfrak{A}_3$. Son seul conjugué sous $\mathfrak{S}_3$ est $\Psi' = (X_1 + j^2X_2 + jX_3)^3$. La résolvante associée, que nous calculons grâce au domaine* `PolynomesSymetriques` *du chapitre 2, est alors*

$$\mathcal{L}_\Psi = (T - \Psi)(T - \Psi') = T^2 - (2E_1^3 - 9E_2E_1 + 27E_3)T + E_1^6 - 9E_2E_1^4 + 27E_2^2E_1^2 - 27E_2^3 \in k[\mathbf{E}][T]$$

où les E_i sont les polynômes symétriques élémentaires, qui se spécialisent, au signe près, en les coefficients de f. La méthode de Cardan consiste à résoudre par radicaux l'équation du second degré $\mathcal{L}_{\Psi,f} = 0$ pour trouver les valeurs $\psi = \Psi(x_1, x_2, x_3)$ et $\psi' = \Psi'(x_1, x_2, x_3)$, et à en déduire x_1, x_2 et x_3.

Exemple 6.6 (Méthode de Ferrari) *Ici $n = 4$. On pose $\Psi = X_1X_2 + X_3X_4$, invariant primitif du groupe $H =< (1\,3\,2\,4), (1\,2) >\simeq \mathfrak{D}_4$. Il admet les conjugués $\Psi' = X_1X_3 + X_2X_4$ et $\Psi'' = X_1X_4 + X_2X_3$ sous l'action de $\mathfrak{S}_4$. La résolvante associée, calculée elle aussi grâce au domaine* `PolynomesSymetriques`*, est*

$$\mathcal{L}_\Psi = (T - \Psi)(T - \Psi')(T - \Psi'') = T^3 - E_2T^2 + (E_3E_1 - 4E_4)T - E_4E_1^2 + 4\ E_4E_2 - E_3^2 \in k[\mathbf{E}][T].$$

La méthode de Ferrari consiste à résoudre par radicaux l'équation du troisième degré $\mathcal{L}_{\Psi,f} = 0$ pour calculer $\psi = \Psi(\mathbf{x})$, $\psi' = \Psi'(\mathbf{x})$, $\psi'' = \Psi''(\mathbf{x})$, et à en déduire la valeur $\mathbf{x} = (x_1, x_2, x_3, x_4)$ des racines de f.

Définition 6.7 *Un invariant primitif Ψ relatif à un groupe L (resp. la résolvante $\mathcal{L}^L_\Psi$) sera dit* $\mathbf{x}$*-séparable si et seulement si $\mathcal{L}^L_{\Psi,\mathbf{x}}$ est séparable.*

Remarquons que comme le polynôme f, et donc l'extension $k(\mathbf{x}) : k$, sont séparables par hypothèse, les facteurs irréductibles de $\mathcal{L}^L_{\Psi,\mathbf{x}}$ sont aussi tous séparables. La non-séparabilité de $\mathcal{L}^L_{\Psi,\mathbf{x}}$ ne peut donc venir que de l'apparition de facteurs multiples lors de la spécialisation de $\mathcal{L}^L_\Psi$, qui elle est séparable sur $k(\mathbf{X})^L$.

Signalons le résultat [7, Théorème 6.5] qui montre que si $\mathcal{L}^L_{\Psi,\mathbf{x}}$ admet un facteur multiple h^ν (h irréductible sur k) et si Ψ' est un autre H-invariant primitif L-relatif tel que $\mathcal{L}^L_{\Psi',\mathbf{x}}$ soit séparable, alors le facteur «parallèle» à h^ν dans $\mathcal{L}^L_{\Psi',\mathbf{x}}$ (c'est-à-dire le facteur dont les racines dans $\hat{k}$ sont obtenues en spécialisant les mêmes éléments de $k(\mathbf{X})^H$) est un produit de polynômes irréductibles de degrés multiples de celui de h.

Signalons aussi que l'on peut toujours se ramener à une résolvante séparable quitte à effectuer une transformation sur le polynôme f, qui laisse inchangé son corps de décomposition, donc son groupe de Galois, et même l'action de ce groupe sur l'ensemble des racines : voir la Proposition 8.5, où est donnée une borne sur le nombre d'essais à effectuer avant d'être certain d'obtenir une résolvante séparable.

La résolvante $\mathcal{L}^L_{\Psi,\mathbf{x}}$ a donc pour degré l'indice $[L : H]$ du groupe H dans le groupe L. Sa factorisation sur le corps k renseignera sur le groupe de Galois de f sur k.

6.3 Résolvante et groupe de Galois

Dans cette section nous mettons en évidence l'utilité des résolvantes pour la détermination du groupe de Galois d'un polynôme, et nous présentons les résultats qui sont à la base de toutes les méthodes qui utilisent des résolvantes. Commençons par des considérations sur les groupes.

Définition 6.8 *Soit L un sous-groupe de $\mathfrak{S}_n$, et G et H deux sous-groupes de L. On fait agir G sur l'ensemble $(L/H)_g$ des classes à gauche de H dans L. Soit $\{O_1, \ldots, O_r\}$ la partition de $(L/H)_g$ en les orbites pour cette action. Nous noterons $\varpi^L(G, H)$ la famille $(n_1, \ldots, n_r) \in \mathbb{N}^r$, supposée ordonnée de façon décroissante, des cardinaux des orbites O_i ($n_i = \mathrm{Card}(O_i)$). Elle vérifie $n_1 + \ldots + n_r = [L : H]$.*

Pour tout $i \in \{1, \ldots, r\}$, on note $S_i = \mathcal{S}tab_L(O_i)$. Alors S_i agit par restriction sur O_i, ensemble de cardinal n_i, ce qui définit à conjugaison près une représentation, pas forcément fidèle en général, de S_i dans $\mathfrak{S}_{n_i}$. Soit $G_i \subset \mathfrak{S}_{n_i}$ l'image de S_i par cette représentation, qui est donc isomorphe à un quotient de S_i. Alors G_i dépend de la numérotation des éléments de O_i, mais sa classe de conjugaison $[G_i]_{\mathfrak{S}_{n_i}}$ n'en dépend plus. On note $\varpi'^L(G, H) = ([G_1]_{\mathfrak{S}_{n_1}}, \ldots, [G_r]_{\mathfrak{S}_{n_r}})$ la famille de ces classes de conjugaison.

Proposition 6.9 *Les familles $\varpi^L(G, H)$ et $\varpi'^L(G, H)$ ne dépendent de G et H que par leur classe de conjugaison respective, $[G]_L$ et $[H]_L$, sous l'action de L.*

Preuve – Pour $\varpi^L(G, H)$, voir [7, Par. 3.2]. Le cas de $\varpi'^L(G, H)$ est laissé en exercice. □

Le calcul des familles $\varpi^L(G, H)$ et $\varpi'^L(G, H)$ a été implanté dans le langage GAP [58] par A. Valibouze.

Théorème 6.10 (Groupe de Galois des résolvantes) *Soit $H \subset L$ deux sous-groupes finis de $\mathfrak{S}_n$ et Ψ un H-invariant primitif L-relatif tel que $\mathcal{L}^L_{\Psi,\mathbf{x}}$ soit séparable. Soit $e = [L : H]$ le degré de cette résolvante. Le groupe $\Gamma \subset L$ (qui a été défini au Paragraphe 6.1) agit par produit à gauche sur $(L/H)_g$, ce qui définit, si l'on a numéroté les e éléments de $(L/H)_g$, une représentation de Γ dans $\mathfrak{S}_e$. Soit $\Gamma' \subset \mathfrak{S}_e$ l'image de Γ par cette représentation (Γ' est donc isomorphe à un quotient de Γ). La classe de conjugaison $[\Gamma']_{\mathfrak{S}_e}$ de Γ' dans $\mathfrak{S}_e$ ne dépend plus du choix de la numérotation des éléments de $(L/H)_g$: elle ne dépend que de L, $[H]_L$ et $[\Gamma]_L$.*

D'autre part, $\mathrm{Gal}_k(\mathcal{L}^L_{\Psi,\mathbf{x}})$ opère fidèlement sur l'ensemble des e racines de $\mathcal{L}^L_{\Psi,\mathbf{x}}$, ce qui définit, pour une numérotation donnée (arbitraire) de ces racines, un sous-groupe M de $\mathfrak{S}_e$ isomorphe à $\mathrm{Gal}_k(\mathcal{L}^L_{\Psi,\mathbf{x}})$. Le théorème affirme alors que : $[\Gamma']_{\mathfrak{S}_e} = [M]_{\mathfrak{S}_e}$ (les groupes Γ' et M sont conjugués dans $\mathfrak{S}_e$).

Preuve – Voir [70, Theorem 3], où le résultat est montré pour les groupes abstraits, et [28] où il est montré pour les opérations de groupes. □

Ce théorème peut être utilisé de la façon suivante : on calcule *a priori* les différentes classes $[\Gamma']_{\mathfrak{S}_e}$ correspondant aux diverses possibilités pour les classes $[\Gamma]_L$ et $[H]_L$. On calcule ensuite pour certains $[H]_L$ des résolvantes et la représentation dans $\mathfrak{S}_e$ de leur groupe de Galois, et on utilise le résultat du

théorème pour exclure des candidats à être représentation du groupe de Galois de f, jusqu'à ce qu'il n'en reste plus qu'un seul.

Le théorème cependant n'est pas très intéressant par lui-même en pratique, car les résolvantes sont le plus souvent de degré plus élevé que le polynôme f de départ, et calculer leur groupe de Galois est donc plus compliqué en général que calculer celui de f. Par contre, on peut s'intéresser aux facteurs irréductibles sur k des résolvantes, ce que permettent les corollaires qui suivent.

Corollaire 6.11 (Groupe de Galois des facteurs irréductibles des résolvantes) *En gardant les hypothèses du Théorème 6.10 (toujours en supposant $\mathcal{L}^L_{\Psi,\mathbf{x}}$ séparable), soit $(h_1,\ldots,h_s)$ la famille des facteurs irréductibles sur k de $\mathcal{L}^L_{\Psi,\mathbf{x}}$, et m_i le degré de h_i. Soit M_i la représentation de $\mathrm{Gal}_k(h_i)$ dans $\mathfrak{S}_{m_i}$ définie par une certaine numérotation (arbitraire) des racines de h_i. Alors, la famille $([M_1]_{\mathfrak{S}_{m_1}},\ldots,[M_s]_{\mathfrak{S}_{m_s}})$ est égale, à l'ordre près de ses éléments, à $\varpi'^L(\Gamma,H)$.*

Preuve – Voir [70, Theorem 4], et l'adapter aux actions de groupes (exercice).

Corollaire 6.12 (Degrés des facteurs irréductibles des résolvantes) *Sous les hypothèses précédentes, on a en particulier $r=s$ et $(m_1,\ldots,m_r)$ est égale, à l'ordre près de ses éléments, à la famille $\varpi^L(\Gamma,H)$.*

Preuve – Cela résulte du Corollaire 6.11. Voir aussi [7, Théorème 6.6], qui traite le cas où les résolvantes ne sont pas nécessairement séparables. Notons que dans [7], $\varpi^L(\Gamma,H)$ désigne la suite duale (au sens de [6]) de celle que nous considérons ici. □

Corollaire 6.13 (Racine de la résolvante) *Avec les hypothèses qui précèdent, H contient un conjugué dans L de Γ si et seulement si $\mathcal{L}^L_{\Psi,\mathbf{x}}$ a une racine dans k.*

Le Corollaire 6.13 peut s'écrire d'ailleurs avec les hypothèses plus faibles que voici (où $\mathcal{L}^L_{\Psi,\mathbf{x}}$ n'est plus nécessairement séparable) :

Proposition 6.14 *Soit Ψ un H-invariant L-relatif (où $H\subset L\subset\mathfrak{S}_n$) et $\psi=\Psi(\mathbf{x})$ sa spécialisation en les racines de f. Alors*

i. Si $\Gamma\subset H$ alors $\psi\in k$.

ii. Si $\psi\in k$ et est racine simple de $\mathcal{L}^L_{\Psi,\mathbf{x}}$, alors $\Gamma\subset H$.

Preuve – Voir [61] et [7, Th. 5.2]. □

Arnaudiès et Valibouze on montré la généralisation suivante de cette proposition :

Proposition 6.15 *Soit Ψ un H-invariant L-relatif (où $H\subset L\subset\mathfrak{S}_n$ et $\Gamma\subset L$). Posons $\psi=\Psi(\mathbf{x})$. Notons $\Psi_1,\ldots,\Psi_e$ les conjugués de $\Psi=\Psi_1$ dans l'extension $k(\mathbf{X})^H$ de $k(\mathbf{X})^L$. Soit $C_i=\{s\in L\ /\ s.\Psi=\Psi_i\}$. Soit h le facteur unitaire irréductible dans $k[T]$ de $\mathcal{L}^L_{\Psi,\mathbf{x}}$ qui s'annule en ψ. Supposons la numérotation (Ψ_i) choisie de sorte que $h(T)=(T-\Psi_1(\mathbf{x}))\ldots(T-\Psi_r(\mathbf{x}))$, $1\le r\le e$. Notons $S=\mathcal{S}tab_L(\{\Psi_1,\ldots,\Psi_r\})$. Alors :*

i. L'orbite de Ψ sous l'action de Γ est $\Gamma.\Psi=\{\Psi_1,\ldots,\Psi_r\}$.

ii. On a $\Gamma\subset S\subset\bigcup_{i=1}^r C_i$, et $[S:\Gamma]=[S\bigcap H:\Gamma\bigcap H]$.

Preuve – Voir [7, Th. 5.3]. □

6.4 Revue des méthodes

Nous présentons ici les différentes méthodes utilisées pour résoudre le problème direct de la théorie de Galois, c'est-à-dire identifier le groupe de Galois d'un polynôme $f \in k[T]$ donné par ses coefficients.

6.4.1 Méthodes numériques

Nous rangeons dans la catégorie *méthodes numériques* toutes les méthodes qui utilisent des approximations des racines du polynôme f. Cela suppose que f est à coefficients dans $\mathbb{Q}$, voire $\mathbb{Q}(U_1, \ldots, U_m)$ (cf. [21, Par. 1.2.4]). Quitte à appliquer une transformation affine aux racines, ce qui laisse invariant le groupe de Galois, on peut même supposer $f \in \mathbb{Z}[T]$. On se donne donc alors des approximations des racines dans $\mathbb{C}$, par exemple

$$x_1 = -12.0159713 + 0.2798203\, i, \quad x_2 = 0.0001345 - 3.1648291\, i, \ \ldots$$

À cause de cela, les méthodes numériques se distinguent essentiellement des autres : en effet, se donner des valeurs approchées des racines fixe une numérotation de ces racines, ce que ne fait pas la seule donnée des coefficients. Par conséquent, les méthodes numériques peuvent permettre d'identifier le sous-groupe $\Gamma \subset \mathfrak{S}_n$ précis, quand les autres méthodes ne permettent par essence que d'identifier sa classe de conjugaison $[\Gamma]$ dans $\mathfrak{S}_n$ (voir le Paragraphe 6.1).

Méthode de Stauduhar: Les méthodes numériques furent introduites par Stauduhar (voir [61]), qui utilise la Proposition 6.14 pour déterminer Γ. Le principe est le suivant. On construit le graphe d'inclusion de tous les sous-groupes de $\mathfrak{S}_n$ (en se limitant aux groupes transitifs quand f est irréductible), et on part de sa racine, $\mathfrak{S}_n$. On prend $L = \mathfrak{S}_n$, H un sous-groupe maximal (pour l'inclusion) de $\mathfrak{S}_n$, Ψ un invariant primitif de H relatif à L (donc absolu pour cette première étape où $L = \mathfrak{S}_n$). On calcule la résolvante $\mathcal{L}^L_{\Psi,\mathbf{x}}$ grâce à des approximations suffisamment précises des racines de f, sachant que les coefficients de cette résolvante sont des entiers (un calcul d'erreur permet alors de déterminer avec certitude ces coefficients entiers). Si $\mathcal{L}^L_{\Psi,\mathbf{x}}$ est séparable, la Proposition 6.14 permet alors de tester si Γ est inclus dans un conjugué dans L de H : ce sera vrai si et seulement si $\mathcal{L}^L_{\Psi,\mathbf{x}}$ admet une racine dans k, ce que l'on peut tester par un algorithme de factorisation. On peut même tester précisément quelle racine de $\mathcal{L}^L_{\Psi,\mathbf{x}}$ appartient à k, et identifier ainsi le conjugué précis de H qui contient Γ.

Aussi, si Γ est inclus dans un conjugué H' de H, on poursuit l'algorithme en remplaçant L par H' dans ce qui précède. Si au contraire Γ n'est pas inclus dans un conjugué de H, on poursuit avec le même groupe L, mais en remplaçant H par un autre sous-groupe maximal de L qui ne soit pas conjugué de H.

L'algorithme s'arrête quand on a obtenu un groupe L, qui contient donc Γ d'après l'algorithme, et dont aucun sous-groupe maximal ne contient Γ : on sait alors que $\Gamma = L$.

Améliorations La méthode de Stauduhar a été poursuivie notamment par Olivier, Eichenlaub (voir [21, 22]) et Geyer (voir [27]).

Eichenlaub donne dans [21, Par. 2.1.3] une évaluation de la précision qu'il faut se donner sur les racines des résolvantes pour pouvoir tester leur appartenance à $\mathbb{Z}$. On peut ainsi se passer du calcul de la résolvante complète et tester directement si une racine dans $\mathbb{C}$ d'une résolvante, dont on a calculé une approximation, appartient ou non en fait à $\mathbb{Z}$ (ce qui équivaut à ce qu'elle appartienne à $\mathbb{Q}$ car les résolvantes sont unitaires à coefficients entiers).

Les autres améliorations consistent en l'association des méthodes du Paragraphe 6.4.2 (factorisation complète des résolvantes, avec utilisation des corollaires 6.11 et 6.12) aux techniques numériques : les résolvantes utilisées sont calculées en utilisant des approximations des racines au lieu d'être calculées à l'aide des seuls coefficients de f.

Comparaison avec les autres méthodes Les méthodes numériques présentent l'avantage de pouvoir fournir rapidement un résultat non garanti. En effet, même quand on ne respecte pas la précision sur les racines qui serait nécessaire, on a de très bonnes chances de trouver le bon groupe de Galois (mais il y a des contrexemples). Un autre avantage est qu'elles ne nécessitent pas de stocker la formule générique des résolvantes.

Elles ont par contre pour inconvénient d'être très coûteuses lorsqu'on leur demande un résultat certifié (c'est-à-dire quand on respecte la précision indiquée par le calcul d'erreur de [21, Par. 2.1.3]). On peut cependant commencer par «élaguer» le graphe avec une mauvaise précision, pour pouvoir ensuite optimiser la recherche du groupe de Galois avec une bonne précision en prenant tout de suite le chemin le plus direct dans le graphe.

Un autre inconvénient est qu'elles ne permettent pas de travailler à conjugaison près dans $\mathfrak{S}_n$: pour calculer une résolvante relative $\mathcal{L}^L_{\Psi,\mathbf{x}}$, on est obligé de savoir à l'avance que Γ (représentation de $\mathrm{Gal}_k(f)$) est précisément inclus dans L, et non dans un de ses conjugués ; et c'est coûteux : en effet, pour savoir qu'un conjugué de L contient Γ, il suffit de vérifier qu'une résolvante d'un invariant de L admet une racine simple dans k, ce qu'un algorithme de factorisation donne facilement. Mais pour identifier précisément quel conjugué de L contient Γ, il faut tester, à partir des valeurs approchées de $x_1, \ldots, x_n$, quelle racine de cette résolvante appartient à k. La méthode formelle du chapitre 8 permettra de s'affranchir de ces deux inconvénients des méthodes numériques.

6.4.2 Factorisation complète des résolvantes

Les méthodes par factorisation complète des résolvantes furent utilisées par Berwick [10, 11] pour une résolution complète du cas transitif en degré 6, avec les corollaires 6.11 et 6.12. Ces travaux furent poursuivis par Foulkes (1931) en degré 7, puis plus récemment par McKay et Soicher [52, 59], qui utilisent uniquement des résolvantes associées à des invariants linéaires (*i.e.* polynomiaux de degré un).

En 1993, Arnaudiès et Valibouze montrent que le Corollaire 6.12 permet dans tous les cas d'identifier la classe de conjugaison $[\Gamma]$ du groupe de Galois, et ils donnent la définition 6.8 des familles $\varpi^L(G,H)$, qui permet de les calculer *a priori* par des algorithmes portant uniquement sur les groupes, alors qu'elles étaient auparavant calculées de façon heuristique.

En 1995, Valibouze donne une optimisation, jusqu'au degré 10, de cette méthode en utilisant le Corollaire 6.11, c'est-à-dire en testant non seulement les degrés des facteurs irréductibles (sur k) des résolvantes, mais encore les groupes de Galois de ceux de ces facteurs dont le degré est inférieur à celui de f (on peut aussi tester la parité du groupe, qui s'obtient par un simple calcul de discriminant, quand le degré de ce facteur est plus élevé). L'utilisation du Corollaire 6.11 lui permet ainsi d'améliorer un algorithme qui était pourtant déjà déterministe sans cela. Cette optimisation par le calcul du groupe de Galois des facteurs irréductibles a été indépendamment développée, dans le cadre des méthodes numériques, par Eichenlaub (voir [21]).

Sur le calcul même des résolvantes, signalons les travaux de Lehobey, Rennert et Valibouze [49, 57], qui permettent de calculer les résolvantes à l'aide de résultants et en éliminant les facteurs et puissances parasites que ceux-ci introduisent ordinairement: leur idée est fondée sur l'utilisation des polynômes d'Ampère (modules de Cauchy).

Enfin, Arnaudiès et Valibouze ont montré dans [7] que tout ce qu'ils faisaient avec des résolvantes absolues se transposait avec des résolvantes relatives. Arnaudiès a appliqué cela au degré 4 dans [6, page 437]. Il préconise aussi avec Valibouze dans [7] d'utiliser la démonstration du Théorème 3.4 de Lagrange pour spécialiser les résolvantes relatives, mais cela ne donne pas encore un algorithme efficace pour traiter les degrés plus élevés que 4. Aussi, les résolvantes relatives sont-elles restées l'apanage des numériciens.

6.4.3 Présentation des méthodes des chapitres 8 et 9

Les chapitres 8 et 9 présentent deux méthodes, dont la seconde est une généralisation de la première, qui permettent d'introduire efficacement des résolvantes relatives dans le cadre des méthodes formelles par factorisation de résolvantes absolues qui utilisent le Corollaire 6.11. Le chapitre 8 reprend l'article [17], avec quelques modifications tandis que le chapitre 9 reprend [18].

Soit Ψ un H-invariant primitif L-relatif, où $H \subset L \subset \mathfrak{S}_n$ et où $\Gamma \subset L$. On cherche à calculer $\mathcal{L}^L_{\Psi,\mathbf{x}}$, qui appartient bien à $k[T]$ d'après l'hypothèse $\Gamma \subset L$. Il s'agit pour cela de spécialiser les coefficients de $\mathcal{L}^L_\Psi$, qui appartiennent à $k[\mathbf{X}]^L$.

On voit immédiatement le problème qui se pose : la seule donnée que l'on ait est les coefficients c_i de f. Cela permet certes de spécialiser les polynômes symétriques élémentaires : $\widetilde{E_i} = (-1)^i c_i$, et donc tous les polynômes symétriques, mais certainement pas tous les invariants de L. L'idée commune aux chapitres 8 et 9 consiste à connaître la valeur spécialisée d'un petit nombre d'invariants de L par la factorisation d'autres résolvantes : d'un invariant primitif de L au chapitre 8 et d'un invariant d'un autre groupe qui n'a qu'un rapport plus lointain avec L au chapitre 9.

La descente directe

L'idée du chapitre 8 consiste à spécialiser un invariant primitif Θ du groupe L par le calcul d'une résolvante spécialisée de Θ et par sa factorisation, et à l'utiliser pour spécialiser tous les invariants de L. En effet, une racine θ d'une résolvante $\mathcal{L}^M_{\Theta,\mathbf{x}}$ de Θ sera alors la valeur spécialisée $\theta = \widetilde{\tau.\Theta}$ d'un conjugué $\tau.\Theta$ de Θ.

Bien sûr, on ne connaît pas τ. Mais nous montrons que ce n'est pas un problème : en effet, on sait (d'après la Proposition 6.14) que $\tau.L\tau^{-1}$ contient Γ si θ appartient à k et est racine simple de la résolvante — cas auquel on peut toujours se ramener, voir la Prop. 8.5. Comme on travaille à conjugaison près, peu importe le τ inconnu : on est en tout cas sûr que c'est le même τ pour lequel $\tau.L.\tau^{-1} \supset \Gamma$ et $\theta = \tau.\Theta$ (et on prouve ainsi, par la factorisation sur k de la résolvante spécialisée de Θ, que Γ est inclus dans un conjugué de L, en même temps qu'on détermine la valeur spécialisée de $\tau.\Theta$).

On peut donc, grâce à θ, spécialiser les éléments, sinon de L du moins de $\tau.L.\tau^{-1}$ pour un certain τ inconnu en utilisant le chapitre 3 et l'algorithme 3.10, en écrivant $k(\mathbf{X})^{\tau.L.\tau^{-1}} = k(\mathbf{X})^{\mathfrak{S}_n}[\tau.\Theta]$ au cas où Θ est un invariant absolu de L. On peut d'ailleurs itérer le processus : Si Θ n'est qu'un invariant relatif à un groupe $M \supset L$, on peut chercher tout d'abord à spécialiser les invariants de $\tau.M.\tau - 1$ puis grâce à Θ et à l'algorithme de la Prop. 3.10, en déduire la spécialisation des invariants de $\tau.L.\tau^{-1}$ (car $k(\mathbf{X})^{\tau.L.\tau-1} = k(\mathbf{X})^{\tau.M.\tau^{-1}}[\tau.\Theta]$).

Le problème de l'annulation des dénominateurs par spécialisation peut toujours être évité grâce à la Prop. 8.4.

La méthode de «descente directe» consiste alors à parcourir le graphe des classes de conjugaison de sous-groupes de $\mathfrak{S}_n$, à partir de sa racine $[\mathfrak{S}_n]$, en descendant par inclusions successives à conjugaison près dans des sous-groupes maximaux, comme dans la méthode de Stauduhar (cf. § 6.4.1). Comme nous l'avons montré plus haut, les tests d'inclusion ($\Gamma \subset \tau.L.\tau^{-1}$) et les calculs de résolvantes relatives (en calculant la valeur spécialisée $\theta = \widetilde{\tau.\Theta}$) sont alors imbriqués l'un dans l'autre.

Le nom «descente directe» vient de ce que l'on n'effectue que des tests d'inclusion par l'existence de facteurs linéaires de la résolvante (Prop.6.14). On peut aussi l'appeler «Méthode de Stauduhar formelle».

$\star$

L'article [17], que reprend le chapitre 8, a été écrit avant que nous prouvions le Théorème 4.14. C'est pourquoi nous n'y utilisons que le point de vue du chapitre 3 et non le point de vue dual du chapitre 4. Mais le Théorème 4.14 montre qu'on peut très bien utiliser une décomposition d'Hironaka (voir le

chap. 4) au lieu d'éléments primitifs pour spécialiser les invariants de L, sous l'hypothèse que k soit de caractéristique nulle bien sûr, comme chaque fois que l'on utilise le point de vue polynomial au lieu du point de vue fractionnaire.

Voici comment cela fonctionnerait (voir aussi un exemple illustratif à l'Annexe A). On cherche toujours à calculer une résolvante spécialisée d'un H-invariant Ψ relatif à un groupe L. Le problème est donc de savoir spécialiser les éléments de $k[\mathbf{X}]^L$.

Pour cela, on utilise une décomposition de Cohen-Macaulay de $k[\mathbf{X}]^L$, du type

$$k[\mathbf{X}]^L = \bigoplus_{i=1}^{e} k[\mathbf{\Pi}]\Sigma_i \qquad \text{avec} \qquad k[\mathbf{\Pi}] = k[\mathbf{X}]^M$$

où M est un groupe de réflexions (donc un produit de groupes symétriques, voir le Cor. 4.3) qui contient L. Si on sait spécialiser $\Pi_1, \ldots, \Pi_n$ et $\Sigma_1, \ldots, \Sigma_e$, alors on saura spécialiser tous les invariants de L.

Ici, spécialiser les éléments de M ne pose pas de problème : en effet, si f est irréductible on a forcément $M = \mathfrak{S}_n$ et il s'agit alors de spécialiser les polynômes symétriques élémentaires grâce aux coefficients de f, et si f n'est pas irréductible, ce sont les coefficients des facteurs irréductibles de f qu'on utilise.

Pour les invariants secondaires Σ_i, on peut aussi, comme Θ plus haut, les spécialiser en calculant une résolvante $\mathcal{L}^M_{\Sigma_i,\mathbf{x}}$ de chaque Σ_i et en la factorisant sur k. Si σ_i est une racine de $\mathcal{L}^M_{\Sigma_i,\mathbf{x}}$ dans k, alors il existe $\tau_i \in M$ tel que $\Gamma \subset \tau_i.L.\tau_i^{-1}$ et $\sigma_i = \widetilde{\tau_i.\Sigma_i}$. Mais contrairement à la méthode utilisant un élément primitif Θ, où l'on pouvait travailler à conjugaison près, ici, s'il l'on peut certes toujours travailler à conjugaison près il faut cependant que l'on ait $\sigma_i = \widetilde{\tau.\Sigma_i}$ avec le même élément τ pour tout i. Le problème se pose quand certaines des résolvantes $\mathcal{L}^M_{\Sigma_i,\mathbf{x}}$ ont plusieurs racines dans k : quelle racine choisir alors?

Le Théorème 4.14 nous donne un algorithme pour choisir la «bonne» racine des résolvantes : il suffit pour cela de vérifier que $(\sigma_1, \ldots, \sigma_e)$ satisfait les syzygies entre $\Sigma_1, \ldots, \Sigma_e$ sur l'anneau $k[\mathbf{X}]^M$, dont on a spécialisé les coefficients. Et on peut se limiter à des générateurs de l'idéal des syzygies : par exemple la base standard qui est donnée au Lemme 4.13. On peut en général se limiter encore plus, car le nombre de racines dans k des résolvantes est souvent réduit ; une seule syzygie peut alors suffire à identifier les bonnes racines, ou même zéro quand les résolvantes n'ont qu'une racine dans k : c'est le cas dans l'exemple donné à l'Annexe A.

La descente diagonale

L'article [18], dont est tiré le chapitre 9, généralise la «descente directe» en utilisant tous les facteurs des résolvantes pour spécialiser les invariants, alors que la «descente directe» ne tire parti pour la spécialisation que des facteurs linéaires (c'est-à-dire des racines appartenant à k) de ces résolvantes — mais elle utilise aussi la factorisation complète pour identifier le groupe de Galois.

D'autre part, l'outil de théorie des invariants utilisé est indifféremment le chapitre 3 ou 4 : les deux descriptions duales des invariants conviennent l'une comme l'autre.

L'idée du chapitre 9 consiste à calculer un invariant d'un groupe L, et à le spécialiser, à partir des invariants d'un autre groupe. Par exemple, si Θ est un H-invariant primitif L-relatif et si la résolvante $\mathcal{L}^L_{\Theta,\mathbf{x}}$ admet un facteur $h \in k[T]$ tel que les racines de h sont les spécialisés $\widetilde{\tau_i.\Theta} = (\tau_i.\Theta)(\mathbf{x})$ de conjugués $\tau_i.\Theta$ de Θ, $1 \leq i \leq r$, alors $\tau_1.\Theta + \ldots + \tau_r.\Theta$ est un invariant d'un autre groupe G, et sa valeur spécialisée n'est autre que $(\tau_1.\Theta)(\mathbf{x}) + \ldots + (\tau_r.\Theta)(\mathbf{x})$, c'est-à-dire le coefficient sous-dominant de h.

Ainsi, le calcul d'une résolvante d'un invariant de H permet de spécialiser des invariants de G. C'est cette idée que nous exploitons et qui est à la base de l'algorithme du chapitre 9 (voir le Théorème 9.7).

6.4.4 Autres méthodes

Rappelons pour commencer le théorème de densité de Tchebotarev :

Théorème 6.16 *Soit $f \in \mathbb{Z}[T]$ de degré n et $\pi = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$ tel que $\alpha_1 + \ldots + \alpha_r = n$. Alors quand p, nombre premier, tend vers l'infini, les degrés des facteurs irréductibles de f modulo p (c'est-à-dire qu'on factorise l'image de f dans $\mathbb{F}_p[T]$) sont les éléments de π dans une proportion qui tend vers la proportion des permutations de $\mathrm{Gal}_{\mathbb{Q}}(f)$ dont les tailles des cycles sont données par π.*

Preuve – Voir [43]. □

Ce résultat n'est pas en général suffisant pour identifier le groupe de Galois, mais il peut donner une indication. Dedekind, Van der Waerden et Brauer montrent aussi que le groupe de Galois de f modulo p, quand ce polynôme est séparable, est un sous-groupe du groupe de Galois de f et lui est isomorphe quand f est galoisien. On trouvera une démonstration de ce résultat dans [7, Théorème 7.2] ou dans [13, AC V.38, Théorème 2]. Dans cet article, les auteurs donnent un résultat nouveau qui l'étend considérablement :

Théorème 6.17 *Soit A un anneau intégralement clos, k son corps des fractions, $\mathfrak{P}$ un idéal premier de A, ϕ la surjection canonique de A sur $A^\bullet = A/\mathfrak{P}$ et $\bar{\phi}$ de $A[T]$ sur $(A/\mathfrak{P})[T]$. Soit $f \in A[T]$. Si $\bar{\phi}(f)$ est séparable, alors son groupe de Galois sur le corps des fractions $k^\bullet$ de $A/\mathfrak{P}$ s'identifie à un sous-groupe de $\mathrm{Gal}_k(f)$, et f est alors aussi séparable.*

Soit $(H_1, \ldots, H_r)$ une famille de sous-groupes de $\mathfrak{S}_n$ telle que les vecteurs $(\varpi(G, H_i))_{1 \leq i \leq r}$ soient deux à deux distincts quand G parcourt l'ensemble des classes de conjugaisons de sous-groupes de $\mathfrak{S}_n$, et Θ_i un invariant primitif de H_i, pour tout i (c'est-à-dire que l'on choisit une famille d'invariants qui permette d'identifier le groupe de Galois de n'importe quel polynôme à l'aide du Corollaire 6.12 appliqué avec $L = \mathfrak{S}_n$). Supposons que, pour tout $i \in \{1, \ldots, r\}$, $\bar{\phi}(f)$ soit séparable ainsi que $\bar{\phi}(\mathcal{L}_{\Theta_i, f})$, et que pour tout facteur P de $\mathcal{L}_{\Theta_i, f}$ normalisé et irréductible dans $k[T]$, le polynôme $\bar{\phi}(P)$ soit irréductible dans $k^\bullet[T]$. Alors les groupes de Galois de f sur k et de $\bar{\phi}(f)$ sur $k^\bullet$ sont isomorphes, et ont la même représentation dans $\mathfrak{S}_n$ pour une numérotation donnée des racines de f.

Preuve – Voir [7, Théorème 7.3]. □

⋆

Signalons aussi la méthode de Yokoyama (voir [73]) qui consiste à remplacer un calcul numérique approchés des racines par des calculs p-adiques. Cela lui permet ainsi de déterminer le groupe de Galois d'un polynôme sans calculer de résolvantes, de même que les méthodes numériques, qui peuvent tester si une racine de la résolvante appartient au corps de base sans calculer cette résolvante.

Chapitre 7

Idéal des relations

Dans ce chapitre, k est un corps commutatif (de caractéristique quelconque).

7.1 Idéal des relations et groupe de Galois

Dans tout ce paragraphe, nous définissons l'idéal des relations entre les racines d'un polynôme et nous présentons des résultats bien connus concernant les liens entre cet idéal et le groupe de Galois du polynôme.

Définition 7.1 *Soit $f = \prod_{i=1}^{n}(T - x_i) \in k[T]$ un polynôme séparable de degré n à coefficients dans un corps k (les racines x_i appartenant à une clôture algébrique $\hat{k}$ de k). On appelle idéal des relations entre les racines de f et on note $I(f)$ l'idéal de $k[X_1, ..., X_n]$ défini de la façon suivante :*

$$I(f) = \{r \in k[X_1, ..., X_n] / \ r(x_1, ..., x_n) = 0\}.$$

L'idéal $I(f)$ dépend donc de la numérotation $\mathbf{x} = \{x_1, \ldots, x_n\}$ choisie sur les racines de f.
Le résultat suivant est alors bien connu :

Proposition 7.2 *Soit $f \in k[T]$ séparable de degré n. Définissons le groupe*

$$G = \{\sigma \in \mathfrak{S}_n / \ \forall \ r \in I(f), r(X_{\sigma(1)}, ..., X_{\sigma(n)}) \in I(f)\},$$

c'est à dire $G = Stab_{\mathfrak{S}_n}(I(f))$ pour l'action de $\mathfrak{S}_n$ sur $k[X_1, ..., X_n]$ définie par $\sigma.r(X_1, ..., X_n) = r(X_{\sigma(1)}, ..., X_{\sigma(n)})$.

Alors G est isomorphe à $\mathrm{Gal}_k(f)$, où l'isomorphisme est induit par l'action de $\mathrm{Gal}_k(f)$ sur les racines de f.

Preuve – Soit

$$\Phi : \left| \begin{array}{lll} \mathrm{Gal}_k(f) & \longrightarrow & \mathfrak{S}_n \\ g & \longmapsto & \Phi(g) = \sigma \\ & & \text{où } \sigma \text{ est défini par } \forall\ i \in \mathbb{N}_n^*, g(x_i) = x_{\sigma(i)}. \end{array} \right.$$

Alors Φ est un morphisme injectif de groupes car $\mathrm{Gal}_k(f)$ opère fidèlement sur $\{x_1, ..., x_n\}$. Reste donc à montrer que $\mathrm{Im}\ \Phi = G$.

- Déjà, $\mathrm{Im}\ \Phi \subset G$; en effet, $\forall\ g \in \mathrm{Gal}_k(f), \forall\ r \in I(f)$,

$$\begin{aligned} \Phi(g).r(x_1..., x_n) &= r(g(x_1), ..., g(x_n)) \\ &= g(r(x_1, ..., x_n)) \end{aligned}$$

car g appartient à $\mathrm{Gal}_k(f)$ donc est un endomorphisme de k-algèbre de $k[x_1, ..., x_n]$;
d'où : $\Phi(g).r(x_1..., x_n) = g(0) = 0$.

- En outre, $G \subset \mathrm{Im}\ \Phi$; en effet, soit $\sigma \in G$; alors $\forall\ r \in I(f), \sigma.r \in I(f)$. On va construire un antécédent g de σ par Φ à. Montrons que l'on peut définir un morphisme de k-algèbre g de $k(x_1, ..., x_n)$ dans lui-même par : $\forall\ i \in \mathbb{N}_n^*, g(x_i) = x_{\sigma(i)}$. En effet, si $x \in k(x_1, ..., x_n)$, on peut écrire $x = P(x_1, ..., x_n)/Q(x_1, ..., x_n)$ avec $(P, Q) \in (k[X_1, ..., X_n])^2$. On définit alors

$$g(x) = P(x_{\sigma(1)}, ..., x_{\sigma(n)})/\ Q(x_{\sigma(1)}, ..., x_{\sigma(n)})\ ;$$

c'est indépendant du choix de la fraction rationnelle P/Q, vu que si $x = P_1(x_1, ..., x_n)/Q_1(x_1, ..., x_n)$ avec $(P_1, Q_1) \in (k[\mathbf{X}])^2$ alors on a $(P/Q - P_1/Q_1)(x_1, ..., x_n) = 0$ donc $(PQ_1 - P_1Q)(x_1, ..., x_n) = 0$ donc $PQ_1 - P_1Q \in I(f)$ donc, comme $\sigma \in G$, $\sigma.(PQ_1 - P_1Q) = 0$ d'où $(P/Q)(x_{\sigma(1)}, ..., x_{\sigma(n)}) = (P_1/Q_1)(x_{\sigma(1)}, ..., x_{\sigma(n)})$.

Alors g est par définition un endomorphisme de k-algèbre de $k(x_1, ..., x_n)$, donc un endomorphisme de corps de $k(x_1, ..., x_n)$ qui fixe les points de k. Il est clair que g est injectif (si $g(P(x_1, ..., x_n)) = 0$ alors $\sigma.P \in I(f)$ donc $P \in I(f)$ et $P(x_1, ..., x_n) = 0$). Or, $k(x_1, ..., x_n)$ est de dimension finie comme espace vectoriel sur k donc g est aussi surjectif, d'où $g \in \mathrm{Gal}_k(f)$. Or, $\Phi(g) = \sigma$ d'après la définition de g, d'où le résultat. □

Corollaire 7.3 *L'idéal $J(f) = k(\mathbf{x}) \otimes_k I(f)$, où $k(\mathbf{x}) = k(x_1, \ldots, x_n)$, définit dans le k-espace affine $(k(\mathbf{x}))^n$ un ensemble algébrique affine de dimension 0 et de cardinal $|\mathrm{Gal}_k(f)|$. Plus précisément, cet ensemble s'écrit :*

$$V(J(f)) = \{(x_{\sigma(1)}, ..., x_{\sigma(n)})/\ \sigma \in G\}.$$

Preuve – Déjà, il est clair que $\forall\ \sigma \in G, (x_{\sigma(1)}, ..., x_{\sigma(n)}) \in V(J(f))$ par définition de G.

Réciproquement, soit $(y_1, ..., y_n) \in V(J(f))$. On a : $\forall\ r \in J(f), r(y_1, ..., y_n) = 0$. En particulier, comme $\forall\ i \in \mathbb{N}_n^*, E_i - a_i \in J(f)$, où

$$f(T) = T^n + \sum_{i=1}^{n} (-1)^i a_i T^{n-i}, \qquad \text{et} \qquad E_i = \sum_{1 \leq \alpha_1 < ... < \alpha_i \leq n} \prod_{k=1}^{i} X_{\alpha_k},$$

on a : $\forall\ i \in \mathbb{N}_n^*, E_i(y_1, ..., y_n) = a_i$; donc $\prod_{k=1}^{n}(T - y_i) = X^n + \sum_{i=1}^{n}(-1)^i a_i T^{n-i} = f(T) = \prod_{k=1}^{n}(T - x_i)$ donc $\exists\ \sigma \in \mathfrak{S}_n/\ \forall\ i \in \mathbb{N}_n^*, y_i = x_{\sigma(i)}$; et comme $\forall\ r \in J(f), r(x_{\sigma(1)}, ..., x_{\sigma(n)}) = 0$, σ appartient bien à G. □

7.2 Idéal d'un produit de polynômes

Dans ce paragraphe, nous nous proposons d'exprimer l'idéal des relations d'un produit $f.g$ de polynômes en fonction de $I(f)$ et $I(g)$ lorsque c'est possible, et d'étudier les conditions de validité de la relation trouvée.

On se donne donc deux polynômes unitaires $(f, g) \in k[T]^2$ (où T est une indéterminée sur k) qui s'écrivent $f = \prod_{i=1}^{p}(T - x_i)$ et $g = \prod_{j=1}^{q}(T - y_j)$ dans une extension $\hat{k}$ de k. On note $k[\mathbf{X}] = k[X_1, ..., X_p]$ et $k[\mathbf{Y}] = k[Y_1, ..., Y_q]$, et on définit de même $k[\mathbf{x}] = k[x_1, ..., x_p] \subset \hat{k}$ et $k[\mathbf{y}] = k[y_1, \ldots, y_q] \subset \hat{k}$. On note $I(f) \subset k[\mathbf{X}], I(g) \subset k[\mathbf{Y}], I(f.g) \subset k[\mathbf{X}, \mathbf{Y}]$ les idéaux respectifs de $f, g, f.g$. Remarquons que $k(\mathbf{x}) = k[\mathbf{x}]$ car les x_i sont algébriques sur k. Avec ces notations, rappelons le lemme suivant (voir [13, A V.13]) :

Lemme 7.4 – $[k(\mathbf{x}, \mathbf{y}) : k(\mathbf{x})] \leqslant [k(\mathbf{y}) : k]$

– $[k(\mathbf{x},\mathbf{y}) : k] \leqslant [k(\mathbf{x}) : k][k(\mathbf{y}) : k]$

– *Les propriétés suivantes sont équivalentes :*

i. $k[\mathbf{x},\mathbf{y}] \simeq k[\mathbf{x}] \otimes_k k[\mathbf{y}]$

ii. $[k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})] = [k(\mathbf{y}) : k]$

iii. $[k(\mathbf{x},\mathbf{y}) : k] = [k(\mathbf{x}) : k][k(\mathbf{y}) : k]$

iv. $|\mathrm{Gal}_k(f.g)| = |\mathrm{Gal}_k(f)|.|\mathrm{Gal}_k(g)|$.

Lorsqu'elles sont vérifiées, on dit que les sous-extensions $k(\mathbf{x})$ et $k(\mathbf{y})$ de $\hat{k}$ linéairement disjointes sur k. Cela implique en particulier que $k(\mathbf{x}) \cap k(\mathbf{y}) = k$.

Preuve –

$$\tilde{\varphi} : \left| \begin{array}{ccc} k[\mathbf{x}] \times k[\mathbf{y}] & \longrightarrow & k[\mathbf{x},\mathbf{y}] \\ (P,Q) & \longmapsto & P.Q \end{array} \right.$$

est une application bilinéaire de k-algèbres. Donc il existe une unique application linéaire $\varphi : k[\mathbf{x}] \otimes_k k[\mathbf{y}] \longrightarrow k[\mathbf{x},\mathbf{y}]$ qui factorise $\tilde{\varphi}$. En outre, φ est toujours surjective car tout $R \in k[\mathbf{x},\mathbf{y}]$ s'écrit sous la forme $R = \sum_{\mathbf{i}\in\mathbb{N}_q^*} R_{\mathbf{i}}(\mathbf{x})\mathbf{y}^{\mathbf{i}}$ donc $R = \varphi(\sum_{\mathbf{i}} R_{\mathbf{i}}(\mathbf{x}) \otimes_k \mathbf{y}^{\mathbf{i}})$.

Soit $(b_j)_{1\leqslant j\leqslant n}$ une base du k-espace vectoriel de dimension finie $k[\mathbf{y}]$. Alors $(b_j)_{1\leqslant j\leqslant n}$ est une famille génératrice du $k(\mathbf{x})$-espace vectoriel $k[\mathbf{x},\mathbf{y}]$, d'où les deux premiers points de la proposition.

Enfin, $[k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})] = [k(\mathbf{y}) : k]$ veut donc dire exactement que $(b_j)_{1\leqslant j\leqslant n}$ est une famille libre de $k[\mathbf{x},\mathbf{y}]$ sur $k(\mathbf{x})$, ce qui équivaut bien sûr à l'injectivité de φ (en effet tout élément de $k[\mathbf{x}] \otimes_k k[\mathbf{y}]$ se met sous la forme $\sum_{i,j} \alpha_i \otimes_k b_j$ avec des $\alpha_i \in k(\mathbf{x})$, donc $\varphi(\sum_{i,j} \alpha_i \otimes_k b_j) = \sum_{i,j} \alpha_i b_j$ est nul si et seulement si tous les α_i sont nuls, à la condition (nécessaire et suffisante) que $(b_j)_{1\leqslant j\leqslant n}$ soit libre sur $k(\mathbf{x})$) ; d'où l'équivalence de (i) et (ii). L'équivalence avec (iii) résulte simplement de la relation $[k(\mathbf{x},\mathbf{y}) : k] = [k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})][k(\mathbf{x}) : k]$, et l'équivalence avec (iv) de ce que les extensions sont galoisiennes. □

Nous prouvons la proposition suivante, qui établit un lien entre l'existence de relations algébriques entre les racines de f et celles de g et le fait que l'ordre du groupe $\mathrm{Gal}_k(f.g)$ soit égal au produit des ordres de $\mathrm{Gal}_k(f)$ et $\mathrm{Gal}_k(g)$.

Proposition 7.5 *Les affirmations suivantes sont équivalentes :*

i. *$k(\mathbf{x})$ et $k(\mathbf{y})$ sont linéairement disjointes sur k (ce qui veut dire que $|\mathrm{Gal}_k(f.g)| = |\mathrm{Gal}_k(f)|.|\mathrm{Gal}_k(g)|$ d'après le lemme précédent).*

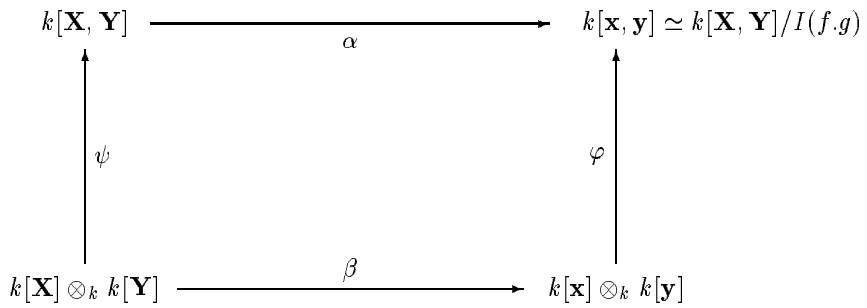
ii. *$I(f.g) = \psi(k[\mathbf{X}] \otimes_k I(g) + I(f) \otimes_k k[\mathbf{Y}])$, où ψ désigne l'isomorphisme canonique entre $k[\mathbf{X}] \otimes_k k[\mathbf{Y}]$ et $k[\mathbf{X},\mathbf{Y}]$.*

(ii) s'écrit encore :

$$I(f.g) = \bigoplus_{i\in\mathbb{N}} X^i I(g) \; + \; \bigoplus_{i\in\mathbb{N}} Y^i I(f) \qquad \text{(somme directe de } k\text{-espaces vectoriels).}$$

Autrement dit, cela signifie que les relations entre les racines de $f.g$ s'expriment toutes en fonction de relations entre les racines de f d'une part, et celles de g d'autre part.

Preuve – On a le diagramme commutatif suivant:



où α et β sont les surjections canoniques, et où φ a été définie dans la démonstration du lemme précédent.

Commençons par montrer que (i) $\Longrightarrow$ (ii).

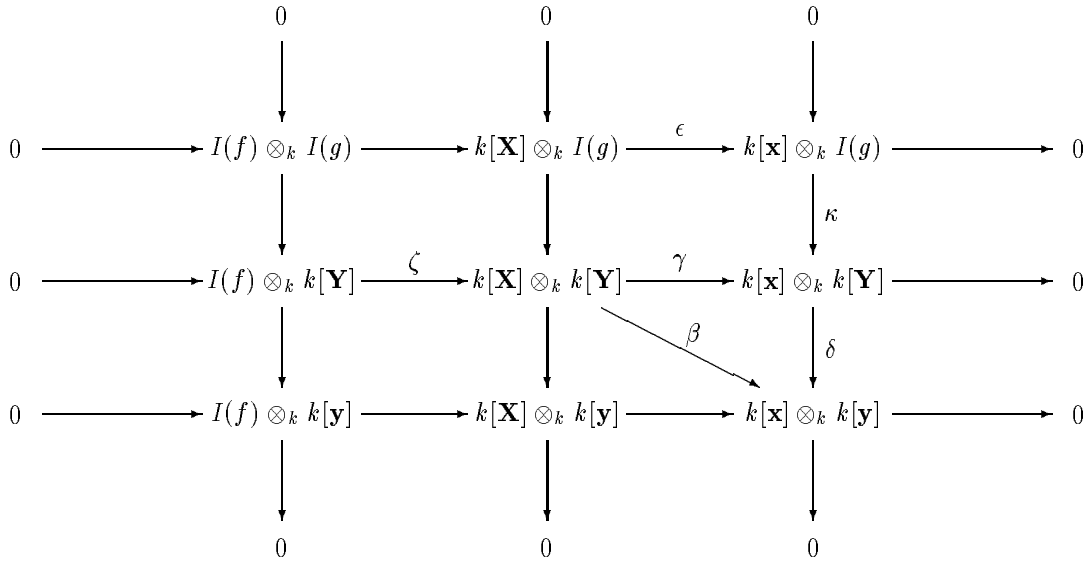
On suppose donc (i) vérifiée. Alors φ est un isomorphisme d'après le lemme précédent, et ψ aussi d'après ce même lemme appliqué avec $I(f) = 0$ et $I(g) = 0$.

L'idéal $I(f.g) = \ker\alpha$ est donc égal à $\psi(\ker\beta)$. On est donc conduit à calculer $\ker\beta$. Il est déjà clair qu'il contient $k[\mathbf{X}] \otimes_k I(g) + I(f) \otimes_k k[\mathbf{Y}]$.

Étudions l'inclusion inverse. On a la suite exacte

$$0 \longrightarrow I(f) \longrightarrow k[\mathbf{X}] \longrightarrow k[\mathbf{x}] \longrightarrow 0$$

donc en tensorisant par des k-espaces vectoriels on obtient encore des suites exactes ; d'où le diagramme commutatif suivant, dont les lignes et les colonnes sont exactes :



On part alors à la chasse dans le diagramme.

Un élément u de $\ker\beta$ a pour image $\bar{u} \in \ker\delta = \mathrm{Im}\,\kappa$ par γ, donc $\bar{u}$ peut être tiré en arrière par κ puis par ϵ en un v. Alors $\gamma(u - v) = \gamma(u) - \epsilon(v) = 0$ donc $u - v$ peut être tiré en arrière en un w par ζ. On en déduit que $u = v + w$ avec $v \in k[\mathbf{X}] \otimes_k I(g)$ et $w \in k[\mathbf{Y}] \otimes_k I(f)$.

En fin de compte, on a bien montré que

$$\ker \beta = k[\mathbf{X}] \otimes_k I(g) + I(f) \otimes_k k[\mathbf{Y}] \otimes_k I(f)$$

et donc :

$$I(f.g) = \psi(k[\mathbf{X}] \otimes_k I(g) + I(f) \otimes_k k[\mathbf{Y}]).$$

Montrons maintenant que (ii) $\Longrightarrow$ (i).

Supposons donc (ii) vérifiée. Comme φ est déjà surjective, il nous suffit de montrer qu'elle est injective. Soit donc $u \in \ker \varphi$. L'application β étant surjective, u admet un antécédent v par β. Alors d'après la commutativité du diagramme, $\alpha(\psi(v)) = 0$ donc $\psi(v)$ appartient à $\ker \alpha$, c'est à dire à $I(f.g)$; or, on vient de voir que $I(f.g) = \psi(k[\mathbf{X}] \otimes_k I(g) + I(f) \otimes_k k[\mathbf{Y}] \otimes_k I(f))$ par hypothèse, qui est égal à $\psi(\ker \beta)$ d'après la démonstration faite dans la partie ((i) $\Longrightarrow$ (ii)). Donc v appartient à $\ker \beta$ car ψ est injective, et donc $u = \beta(v) = 0$. □

La proposition suivante est bien connue :

Proposition 7.6 *Les deux propriétés suivantes sont équivalentes :*

i. $k(\mathbf{x}) \cap k(\mathbf{y}) = k$ *(notons que cette propriété est impliquée par les propriétés (i) et (ii) de la proposition précédente).*

ii. $\mathrm{Gal}_k(f.g) = \mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k)$ *est produit interne de ses sous-groupes distingués* $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x}))$ *et* $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$ *; ou, en d'autres termes, il est isomorphe au groupe produit* $\mathrm{Gal}_k(f) \times \mathrm{Gal}_k(g)$.

Preuve – (démonstration d'après [13])

$\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k)$ produit direct de $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x}))$ et de $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$ veut dire deux choses :
- premièrement que $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})) \cap \mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y})) = \{1\}$
- deuxièmement que $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k) = \mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})).\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$.

Le premier point est toujours vérifié par définition du groupe de Galois (et parce que $k(k(\mathbf{x}) \cup k(\mathbf{y})) = k(\mathbf{x},\mathbf{y})$).

$\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x})).\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$ est le plus petit sous-groupe de $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k)$ qui contienne à la fois $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x}))$ et $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$. D'après le théorème de dualité de Galois, le sous-corps des points qu'il laisse invariant est donc le plus grand corps qui soit inclus à la fois dans $k(\mathbf{x})$ et $k(\mathbf{y})$, c'est à dire $k(\mathbf{x}) \cap k(\mathbf{y})$. Donc le second point équivaut à ce que $k(\mathbf{x}) \cap k(\mathbf{y})$ soit égal à $k(\mathbf{x},\mathbf{y})^{\mathrm{Gal}_k(f)}$, c'est à dire à k. □

Les propositions 7.5 et 7.6 prises ensemble montrent le corollaire suivant :

Corollaire 7.7 *Soit $k(\mathbf{x})$ et $k(\mathbf{y})$ les corps de décomposition respectifs dans une extension algébriquement close $\hat{k}$ de k de deux polynômes $f, g \in k[T]$. Alors les propositions suivantes sont équivalentes :*

i. $\mathrm{Gal}_k(f.g) \simeq \mathrm{Gal}_k(f) \times \mathrm{Gal}_k(g)$

ii. $|\mathrm{Gal}_k(f.g)| = |\mathrm{Gal}_k(f)|.|\mathrm{Gal}_k(g)|$

iii. $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k)$ *est produit direct de ses sous-groupes distingués* $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{x}))$ *et* $\mathrm{Gal}(k(\mathbf{x},\mathbf{y}) : k(\mathbf{y}))$

iv. $k(\mathbf{x})$ *et* $k(\mathbf{y})$ *sont linéairement disjointes sur* k

v. $k(\mathbf{x}) \cap k(\mathbf{y}) = k$

vi. $I(f.g) = \bigoplus_{i \in \mathbb{N}} X^i I(g) \ + \ \bigoplus_{i \in \mathbb{N}} Y^i I(f)$

7.3 Compléments

L'idéal $I(f)$ est bien sûr un idéal maximal de $k[\mathbf{X}]$ car $k[\mathbf{X}]/I(f)$ est un corps, puisqu'il est isomorphe à $k[\mathbf{x}] = k(\mathbf{x})$. Nous avons vu précédemment que l'idéal $I(f)$ contient les n polynômes symétriques $E_i - a_i$, où les E_i sont les polynômes symétriques élémentaires et où $f(T) = T^n + \sum_{i=1}^{n}(-1)^i a_i T^{n-i}$. Bien sûr, en général, il ne contient pas que des relations symétriques, mais le théorème suivant, énoncé et démontré dans [7], montre qu'il suffit d'ajouter un polynôme aux n polynômes symétriques $E_i - a_i$ pour engendrer $I(f)$.

Théorème 7.8 *Soit $\Theta \in k[X_1, ..., X_n]$ un invariant primitif de H, sous-groupe de $\mathfrak{S}_n$, tel que H contienne la représentation Γ de $\mathrm{Gal}_k(f)$ dans $\mathfrak{S}_n$ et que $\theta = \Theta(x_1, ..., x_n) \in k$ soit racine simple de $\mathcal{L}_{\Theta,f}$. Alors on a:*

$$I(f) = (E_1 - a_1, ..., E_n - a_n, \Theta - \theta) \iff H = \Gamma.$$

Preuve – Voir [7, Théorèmes 5.1 et 5.2]. □

Plus généralement, on a même:

Théorème 7.9 *Soit $\Theta \in k[\mathbf{X}]$ un invariant primitif du sous-groupe H de $\mathfrak{S}_n$. On suppose que $\theta = \Theta(\mathbf{x})$ est racine simple dans $\hat{k}$ de $\mathcal{L}_{\Theta,f}$. Soit h le facteur irréductible de $\mathcal{L}_{\Theta,f}$ qui a θ pour racine. Soit $\Theta_1, \ldots, \Theta_r \in k[\mathbf{X}]^{\mathfrak{S}_n}$ tel que $h = \prod_{i=1}^{r}(T - \Theta_i(\mathbf{x}))$ et $S = \mathcal{S}tab_{\mathfrak{S}_n}(\Theta_1, \ldots, \Theta_r)$. On a alors:*

$$I(f) = (E_1 - a_1, ..., E_n - a_n, h(\Theta)) \iff H = S.$$

Preuve – Voir [7, Théorème 5.3]. Voir aussi un résultat plus précis dans [64]. □

Chapitre 8

Calcul du groupe de Galois par descente directe dans le graphe des classes de conjugaison de sous-groupes

Résumé

We propound a systematic and formal method to compute the Galois group of a non-necessarily irreducible polynomial: we proceed by successive inclusions, using mostly computations on scalars (and very few on polynomials). It is based on a formal method of specialization of relative resolvents: it consists in expressing the generic coefficients of the resolvent using the powers of a primitive element, thanks to a quadratic space structure; this reduces the problem to that of specializing a primitive element, which we are able to do in the case of the descending by successive inclusions. We incidentally supply a way to make separable a resolvent.

8.1 Introduction

Let $f \in k[T]$ be a monic polynomial — which need not be irreducible —, with degree $n \geq 2$, where k is a field of characteristic zero. Let $\mathbf{x} = (x_1, \ldots, x_n)$ the family of the roots of f in a splitting field of f over k. The Galois group $\mathrm{Gal}_k(f) = \mathrm{Gal}(k(\mathbf{x}) : k)$ — that is, by definition, the group of k-algebra automorphismes of $k(\mathbf{x})$ — acts faithfully on the set of the roots of f; so, the chosen numbering $\mathbf{x}$ of the roots defines a faithfully action of $\mathrm{Gal}_k(f)$ on the set $\mathbb{N}_n^* = \{1, 2, \ldots, n\}$, *i.e.* a representation Γ of the group $\mathrm{Gal}_k(f)$ in the symmetric group $\mathfrak{S}_n$. The aim of this article is to give a formal method to compute the conjugacy class $[\Gamma]$ of Γ in $\mathfrak{S}_n$, *i.e.* Γ up to a permutation of the roots.

Up to now, two different types of methods grounded on resolvents are used to compute the Galois group of a polynomial — saying nothing of methods grounded on factorization in successive field-extensions (for these methods, introduced by Tchebotarev, see a practical realization in [3]).

The first ones are formal methods. Grounded on the factorization of absolute Lagrange resolvents — they are polynomials obtained from f by a transformation linked to an invariant of a subgroup of $\mathfrak{S}_n$ (see Paragraph 8.3.1) —, they were introduced by Lagrange, used by Berwick (see [10], [11]), McKay and Soicher (see [52] and [59]), then by Arnaudiès and Valibouze (see the *chasse aux résolvantes* in [7], and [70], [69]). These methods used to be non-deterministic; Arnaudiès and Valibouze made them deterministic by a systematic *a priori* construction of tables of partitions related to the subgroups of

the symmetric group. Besides, they showed that relative resolvents — which used to be used only in numerical methods — can be used also in the *chasse aux résolvantes*.

The second ones are numerical, *i.e.* they use approximated values of the roots of f. If we give approximated values of the roots that are accurate enough to enable to distinguish them one another, then we can define Γ effectively (as long as we cannot distinguish the roots, only its conjugacy class has a sense, from an effective point of view). Innovated by Stauduhar (see [61]) and continued by Eichenlaub and Olivier (see [22]), these methods work by descending in the oriented graph of subgroups of $\mathfrak{S}_n$ by successive inclusions, till meeting Γ (for the details, see Paragraph 8.4.2). The inclusion tests use relative resolvents (*i.e.* resolvents where the role of $\mathfrak{S}_n$ is played by one of its subgroups).

The dichotomy between these two types of methods (formal methods for absolute resolvents, numerical methods for relative ones) was justified because one did not know how to compute relative resolvents but numerically. The goal of this article is to show that we can compute formally relative resolvents. On the one hand, it enables to make formal Stauduhar's method; on the other hand, to introduce relative resolvents (it is interesting because their degree is lower, hence their factorization faster) in the methods using absolute resolvents, as Arnaudiès and Valibouze suggested.

The Results

Section 8.4 presents the "formal Stauduhar method". It is exposed in Lemma 8.9.

For this aim, Section 8.3 introduces a formal method to specialize relative resolvents by the roots $\mathbf{x}$ of f ("specialize by $\mathbf{x}$" means to replace each indeterminate X_i by the root x_i).

We stress the Proposition 8.5, which gives an algorithm to make separable an invariant thanks to an easy transformation.

Section 8.2 explains how we can reduce the specialization of a resolvent to that of a single primitive element (it will be applied to Section 8.4, where the specialized value of this primitive element will be known).

In Section 8.5, we explain the current state and the prospects of implementation, and conclude by the expectable field of application of our method.

Remark 8.1 *Talking of a formal way to specialize relative resolvents can seem paradoxical, because formal methods don't allow to label the roots of f; so, as it prevented us of defining Γ but up to conjugation (see* supra*), it prevents us of defining a specialized relative resolvent. This paradox will be solved later, in fact in the proof of Lemma 8.9: we shall show that we can do all the middle computations without knowing exactly which relative resolvents we are computing, while the final result (*i.e. $[\Gamma]$*) doesn't depend on these uncertain middle results.*

Notations

If a group G acts on a set E, we note $\mathcal{S}tab_G(A)$ the stabilizer in G of an element or a subset A of E. If H is a subgroup of a group G, we note $(G/H)_g$ the set of left classes modulo H and $(G//H)_g$ a representing family for these classes. If K is a field and G a group of automorphismes of K, we note K^G the subfield of the elements of K unmoved by all G. Let $\mathbf{X} = (X_1, \ldots, X_n)$, where the X_i are indeterminates on k. The symmetric group $\mathfrak{S}_n$ acts on $k[X_1, \ldots, X_n]$ with $\sigma.X_i = X_{\sigma(i)}, i \in \mathbb{N}_n^*, \sigma \in \mathfrak{S}_n$; and on $\mathbb{N}^n$ with $\sigma.(\alpha_1, \ldots, \alpha_n) = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ (so, $\sigma.\mathbf{X}^\alpha = \mathbf{X}^{\sigma^{-1}.\alpha}$). Let $\mathbf{E} = (E_1, \ldots, E_n)$, where $E_i = \sum_{j \in (\mathbb{N}_n^*)^i, j_1 < \ldots < j_i} \prod_{l=1}^{i} X_{j_l}$ for all $i \in \mathbb{N}_n^*$ (elementary symmetric polynomials). By the fundamental theorem on symmetric polynomials, $k[\mathbf{E}] = k[E_1, \ldots, E_n]$ is the ring of symmetric polynomials in $X_1, \ldots, X_n$.

In the following, f shall be supposed separable. Anyway, if f were not, we could replace it by the associated square-free polynomial, *i.e.* $f/\text{PGCD}(f, f')$: it wouldn't change $k(\mathbf{x})$, neither $\text{Gal}(k(\mathbf{x}) : k)$.

We suppose given for the whole article a numbering $\mathbf{x} = (x_1, \ldots, x_n)$ of the roots of f; let's recall that this numbering is non-effective, as we don't give any approximated value of the roots.

8.2 Expression of the $k(\mathbf{X})^L$ Elements Thanks to a Primitive Element

For this problem, we refer to chapter 3. We just remind that it proves that if $L \subset M \subset \mathfrak{S}_n$ and if Θ is a primitive M-relative L-invariant, *i.e.* if $\mathcal{S}tab_M(\Theta) = L$, then

$$k(\mathbf{X})^L = \bigoplus_{i=0}^{e-1} k(\mathbf{X})^M.\Theta^i \qquad \text{where} \quad e = [M : L].$$

Besides, chapter 3 (see Prop. 3.10) gives an efficient algorithm to express an invariant of L in terms of Θ and invariants of M.

8.3 Specialization of a Relative Resolvent Polynomial

We show in this section how the method expounded in Paragraph 8.2 enables to specialize an L-relative resolvent, where L is a subgroup of $\mathfrak{S}_n$, provided the specialized value of a primitive element of the field-extension $k(\mathbf{X})^L : k(\mathbf{E})$ is known.

In the rest of the article, for a $P \in k(\mathbf{X})$, $\tilde{P}$ will denote $P(x_1, \ldots, x_n)$, *i.e.* P specialized in the roots of f.

8.3.1 Lagrange Resolvents

Resolvents were introduced by Lagrange (see [44], [45], [46]) in order to compute the relations between the roots of a polynomial and to study (in his own language) the field-extensions associated to these roots. It enabled him to unify in a way the former methods (Cardan, Ferrari) used to solve algebraic equations up to degree 4, and to understand why should not exist such methods beyond degree 4.

The presentation we use was introduced in [7] by Arnaudiès and Valibouze.

Definition 8.2 Let L a subgroup of $\mathfrak{S}_n$ and H a subgroup of L. We call L-relative H-invariant in degree n a polynomial $\Psi \in k[\mathbf{X}]$ such that $\mathcal{S}tab_L(\Psi) = H$, *i.e.* a primitive element of the field-extension $k(\mathbf{X})^H : k(\mathbf{X})^L$. We call generic L-relative resolvent of such a Ψ the minimal polynomial of Ψ over $k(\mathbf{X})^L$, *i.e.* the polynomial

$$\mathcal{L}_\Psi^L = \prod_{\sigma \in (L//H)_g} (T - \sigma.\Psi(X_1, \ldots, X_n)) \in k(\mathbf{X})^L[T] \qquad .$$

When L contains Γ, we define the specialized form of $\mathcal{L}_\Psi^L$ by the roots $\mathbf{x} = (x_1, \ldots, x_n)$ of f as the polynomial $\mathcal{L}_{\Psi,\mathbf{x}}^L$ computed by substituting the root x_i to each X_i. It belongs to $k[T]$, as the elements of Γ leave its coefficients unaltered (because $\Gamma \subset L$).

We call absolute resolvent (resp. invariant) an $\mathfrak{S}_n$-relative resolvent (resp. invariant). We note $\mathcal{L}_\Psi$ for $\mathcal{L}_\Psi^{\mathfrak{S}_n}$ and $\mathcal{L}_{\Psi,\mathbf{x}}$ for $\mathcal{L}_{\Psi,\mathbf{x}}^{\mathfrak{S}_n}$.

An L-relative invariant Ψ (resp. a generic relative resolvent $\mathcal{L}_\Psi^L$) is said $\mathbf{x}$-separable if and only if $\mathcal{L}_{\Psi,\mathbf{x}}^L$ is square-free.

8.3.2 Specialization in the Generic Case

Let L be a subgroup of $\mathfrak{S}_n$ that contains Γ, H a subgroup of L, Θ an absolute L-invariant and Ψ an L-relative H-invariant. It is easy to compute the generic relative resolvent $\mathcal{L}_\Psi^L \in k(\mathbf{X})^L[T]$. We shall give in this paragraph a method to specialize its coefficients, in order to compute $\mathcal{L}_{\Psi,\mathbf{x}}^L$, provided we know the value $\theta = \tilde{\Theta} = \Theta(x_1, \ldots, x_n) \in k$ that Θ takes on the roots $\mathbf{x}$ of f — which we shall suppose granted in the rest of Section 8.3.

Each coefficient P of $\mathcal{L}_\Psi^L$ belongs to $k(\mathbf{X})^L$; so either method of Prop. 3.10 applies, and enables us to express P in Θ and the symmetric polynomials. By hypothesis, $\tilde{\Theta}$ is known; and the $\tilde{E}_i$ are — up to the sign — the coefficients of f. Thus, we know the value of $\tilde{P}$. Of course, all the computations (solvation of a linear system or Gram-Schmidt orthogonalization) are to be done after specializing, in order to compute only on scalars.

But we passed over a very important point: denominators may become zero through specialization... In fact, it happens if and only if $\widetilde{\Delta^\Theta} = 0$ for the method using a linear system (resp. iff $\exists l \in \mathbb{N}_{e-1} / \widetilde{\Delta_l^\Theta} = 0$, for the method using Gram-Schmidt orthogonalization), where $\Delta^\Theta = \det((< \Theta_i, \Theta_j >)_{(i,j)\in(\mathbb{N}_{e-1})^2})$ (resp. $\Delta_l^\Theta = \det((< \Theta_i, \Theta_j >)_{(i,j)\in\mathbb{N}_l^2})$ denotes the Gram determinant of $< ., . >$ (resp. of the form induced by $< ., . >$ on $\bigoplus_{j=0}^{i} k.\Theta^j$) in the basis $(1, \Theta, \ldots, \Theta^{e-1})$ (resp. $(1, \Theta, \ldots, \Theta^l)$).

We shall deal in Paragraph 8.3.3 with the cases when $\exists l \in \mathbb{N}_{e-1}$ / $\widetilde{\Delta_l^\Theta} = 0$.

8.3.3 Case of Cancellation of the Denominators

We now deal with the cases when the k-form $\widetilde{< ., . >}$ ($< ., . >$ composed with specialization) or the form that it induces on a space $\bigoplus_{i=0}^{l} k.\Theta^i$ is degenerated; *i.e.* when one of the symmetric polynomials Δ_l^Θ takes the value 0 on $(x_1, \ldots, x_n)$.

The principle consists in coming down to the generic case (Paragraph 8.3.2) by using an other $\mathbf{x}$-separable L-invariant Θ' such that $\forall l \in \mathbb{N}_{e-1}, \widetilde{\Delta_l^{\Theta'}} \neq 0$. We will exhibit an algorithm that yields such a Θ'. We require $\mathbf{x}$-separability because of the use in the following (see Proposition 8.7).

Propositions 8.3, 8.4 and 8.5 will reduce the problem to that of finding a point out of a given algebraic variety.

Proposition 8.3 *Let $p \in k[T]$ a non-constant polynomial. Then $\Theta' = \Theta(p(X_1), \ldots, p(X_n)) \in k[\mathbf{X}]$ is still an absolute L-invariant.*

Proof – Let $\sigma \in \mathfrak{S}_n$. Then $(\sigma.\Theta)(p(X_1), \ldots, p(X_n)) = \Theta(p(X_1), \ldots, p(X_n))$ if and only if $\sigma.\Theta = \Theta$, because $(p(X_1), \ldots, p(X_n))$ is algebraically free over k. □

In the following, $\Theta \circ p$ shall denote the polynomial $\Theta(p(X_1), \ldots, p(X_n))$.

Proposition 8.4 *Let $f \in k[T]$ a separable polynomial whose expression in a splitting field is $\prod_{i=1}^{n}(T - x_i)$. Then for all non-zero symmetrical polynomial $\Delta \in k[X_1, ..., X_n]$, there exists a polynomial $p \in k[Y]$ such that $\Delta(p(x_1), ..., p(x_n)) \neq 0$. More accurately, there exists an algebraic hypersurface V of k^n, with $\deg(V) = \deg(\Delta)$, such that for all $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n$, the polynomial $p = \lambda_0 + \lambda_1.Y + \ldots + \lambda_{n-1}.Y^{n-1}$ suits the problem if and only if $(\lambda_0, \ldots, \lambda_{n-1}) \notin V$.*

Proof – Let $\Lambda_0, \ldots, \Lambda_{n-1}$ indeterminates on $k(\mathbf{x})(Y, T)$. Let F be the polynomial belonging to $k(\mathbf{x})[\Lambda_0, \ldots, \Lambda_{n-1}]$ defined by:

$$F = \Delta(\Lambda_0 + x_1.\Lambda_1 + \ldots + x_1^{n-1}.\Lambda_{n-1}, \ \ldots \ , \Lambda_0 + x_n.\Lambda_1 + \ldots + x_n^{n-1}.\Lambda_{n-1}).$$

Then F belongs to $k[\Lambda_0, \ldots, \Lambda_{n-1}]$, as its coefficients, symmetrical in $x_1, \ldots, x_n$ because Δ is symmetrical, are left unmoved by $\mathrm{Gal}(k(\mathbf{x}) : k)$.

Let us now prove that F is non-zero. There exists $(y_1, \ldots, y_n) \in k^n$ such that $\Delta(y_1, \ldots, y_n) \neq 0$, because $\Delta \neq 0$ and k infinite. Now, there exists $(\lambda_0, \ldots, \lambda_{n-1})$ in $k(\mathbf{x})^n$ such that $\forall i \in \mathbb{N}_n^*$, $y_i = \lambda_0 + \lambda_1 x_i + \ldots + \lambda_{n-1} x_i^{n-1}$, because the λ_l are solutions of a linear system on the field $k(\mathbf{x})$, whose determinant is the Vandermonde determinant of $(x_1, \ldots, x_n)$, *i.e.* $\prod_{1 \leq i < j \leq n}(x_j - x_i)$; which is not zero because f is supposed square-free. Therefore $F(\lambda_0, \ldots, \lambda_{n-1}) = \Delta(y_1, \ldots, y_n) \neq 0$, so $F \neq 0$ as an element of $k(\mathbf{x})[\Lambda_0, \ldots, \Lambda_{n-1}]$, hence also as a member of $k[\Lambda_0, \ldots, \Lambda_{n-1}]$.

Therefore, the set $V = \{(\lambda_0, \ldots, \lambda_{n-1}) \in k^n / F(\lambda_0, \ldots, \lambda_{n-1}) = 0\}$ is an algebraic hypersurface of k^n; and $V \neq \emptyset$ because k is infinite and $F \neq 0$. The elements of $k^n \setminus V$ are exactly the n-tuples $(\lambda_0, \ldots, \lambda_{n-1})$ such that the scalar $F(\lambda_0, \ldots, \lambda_{n-1}) = \Delta(p(x_1), \ldots, p(x_n))$ is non-zero. □

Proposition 8.5 is written here because its proof looks like Proposition 8.4's; but it has a more general interest. Thus, it completes [7, théorème 4.5], that proved theoretically the existence of an $\mathbf{x}$-separable invariant of a given group.

Proposition 8.5 *Let $f \in k[T]$ a separable polynomial whose expression in a splitting field is $\prod_{i=1}^{n}(T - x_i)$. Let Θ an absolute L-invariant, where L is a subgroup of $\mathfrak{S}_n$. Then the set of the n-tuples $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n$ such that $\Theta \circ p = \Theta(p(X_1), \ldots, p(X_n))$ is $\mathbf{x}$-separable, where p denotes $\sum_{l=0}^{n-1} \lambda_l . Y^l$, is not empty. More accurately, this set can be written $k^n \setminus W$ where W is an algebraic hypersurface of k^n with $\deg(W) \leq dh(h-1)$, where $d = \deg(\Theta)$ and $h = [\mathfrak{S}_n : L]$.*

Proof – By definition, $\Theta \circ p$ is $\mathbf{x}$-separable if and only if the discriminant of $\mathcal{L}_{\Theta \circ p, \mathbf{x}}$ is not zero. Let $\Lambda_0, \ldots, \Lambda_{n-1}$ be indeterminates over $k(\mathbf{x})(\mathbf{X}, Y, T)$. Let $P = \Lambda_0 + \Lambda_1 Y + \ldots + \Lambda_{n-1} Y^{n-1} \in k[\mathbf{\Lambda}][Y]$. We know that $\mathcal{L}_{\Theta \circ P, \mathbf{x}}$ belongs to $k[\Lambda_0, \ldots, \Lambda_{n-1}][T]$, and has degree h in T; and this resolvent can be written $\sum_{i=0}^{h} A_i T^i$ where $A_h = 1$ and $A_i \in k[\Lambda_0, \ldots, \Lambda_{n-1}]$ is homogeneous with $\deg(A_i) \leq d(h - i)$, for all $i \in \mathbb{N}_h$. Now, let us compute its discriminant, F; it is the following resultant in T: $F = \mathcal{R}es_T(\mathcal{L}_{\Theta \circ P, \mathbf{x}}, \partial(\mathcal{L}_{\Theta \circ P, \mathbf{x}})/\partial T) \in k[\Lambda_0, \ldots, \Lambda_{n-1}]$. Writing the Sylvester determinant form of this resultant, we notice that each of its monomial terms can be written $\prod_{i=0}^{h} A_i^{\alpha_i}$ where the α_i are non-negative integers such that $h\alpha_0 + (h-1)\alpha_1 + \ldots + \alpha_{h-1} = h(h-1)$. Therefore, F is an homogeneous polynomial and $\deg(F) \leq dh(h-1)$. So if $F \neq 0$, then it defines an algebraic hypersurface W of k^n, with $\deg(F) \leq dh(h-1)$, such that for all $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n \setminus W$, the discriminant $F(\lambda_0, \ldots, \lambda_{n-1})$ of $\mathcal{L}_{\Theta \circ p, \mathbf{x}} \in k[T]$ is not zero, *i.e.* $\mathcal{L}_{\Theta \circ p, \mathbf{x}}$ is separable (where p still denotes $\sum_{l=0}^{n-1} \lambda_l Y^l$).

There remains to prove that $F \in k[\Lambda_0, \ldots, \Lambda_{n-1}]$ is non-zero. Let $\mathcal{F} = \mathcal{R}es_T(\mathcal{L}_\Theta, \partial\mathcal{L}_\Theta/\partial T) \in k[X_1, \ldots, X_n]$ (discriminant in T of $\mathcal{L}_\Theta$). We notice that $F = \mathcal{F}(P(x_1), \ldots, P(x_n))$; it can be seen *e.g.* by writing the Sylvester determinant form of the resultant. Now, $\mathcal{F} \neq 0$, because $\mathcal{L}_\Theta$ is separable (it is the minimal polynomial of Θ on $k(\mathbf{E})$). As k is infinite, there exists $(y_1, \ldots, y_n) \in k^n$ such that $\mathcal{F}(y_1, \ldots, y_n) \neq 0$. For the same reason as in the proof of Proposition 8.4, f's square-freeness implies that there exists scalars $\lambda_0, \ldots, \lambda_{n-1} \in k(\mathbf{x})$ such that for all $i \in \mathbb{N}_n^*$, $y_i = \sum_{l=0}^{n-1} \lambda_l x_i^l$. Hence, $F(\lambda_0, \ldots, \lambda_{n-1}) = \mathcal{F}(y_1, \ldots, y_n) \neq 0$; thus $F \neq 0$. □

Let W be the variety defined by Proposition 8.5, and for all $i \in \mathbb{N}_{e-1}$, V_i the variety defined by Proposition 8.4 applied to $\Delta = \Delta_i^\Theta$. Propositions 8.3 and 8.4 show that for any point $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n \setminus (W \cup V_0 \cup V_1 \cup \ldots \cup V_{e-1})$, the polynomial $\Theta' = \Theta \circ p$, where $p = \sum_{j=0}^{n-1} \lambda_j . T^j$, is an absolute $\mathbf{x}$-separable L-invariant such that $\forall\, i \in \mathbb{N}_{e-1}, \widetilde{\Delta_i^{\Theta'}} \neq 0$.

We have reduced the problem to finding a point $(\lambda_0, \ldots, \lambda_n)$ out of the hypersurface $V = W \cup V_0 \cup V_1 \cup \ldots \cup V_{e-1}$. Let $D \in k[X_0, \ldots, X_{n-1}]$ be a polynomial defining V, *e.g.* the l.c.m. of polynomials defining W, V_0, ...,V_{e-1}. We needn't to compute D (it would be to expensive). We just need a bound d for its degree (it is yielded by Propositions 8.5 and 8.4), and to be able to test the nullity of $D(\lambda_0, \ldots, \lambda_{n-1})$ for a given $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n$ (and we are able, thanks to the generic case algorithm, provided k is an effective field).

A classical algorithm to find a $(\lambda_0, \ldots, \lambda_n)$ out of V consists in choosing, for all $i \in \mathbb{N}_{n-1}$, a finite subset A_i of k, with cardinal $d_i + 1$ where d_i is the partial degree of D in X_i. We can prove by induction on n that there exists $(\lambda_0, \ldots, \lambda_{n-1}) \in \prod_{i=0}^{n-1} A_i$ such that $\Delta(\lambda_0, \ldots, \lambda_{n-1}) \neq 0$. It enables us to find a $(\lambda_0, \ldots, \lambda_{n-1}) \in k^n \setminus V$ with at most $(d+1)^n$ evaluation tests.

Let's notice that this algorithm enables to compute p with the lowest possible degree: we chose $A_1, \ldots, A_{n-1}$ so that they all contain 0, and we begin with testing the points $(\lambda_0, \lambda_1, 0, \ldots, 0), (\lambda_0, \lambda_1) \in A_0 \times A_1$. If all of them belong to V, then V contains the whole plan $k^2 \times \{0_{n-2}\}$; so no polynomial p of degree 1 suits our conditions. Then we test all the $(\lambda_0, \lambda_1, \lambda_2, 0, \ldots, 0)$, and if all of them belong to V, no polynomial p of degree 2 is suitable; and so on.

8.4 Formal Stauduhar Method

8.4.1 The Graph of all Conjugacy Classes of Subgroups of $\mathfrak{S}_n$

Stauduhar computes Γ by descending in the Directed Acyclic Graph (D.A.G.) of subgroups of $\mathfrak{S}_n$. We shall follow this scheme to compute $[\Gamma]$, and define the D.A.G. of all conjugacy classes of subgroups of $\mathfrak{S}_n$, thanks to the following proposition:

Proposition 8.6 *Let L a finite group. The relation $\prec$ defined on the set $\mathcal{C}(L)$ of all the L-conjugacy classes of subgroups of L by:*

$$\forall\, \mathcal{H} \in \mathcal{C}(L), \forall\, \mathcal{K} \in \mathcal{C}(L), \mathcal{H} \prec \mathcal{K} \Longleftrightarrow \exists\, H \in \mathcal{H}, \exists\, K \in \mathcal{K}, H \subset K$$

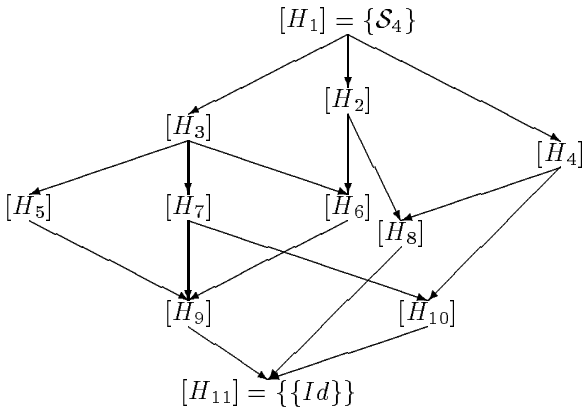
is an order relation.

Proof – Reflexivity and antisymmetry result of the fact that, as L is finite, the only conjugate of a subgroup H of L that contains H is H. □

BEWARE: $(\mathcal{C}(L), \prec)$ is not always a lattice; *e.g.* $(\mathcal{C}(\mathfrak{S}_n), \prec)$ is a lattice for $n \leq 4$, but not for $n = 5$ (for example, in $\mathcal{C}(\mathfrak{S}_5)$, $\{[\mathfrak{S}_2 \times \{Id_3\}], [\mathfrak{A}_3 \times \{Id_2\}]\}$ has no supremum).

If H is a subgroup of L, $L \subset \mathfrak{S}_n$, we shall note $[H]_L$ the L-conjugacy class of H. When $L = \mathfrak{S}_n$, we shall note it $[H]$.

Let us note $\mathcal{G}_{\mathfrak{S}_n}$ the D.A.G. of all $\mathfrak{S}_n$-conjugacy classes of subgroups of $\mathfrak{S}_n$ defined by $\prec$ on $\mathcal{C}(\mathfrak{S}_n)$; *i.e.* the children of an $\mathcal{H} \in \mathcal{C}(\mathfrak{S}_n)$ are the maximal elements of $\{\mathcal{K} \in \mathcal{C}(\mathfrak{S}_n) / \mathcal{K} \precneqq \mathcal{H}\}$. This graph is of course connected. But it is not generally a tree, as a not may have several parents, *e.g.* $[H_9]$ in the following graph $\mathcal{G}_{\mathcal{S}_4}$:



8.4.2 Method of Descending in the Graph

The method consists in descending in the branches of the graph $\mathcal{G}_{\mathfrak{S}_n}$, by testing inclusions, until we find the conjugacy class $[\Gamma]$ of Γ.

More accurately: let us assume for the moment that we know how to test, for a given $[H] \in \mathcal{C}(\mathfrak{S}_n)$, if $[\Gamma] \prec [H]$. The method consists in beginning with $[L] = [\mathfrak{S}_n]$ and the initial graph $\mathcal{G}_{\mathfrak{S}_n}$, and testing for all children (i.e. maximal descendants) $[H]$ of $[L]$ if $[\Gamma] \prec [H]$. If no child $[H]$ matches, then we know that $[\Gamma] = [L]$. Otherwise, let $[H_0]$ be a child such that $[\Gamma] \prec [H_0]$. Then we take it as new $[L]$, the branch it carries as new graph — after having cut off every descendant whose other father has already been ruled out (*e.g.* in the latter example, if we have tested that $[\Gamma] \not\prec [H_3]$ and that $[\Gamma] \prec [H_2]$, then we know that $[\Gamma] \not\prec [H_6]$, and we can cut $[H_6]$ off the branch carried by $[H_2]$) — and we go on with this new graph and this new $[L]$. The algorithm must terminate, because $\mathcal{G}_{\mathfrak{S}_n}$ is finite.

8.4.3 A few Preliminary Results

• The following property, used by Stauduhar, enables to test if $[\Gamma] \prec [H]$ provided we know a resolvent of H:

Proposition 8.7 *Let L and H two subgroups of $\mathfrak{S}_n$ such that $\Gamma \subset L$ and $H \subset L$. Let Ψ an $\mathbf{x}$-separable L-relative H-invariant. Then we have $[\Gamma]_L \prec [H]_L$ if and only if $\mathcal{L}^L_{\Psi,\mathbf{x}}$ has a root in k.*

Proof – See [61] or [7]. □

Testing if $\mathcal{L}^L_{\Psi,\mathbf{x}}$ has a root in k (*i.e.* a linear factor) can be done thanks to a factorizing algorithm.

Remark 8.8 *Proposition 8.7 stresses a central problem: its hypothesis is $\Gamma \subset L$, whereas such an inclusion has no sense for us but up to conjugation (see Remark 8.1). We explain how to solve this problem in the proof of Lemma 8.9.*

• If H and L are subgroups of $\mathfrak{S}_n$ such that $H \subset L$, then there exists an $\mathbf{x}$-separable L-relative H-invariant Ψ; Arnaudiès and Valibouze prove it constructively in [7, théorème 4.5]. But the invariant their algorithm yields has usually a very high degree. On the other hand, Girstmair gives in [29] an algorithm that computes the lowest degree absolute H-invariant. And Proposition 8.5 of this article enables to make $\mathbf{x}$-separable Girstmair's invariant.

• Softwares as G.A.P. (cf. [58]) are able to do all the group computations that we need to descend in the graph $\mathcal{G}_{\mathfrak{S}_n}$: find all conjugacy classes of subgroups of a given group, test inclusions, etc.

8.4.4 A Formal "Stauduhar Method"

We are now able to present the algorithm: we saw in Section 8.3 how to compute an L-relative resolvent, provided we know the specialized value of an L-invariant. We presented in the beginning of this section the method of descent in the graph $\mathcal{G}_{\mathfrak{S}_n}$. It remains to prove that during the descent, we can by the way, at each step, get the specialized value of an invariant of the group relatively to which we work. We also have to show how we manage to use a relative resolvent although we don't know using which order of the roots of f it is defined (see Remarks 8.8 and 8.1).

The algorithm is presented recursively by the proof of Lemma 8.9.

Let $N \in \mathbb{N}^*$ be the greatest index $[H : K]$ for all subgroups H of $\mathfrak{S}_n$ and for all maximal subgroup K of H.

For all $\nu \in \mathbb{N}$, let $\mathcal{HR}(\nu)$ the following induction hypothesis:

$\mathcal{HR}(\nu)$: *We know how to compute formally, using only factorizations of polynomials with degree less than* N,

i. A strictly decreasing (for inclusion) sequence $(L_0 = \mathfrak{S}_n, L_1, \ldots, L_\nu)$ *of subgroups of* $\mathfrak{S}_n$, *such that* $[\Gamma] \prec [L_\nu]$.

ii. If $\nu \geq 1$, *an absolute* L_ν*-invariant* Θ_ν *such that* $\widetilde{\Delta^{\Theta_\nu}} \neq 0$, *and the value* $\theta_\nu \in k$ *of* $\widetilde{\tau.\Theta_\nu}$, *for an unknown* $\tau \in \mathfrak{S}_n$ *(but of course* τ *must satisfy* $\Gamma \subset \tau.L_\nu.\tau^{-1}$*).*

By "unknown $\tau \in \mathfrak{S}_n$", we mean a τ whose existence we can assess but that we cannot specify, as the roots of f haven't been identified (see the Introduction).

Lemm 8.9 *If* $\mathcal{HR}(\nu)$ *is true, then either* $\mathcal{HR}(\nu+1)$ *is true, either we know* $[\Gamma]$.

Proof – Indeed, let's assume $\mathcal{HR}(\nu)$. Let $L = L_\nu$, $\Theta = \Theta_\nu$ and $\theta = \theta_\nu$. Let $\mathcal{M}$ be the set of maximal elements for $\prec$ of $\mathcal{C}(L) \setminus \{L\}$ (in practice, we can first cut off some vertices of the branch carried by L, hence some elements of $\mathcal{M}$, as explained in Paragraph 8.4.2). We know that $\Gamma \subset \tau.L.\tau^{-1}$ for some unknown $\tau \in \mathfrak{S}_n$. Now, either $[\Gamma] = [L]$, or $[\Gamma] \precneqq [L]$. The second assertion is equivalent to: $\exists\, \mathcal{H} \in \mathcal{M}, \exists\, H \in \mathcal{H}, \Gamma \subset \tau.H.\tau^{-1}$. Thus, we shall test if it is true, as follows:

Let $\mathcal{H} \in \mathcal{M}$. We chose at random an $H \in \mathcal{H}$ (so, $[H]_L = \mathcal{H}$), we compute an absolute $\mathbf{x}$-separable H-invariant Ψ (see Paragraph 8.4.3) such that $\Delta^\Psi(\mathbf{x})$ be non-zero (see Paragraph 8.3.3), and we compute the generic resolvent $\mathcal{L}^L_\Psi$. But what we want to compute is $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi,\mathbf{x}}$. We notice that $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi} = \tau.\mathcal{L}^L_\Psi$: indeed,

$$\tau.\mathcal{L}^L_\Psi = \prod_{\sigma \in (L//H)_g} (T - \tau.\sigma.\Psi) = \prod_{\sigma' \in (\tau.L.\tau^{-1}//\tau.H.\tau^{-1})_g} (T - \sigma'.\tau.\Psi) = \mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi} \quad ;$$

so, if we specialize: $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi,\mathbf{x}} = \mathcal{L}^L_{\Psi,\tau.\mathbf{x}}$.

But we are able to compute $\mathcal{L}^L_{\Psi,\tau.\mathbf{x}}$ by the algorithm of Paragraph 8.3.2 applied to $\mathcal{L}^L_\Psi$: indeed, L contains $\tau^{-1}.\Gamma.\tau$, which is the representation in $\mathfrak{S}_n$ of $\mathrm{Gal}_k(f)$ with the numbering $\tau.\mathbf{x}$ of the roots of f; we know the specialized value of Θ by $\tau.\mathbf{x}$ (it is the specialized value of $\tau.\Theta$ by $\mathbf{x}$, which is θ), and Θ is an absolute L-invariant, such that $\Delta^\Theta(\tau.\mathbf{x}) = \Delta^\Theta(\mathbf{x})$ be non-zero. Therefore, we are able to compute $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi,\mathbf{x}}$ (although we don't know τ).

Then, we test if $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi,\mathbf{x}}$ has a linear factor, using a suitable factorization algorithm. If there are some, we take one at random, let it be $T - \psi$. Then there exists $t \in \tau.L$ such that $\psi = \widetilde{t.\Psi}$; and we take $L_{\nu+1} = H$, $\Theta_{\nu+1} = \Psi$ and $\theta_{\nu+1} = \psi$: they satisfy $\mathcal{HR}(\nu+1)$. On the contrary, if $\mathcal{L}^{\tau.L.\tau^{-1}}_{\tau.\Psi,\mathbf{x}}$ has no root in k, then we do again all what we did above with the other $\mathcal{H} \in \mathcal{M}$ till we get a resolvent that has a linear factor. If none has for any $\mathcal{H} \in \mathcal{M}$, it means (from Proposition 8.7) that Γ — which, as we know, is included in $\tau.L.\tau^{-1}$ — isn't included in any maximal subgroup of $\tau.L.\tau^{-1}$; hence $\Gamma = \tau.L.\tau^{-1}$, so we then know $[\Gamma] = [L]$. □

Now, $\mathcal{HR}(0)$ is trivially true, and as the sequence $(L_0, L_1, \ldots, L_\nu)$ cannot decrease indefinitely, Lemma 8.9 proves that we can compute $[\Gamma]$ by formal computation, requiring only factorizations of polynomials in $k[T]$ whose degree is bounded by N.

Remark 8.10 *We can notice that although globally the method consists in a descent in the graph* $\mathcal{G}_{\mathfrak{S}_n}$ *(conjugacy classes relative to* $\mathfrak{S}_n$*), locally* (i.e. *at a given step* ν *of the induction), we have to consider conjugacy classes relative to a subgroup* L *— but then,* L *itself is defined up to conjugacy in* $\mathfrak{S}_n$, *which is quite normal, as conjugacy classes have no sense for us, because we cannot identify the roots (see the Introduction). Besides, contrary to the numerical methods, we never need to guess in which accurate conjugate* Γ *is included.*

Remark 8.11 *If f is irreducible, we should of course replace the graph $\mathcal{G}$ of all conjugacy classes by that of classes of transitive subgroups — because when f is irreducible,* $\mathrm{Gal}_k(f)$ *acts transitively on the roots of f.*

8.5 Implementation of the Algorithm

The algorithm is in process of implementation into the computer algebra system AXIOM (see [37]). Currently, the Section 8.3 is implemented, and also a domain that handles symmetric polynomials and "pseudo-symmetric polynomials" (elements of $k[\mathbf{X}]^L$, where L is a subgroup of $\mathfrak{S}_n$), with a representation that keeps only one monomial for each orbit.

There remains to implement an algorithm based on [29], to compute invariants; and the "formal Stauduhar algorithm" (Section 8.4). For the latter, we shall use G.A.P. (see [58]) for all calculations on groups. We should also implement a procedure that yields all the maximal elements of $\mathcal{C}(L)$ for a given group $L \subset \mathfrak{S}_n$ (there exists already one that computes all the elements of $\mathcal{C}(L)$ but it is of course very slow; we cannot go further than subgroups of $\mathfrak{S}_{15}$): it would enable to compute dynamically the graph $\mathcal{G}_{\mathfrak{S}_n}$ of Paragraph 8.4.1, *i.e.* to build only the branches that we need, as one descends along $\mathcal{G}_{\mathfrak{S}_n}$ by successive inclusions.

As for the prospects: this method should have a rather low complexity because all the degrees of any polynomial that we factorize are bounded by N (see Paragraph 8.4.4); and the "average" value of a bound should look like $(n!)^{1/\delta(n)}$, where $\delta(n)$ is an "average depth" of the graph, provided we can define such notions (the different branches of the graph haven't all the same length...) Yet, it seems to be difficult to find a bound $\varphi(n)$ for N, *i.e.* for the worst cases instead of the average cases. Such a bound may be very bad (some groups have a maximal subgroup of very high index...)

But we haven't yet undertaken any serious study of complexity. For that, we should also take into account the size of the coefficients of the polynomials that we factorize, which grows with n.

Chapitre 9

Calcul du groupe de Galois par descente diagonale dans le graphe des classes de conjugaisons de sous-groupes

Résumé

This article deals with the direct problem of Galois theory (identify the Galois group of a polynomial). It starts from a classical method: factorization of Lagrange resolvents over the ground field — the factorizing type of which enables to identify the Galois group. The aim of the article is to lower the degrees of the resolvents to factorize over the ground field. For instance, the degrees of the resolvents to factorize in order to identify the Galois group of an irreducible polynomial of degree 10 can be reduced from 420 with the former methods to 45 with that of the article when this Galois group is imprimitive (but the method applies to primitive groups too). This method is based on a new result of invariant theory, that enables to get down diagonally (*i.e.* from an uncle to a nephew) in the graph of subgroups of the symmetric group, whereas the traditional Stauduhar method required to get down directly (*i.e.* from a father to its sons) in this graph.

9.1 Introduction

Let k be a field of characteristic zero, such that there be a factorization algorithm for polynomials over k, and $f = T^n + \sum_{i=1}^{n}(-1)^i e_i T^{n-i} \in k[T]$ a monic polynomial — which does not need to be irreducible — with degree $n \geq 2$. If we note $\mathbf{x} = (x_1, \ldots, x_n)$ the set of its roots in an algebraic closure $\hat{k}$ of k, this numbering of the roots defines a faithful representation $\Gamma \subset \mathfrak{S}_n$ of the Galois group $\mathrm{Gal}_k(f) = \mathrm{Gal}(k(\mathbf{x}) : k)$ of f in the symmetric group $\mathfrak{S}_n$ (where $\mathrm{Gal}(k(\mathbf{x}) : k)$ is by definition the group of k-algebra automorphisms of $k(\mathbf{x})$). The aim of this article is to give a new formal method to compute the conjugacy class $[\Gamma]$ of Γ in $\mathfrak{S}_n$, *i.e.* Γ up to a permutation of the roots. In fact, this new method improves that of [17], which is itself a formal version of Stauduhar's method (see [61] and [17]), and that of [7]. We will call it *diagonal method*, because its principle is to get through the graph of subgroups diagonally, *i.e.* from an uncle to a nephew for instance, and not only from a father to a son (we call a *son* of a group G a maximal subgroup of G, a *father* of G a group of whom G is a son, and a *nephew* of G a subgroup of a father of G). That is why it enables to reduce the degrees of the resolvents that we had to factorize over the ground field k with the method of [17] (see the tables of Section 9.4).

We now remind a few useful definitions (which can be found *e.g.* in [7]).

Definition 9.1 *Let H and L be two subgroups of the symmetric group $\mathfrak{S}_n$, with $H \subset L$, and $\Theta \in k[\mathbf{X}] = k[X_1, \ldots, X_n]$. We say that Θ is a* primitive invariant of H relative to L *if and only if $\mathcal{S}tab_L(\Theta) = H$. Then we call* generic resolvent by Θ relative to L *the polynomial $\mathcal{L}^L_\Theta = \prod_{\tau \in (L/\!\!/H)}(T - \tau.\Theta) \in k[\mathbf{X}]^L[T]$, where $L/\!\!/H$ is a set of left coset representatives of H in L. When $L = \mathfrak{S}_n$, we simply note $\mathcal{L}_\Theta$ instead of $\mathcal{L}^{\mathfrak{S}_n}_\Theta$, and we call it an* absolute resolvent.

Assume $\Gamma \subset L$. Let $k[\mathbf{X}]^L$ be the invariants' algebra of L. Then for every $P \in k[\mathbf{X}]^L$, $P(x_1, \ldots, x_n)$ belongs to k because $k(\mathbf{x})^\Gamma = k$. Hence the polynomial $\mathcal{L}^L_{\Theta,\mathbf{x}}$ defined from $\mathcal{L}^L_\Theta$ by specializing the family $\mathbf{X} = (X_1, \ldots, X_n)$ in $\mathbf{x} = (x_1, \ldots, x_n)$ belongs $k[T]$. We call it *resolvent of f by Θ relative to L*. In fact, it depends not only on f but on the chosen numbering $(x_1, \ldots, x_n)$ of its roots (except if $L = \mathfrak{S}_n$).

The already existing methods that use factorization of resolvents over the ground field: The method grounded on the factorization of several absolute resolvents over the ground field was introduced by McKay and Soicher (see [52]), with results up to degree 8, and then carried on by Arnaudiès and Valibouze (see [7]) who proved that the method is deterministic and that the *factorization types* over k of the resolvents (*i.e.* the list of degrees of their irreducible factors over k) can be associated to a partition depending only of groups (see Theorem 9.5). We can improve this method (see [70]) by looking not only at the factorization types of the resolvents $\mathcal{L}_{\Theta,x}$, but also at the Galois groups of the irreducible factors g of $\mathcal{L}_{\Theta,x}$ when $\deg(g) < n$ or when $\deg(g) = n$ and $\mathrm{Gal}_k(g)$ can be identified easier than $\mathrm{Gal}_k(f)$; and by looking at the parity of $\mathrm{Gal}_k(g)$ when $\deg(g) > n$ (by testing whether $\mathrm{discr}(g)$ is a square). This method — with the improvement using the Galois groups of the factors of the resolvents — shall be called the *absolute formal method* in the rest of this article.

A second method uses resolvents $\mathcal{L}^L_{\Theta,\mathbf{x}}$ with various groups L (not only $\mathfrak{S}_n$) to test inclusions: indeed, if we know that $\Gamma \subset L$, if H is a subgroup of L and if Θ is a primitive invariant of H relative to L such that $\mathcal{L}^L_{\Theta,f}$ be square-free, then Γ is a subgroup of a conjugate of L if and only if $\mathcal{L}^L_{\Theta,f}$ has a root in k (see [61] and [17]). We can then get down the graph of conjugacy classes of subgroups of $\mathfrak{S}_n$ — the order relation between these classes being the inclusion of elements of the classes — until we find $[\Gamma]$ (see [61] or [17]). This method involves either a numerical computation of the resolvents involving approximated values of the roots of f (see [61, 21, 22]) — in which case it is necessary to know precisely in which conjugate of L the group Γ is included — or a formal computation of the resolvents (see [17]) — then we can work simply up to conjugation, we do not need to specify which conjugate of L contains Γ. The method of [17] shall be called *formal Stauduhar method*. We will call *relative formal method* the method that uses, according to the group, either the formal Stauduhar method or the absolute formal method (the one that needs the factorizations of lower degree).

About the numerical methods (based on Stauduhar's algorithm [61]), for which we refer to [21], we just mention that they are implemented up to degree 11 in the system PARI (see [9]) and that they are usually fast, but may yield a false result on tricky examples (if a root is near to an integer for example) — except if we ask them to work with the precision that is theoretically necessary, in which case the computations become too big.

Other methods: First, we must mention Tschebotareff's theorem (1925) on the modular factorization of f giving the cycle type of an element of the Galois group of f (see [63]). Anai, Noro and Yokoyama (1994) give in [3] a method based on the factorization over successive extension fields, to find both the Galois group and the splitting field. Another method by Yokoyama (1996, see [73]) consists in applying modular techniques to Stauduhar's method, where numerical approximation of the roots is replaced by computation in p-adic fields; this method needs not any computation of a resolvent.

Computation of the resolvents with the formal Stauduhar method: The coefficients of the generic resolvent $\mathcal{L}^L_\Theta$, where Θ is a primitive invariant of a subgroup H of L relative to L, belong to $k[\mathbf{X}]^L$. When $L = \mathfrak{S}_n$, these coefficients are symmetric, so that the coefficients of $\mathcal{L}^L_{\Theta,\mathbf{x}}$ are symmetric polynomials in the x_i, hence can be expressed in terms of the e_i (coefficients of f up to the sign) which are known. When L is not equal to $\mathfrak{S}_n$ but contains Γ, we have to find another way to specialize the elements of $k[\mathbf{X}]^L$. The method proposed in [17], to which we refer for the details, consists in writing $k(\mathbf{X})^L = k(\mathbf{X})^M(\Psi)$, where $L \subset M \subset \mathfrak{S}_n$ and Ψ is a primitive invariant of L relative to M. If we know how to specialize the elements of $k(\mathbf{X})^M$ and Ψ, then we can specialize all the elements of $k(\mathbf{X})^L$; so that we can reduce recursively the problem to specializing the elements of $k(\mathbf{X})^{\mathfrak{S}_n}$ (which we can do, thanks to the coefficients of f) and a few primitive elements defined by a chain of inclusion $L \subset M_1 \subset M_2 \subset \ldots \subset \mathfrak{S}_n$. And to specialize these primitive elements, we just need to factorize their resolvent; thus, the specialized value of $\psi = \Psi(x_1, \ldots, x_n)$ of Ψ is a root of $\mathcal{L}^M_{\Psi,\mathbf{x}}$. Of course, everything is done up to conjugation (but it does not matter, since we use primitive elements).

Remark 9.2 *We can instead of primitive elements use a Noether normalization of $k[\mathbf{X}]^L$. Indeed, we can write*

$$k[\mathbf{X}]^L = \bigoplus_{i=1}^{e} k[\Pi_1, \ldots, \Pi_n]\Sigma_i$$

*where $(\Pi_1, \ldots, \Pi_n)$ (*primary invariants*) is a pure transcendence basis of $k(\mathbf{X})^L$ over k, and where $(\Sigma_1, \ldots, \Sigma_e)$ (*secondary invariants*) are linearly independent over $k[\Pi_1, \ldots, \Pi_n]$ (see [40] and chapter 4). We can specialize these fundamental invariants thanks to resolvents, as for the primitive element. The calculations are then smaller, and do not involve fractions, but we must be careful when L contains several conjugates of Γ: then the resolvents used to specialize the fundamental invariants will have several roots. We must then be sure that the choice of the roots taken for the different fundamental invariants are coherent; indeed, the choice of one of the roots for the specialized value of a fundamental invariant implies a numbering of the roots; and the choice of the root for the specialized value of another fundamental invariant must imply the same numbering of the roots of f (we cannot number the roots of f in two different ways at the same time). A way to assure this coherence is to check that the candidates for the specialized values of the fundamental invariants satisfy all the syzygy relations between these invariants: see Théorème 4.14, where we prove that it is a (necessary and) sufficient condition. This problem could not appear with primitive elements, where we could choose any of the roots of the resolvent.*

Remark 9.3 *This article answers a wish of Arnaudiès and Valibouze (see [7, page 26]) to use the tables of partitions with relative resolvents. Indeed, in [7] they state the theorems involving the relative case $L \subset \mathfrak{S}_n$, but they do not give an efficient algorithm to specialize the invariants of L.*

In Section 9.2, we show how the degrees of the factorizations involved in the formal Stauduhar method (see above) can be lowered. Section 9.3 is devoted to an example, whereas Section 9.4 deals with the bounds we get with the *diagonal method* in degrees 8, 9 and 10.

9.2 The theory

In this section we show how the degrees of the factorizations involved in the formal Stauduhar method (see above) can be lowered. Stauduhar method uses only linear factors of the resolvents to test inclusions, and get down directly (from a father to a son) in the graph of subgroups of $\mathfrak{S}_n$. The diagonal method uses the whole factorization of resolvents with Theorem 9.5 (like the absolute method, but also with relative resolvents) to get down in the graph.

The following definition and its use in connection with the absolute formal method are due to Arnaudiès and Valibouze (see [7]).

Definition 9.4 *Let L be a subgroup of the symmetric group $\mathfrak{S}_n$, G and H two subgroups of L and $e = [L : H]$. We consider the left action of G on the set $(L/H)_g = \{l_1.H, \ldots, l_e.H\}$ of left-cosets of H by translations (*i.e. *$g.(l.H) = (gl).H$ for every $g \in G$ and $l.H \in (L/H)_g$). We call* partition associated to (G, H) relative to L *and we note $\varpi^L(G, H)$ the increasing sequence $(e_1, \ldots, e_r)$ such that $e_1, \ldots, e_r$ be the lengths of the orbits in $(L/H)_g$ under the action of G (so that $e_1 + \ldots + e_r = [L : H]$). When $L = \mathfrak{S}_n$, we simply write $\varpi(G, H) = \varpi^{\mathfrak{S}_n}(G, H)$.*

The following theorem is due to Arnaudiès and Valibouze. When $L = \mathfrak{S}_n$, it is the keystone of the absolute formal method.

Theorem 9.5 *Let G and H be to subgroups of $L \subset \mathfrak{S}_n$. Then $\varpi^L(G, H)$ depends only on the conjugacy classes of G and H in L, and if G is in the same conjugacy class as Γ ($[\Gamma] = [G]$) and Θ is a primitive invariant of H relative to L such that $\mathcal{L}^L_{\Theta,\mathbf{x}}$ be square-free, then the factorization type of $\mathcal{L}^L_{\Theta,\mathbf{x}}$ is equal to $\varpi^L(G, H)$ (if $\mathcal{L}^L_{\Theta,\mathbf{x}}$ is not square-free, then its factorization type is a subpartition of $\varpi^L(G, H)$).*

Proof – It stems from [7, Lemme 2 and Théorème 6.10] □

The following lemma proves that L acts identically on $(L/H)_g$ and on the orbit of a primitive invariant of H; hence, it gives an easy way to compute a partition $\varpi(G, H)$.

Lemm 9.6 *Let Θ be a primitive invariant of a subgroup H of L relative to L. Let $L.\Theta = \{l.\Theta \ / \ l \in L\}$ be the orbit of Θ under the action of L. Then, the following application*

$$\xi : \left| \begin{array}{ccc} (L/H)_g & \longrightarrow & L.\Theta \\ l.H & \longmapsto & l.\Theta \end{array} \right.$$

*is well defined, is a bijection from $(L/H)_g$ onto $L.\Theta$ and commutes with the action of L by left translation (*i.e. *$\xi(g.H') = g.\xi(H')$ for every $g \in L$ and $H' \in (L/H)_g$).*

Proof – Exercise □

Theorem 9.7 *Let $H \subset L \subset \mathfrak{S}_n$. Let $G_0 \subset L$ acting by left translation on the set $(L/H)_g = \{l_1.H, \ldots, l_e.H\}$ of left cosets of H in L, $\mathcal{O} = G_0.H = \{g_1.H, \ldots, g_r.H\}$ the orbit of H under G_0 and $G = \mathcal{S}tab_L(\mathcal{O}) \subset L$ the stabilizer of $\mathcal{O}$ in L (then $G \supset G_0$, and $\mathcal{O}$ is also the orbit of H under G). The theorem says that $k(\mathbf{X})^G$ is generated as a field and $k(\mathbf{X})^L$-algebra by the polynomials $g_1.P + \ldots + g_r.P$ where P runs along $k[\mathbf{X}]^H$ (in fact, it is sufficient that P runs along the r first powers $\Theta, \ldots, \Theta^r$ of a primitive invariant Θ of H relative to L).*

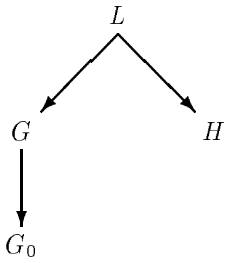
Proof – Let Θ be a primitive invariant of H relative to L (*i.e.* such that $\mathcal{S}tab_L(\Theta) = H$). Since $G = \mathcal{S}tab_L(\{g_1.H, \ldots, g_r.H\})$ we conclude from Lemma 9.6 that $G = \mathcal{S}tab_L(\{g_1.\Theta, \ldots, g_r.\Theta\})$; and hence we also have $\mathcal{S}tab_L(\prod_{i=1}^r (T - g_r.\Theta)) = G$, where T is an indeterminate over $k(\mathbf{X})$. As k is infinite and L is finite, we see that there must exist a $t \in k$ such that $\mathcal{S}tab_L(\prod_{i=1}^r (t - g_r.\Theta)) = G$ (indeed, if we set $\Psi_t = \prod_{i=1}^r (t - g_r.\Theta)$, then each equation $\Psi_t = l.\Psi_t$, with $l \in L$, is either satisfied for every t — when $l \in G$ — either for a finite number of $t \in k$). Now, let $\Xi_k = \sum_{i=1}^r g_i.\Theta^k$ for $k \in \{1, \ldots, r\}$. They are the power sums in $g_1.\Theta, \ldots, g_r.\Theta$. Also, from Newton's formulae, the elementary symmetric polynomials in $g_1.\Theta, \ldots, g_r.\Theta$, and hence the polynomial $\Psi = \prod_{i=1}^r (t - g_r.\Theta)$ which is a linear combination of them, belong to $k[\mathbf{\Xi}] = k[\Xi_1, \ldots, \Xi_r]$. Then, $\mathcal{S}tab_L(\Theta) = H$ entails that $k(\mathbf{X})^G = k(\mathbf{X})^L[\Psi]$ (see Th. 3.1). Therefore, $k(\mathbf{X})^G = k(\mathbf{X})^L[\Xi_1, \ldots, \Xi_r]$ with $\Xi_k = \sum_{i=1}^r g_i \Theta^k$ and $\Theta^k \in k[\mathbf{X}]^H$ for every $k \in \{1, \ldots, r\}$. □

Example: We take $n = 9$, $\Theta = X_1X_2X_3$, $G_0 = T_{26} =< (1,8,4,7,9,2,6,3),(1,3,9,4,5,8)(2,6) >$, and $H = \mathcal{S}tab_{\mathfrak{S}_9}(\Theta) \simeq \mathfrak{S}_3 \times \mathfrak{S}_6$. We compute the orbit $T_{26}.\Theta = \{X_1X_2X_3,\ X_4X_5X_6,\ X_7X_8X_9,\ X_3X_5X_7,\ X_6X_8X_1,\ X_9X_2X_4,\ X_1X_4X_7,\ X_2X_5X_8,\ X_3X_6X_9,\ X_3X_4X_8,\ X_6X_7X_2,\ X_9X_1X_5\}$, and then the stabilizer of this orbit: $G = \mathcal{S}tab_{\mathfrak{S}_9}(T_{26}.\Theta) = T_{26}$ (from Lemma 9.6, we can use the action on polynomials to compute G). So, in this case, $G = G_0$. We define $\Psi = \sum_{\Theta' \in T_{26}.\Theta} \Theta'$. We can verify that it is then a primitive invariant of T_{26} relative to $\mathfrak{S}_9$ (here we are lucky, we do not have to use the powers of Θ like in the theorem; it is often the case).

General principle of the method: We can now explain how the method works. It is recursive.

Recurrence hypothesis: We suppose that we know that a conjugate of Γ (representation of $\mathrm{Gal}_k(f)$ in $\mathfrak{S}_n$) is included in a group L. Up to a renumbering of the roots of f, we can assume that $\Gamma \subset L$. We also suppose that we know how to specialize all the elements of $k[\mathbf{X}]^L$.

At the beginning, $L = \mathfrak{S}_n$ of course: it is then true that we know how to specialize all the elements of $k[\mathbf{X}]^L$. Therefore, the recurrence hypothesis is then satisfied. We want to reproduce this recurrence hypotheses with an other, smaller, group L, called G, in order to find recursively the conjugacy class $[\Gamma]$. We choose a subgroup H of L, a primitive invariant Θ of H relative to L, and we compute a resolvent $\mathcal{L}^L_{\Theta,\mathbf{x}}$. It is possible because the coefficients of $\mathcal{L}^L_\Theta$ belong to $k[\mathbf{X}]^L$, so that by hypothesis we know how to specialize them. We factorize this resolvent, and look at the tables of partitions (given in [69] when $L = \mathfrak{S}_n$, and by a program ([69] and [70, Section 7]) in GAP [58] in the general case) to see what Γ can be (up to conjugacy). Indeed, from [7, Théorème 6.6], the factorizing type of $\mathcal{L}^L_{\Theta,\mathbf{x}}$ is bounded by $\varpi^L(\Gamma, H)$, and equal to it if $\mathcal{L}^L_{\Theta,\mathbf{x}}$ is square-free (for more accurate conclusions, we also can look at the Galois group of the irreducible factors of $\mathcal{L}^L_{\Theta,\mathbf{x}}$ when they are easy to compute). The tables of partitions give then a set of possibilities for Γ, up to conjugacy. Let G_0 be a subgroup of L greater (for the inclusion up to conjugacy) than all these possibilities for Γ. Then, certainly, a conjugate of Γ — let say Γ, up to a new renumbering of the roots by an element of L — is a subgroup of G_0. We then compute the stabilizer G of the orbit $G_0.H = \{g_1.H, \ldots, g_r.H\}$, as in Theorem 9.7. Then $\Gamma \subset G_0 \subset G \subset L$.



Of course if $G = L$, then we have made a bad choice for H (see Remark 9.9), we must try another one. So, we can assume G to be a proper subgroup of L. There remains to be able to specialize the elements of $k[\mathbf{X}]^G$, and then the recurrence hypothesis will be satisfied with G playing the role of L. From Theorem 9.7, it is enough to compute the specialized values of the polynomials $g_1.\Theta^k + \ldots + g_r.\Theta^k$ for $k \in \{1, \ldots, r\}$ (indeed, from the recurrence hypothesis, we know how to specialize the elements of $k(\mathbf{X})^L$; therefore, we will then be able to specialize all the elements of $k(\mathbf{X})^G$). From Newton's formulae, the specialized values of $g_1.\Theta^k + \ldots + g_r.\Theta^k$ for $k \in \{1, \ldots, r\}$ can be deduced from these of the r polynomials $E_1^{(r)}(g_1.\Theta, \ldots, g_r.\Theta) = g_1.\Theta + \ldots + g_r.\Theta$, $\ldots$, $E_r^{(r)}(g_1.\Theta, \ldots, g_r.\Theta) = (g_1.\Theta)\ldots(g_r.\Theta)$ (elementary symmetric polynomials in $g_1.\Theta, \ldots, g_r.\Theta$). Now, these r polynomials are the coefficients — up to the sign — of $\prod_{i=1}^r (T - g_i.\Theta)$, which is a factor of $\mathcal{L}^L_\Theta$. Therefore, after specialization, with get the specialized values of the polynomials $(-1)^i E_i^{(r)}(g_1.\Theta, \ldots, g_r.\Theta)$ for $k \in \{1, \ldots, r\}$. But the specialized value of $\prod_{i=1}^r (T - g_i.\Theta)$ is exactly a (not necessarily irreducible) factor of the resolvent $\mathcal{L}^L_{\Theta,\mathbf{x}}$. Therefore, we get it thanks to the factorized form of $\mathcal{L}^L_{\Theta,\mathbf{x}}$; the only problem is to identify it among the other factors

of this resolvent. If the degree was not enough, we could also use its Galois group when $r < n$ or when it is simple to identify (with a discriminant for instance). Indeed, both the degree and the Galois group of the factor got by specializing $\prod_{i=1}^{r}(T - g_i.\Theta)$ are known from computations on groups only (its degree is already known: it is r, length of the orbit of H under the left translation by G; its Galois group is given by [70, Theorem 4]). But we cannot exclude that on some examples the factor could not be identified thanks to its degree and Galois group. Then we would have to try another group H (we can forecast it, see Remark 9.9).

Remark 9.8 *The algorithm will end because the number of subgroups is finite — but this is not the problem, it was already the case with the formal Stauduhar method. The problem here is efficiency. Indeed, if we take $G_0 = H$ (when $\mathcal{L}^L_{\Theta,\mathbf{x}}$ is square-free and has a root in k, which means from [61] that H contains a conjugate of Γ by an element of L), we have $G = G_0 = H$, and then we are reduced to the formal Stauduhar method. Therefore, the algorithm of this article contains strictly the formal Stauduhar method of [17].*

Remark 9.9 *We can precompute tables of groups G associated to the different possible groups H, for all possible Galois groups Γ. The results in degrees 8, 9 and 10 given in Section 9.4 were obtained from such precomputations, that I did thanks to the tables of [21, Annexe 3]. It allows to choose a good group H,* i.e. *one that will lead to "good" group G (such that $G \neq L$, and that $[L : G]$ be rather small).*

Remark 9.10 *Theorem 9.7 involves fractions ($k(\mathbf{X})^G$ is generated as a field). If we replace it by $k[\mathbf{X}]^G$ and leave unchanged the rest of the theorem, it becomes false. Indeed, the following counterexample was found by Yves Eichenlaub, whom I would like to thank here for it: $n = 8$, $H = T_{48}$, $G = G_0 = T_{44}$. Nonetheless, in all the examples I needed in the frame of the diagonal method, $k[\mathbf{X}]^G$ was generated by polynomials $g_1.P + \ldots + g_r.P$ with $P \in k[\mathbf{X}]^H$. In Section 9.3, we illustrate this fact by generating $k[\mathbf{X}]^G$ (without fractions) instead of $k(\mathbf{X})^G$*

9.3 Example: odd imprimitive transitive degree 8

In this paragraph, we explain how we can improve the formal Stauduhar method on the example of the odd imprimitive transitive degree 8, by applying the general method described in Section 9.2. So, we assume f to be an irreducible polynomial of degree $n = 8$ (therefore, Γ is a transitive subgroup of $\mathfrak{S}_8$). Let H be the usual representation of $\mathfrak{S}_2 \times \mathfrak{S}_6$ in $\mathfrak{S}_8$ and Θ be a primitive invariant of H (for instance $\Theta = X_1X_2$) such that the resolvent $\mathcal{L}_{\Theta,\mathbf{x}}$ be square-free (such a Θ always exists from [7, Théorème 4.5] or [17, Proposition 9]). We also compute the discriminant $\mathrm{discr}(f)$ of f. We can see from the tables given in [69] or [21, Annexe 3] that Γ is a primitive subgroup of $\mathfrak{S}_8$ if and only if $\mathcal{L}_{\Theta,\mathbf{x}}$ is irreducible.

Let us suppose that Γ is odd and imprimitive, *i.e.* that $\mathcal{L}_{\Theta,\mathbf{x}}$ is reducible and $\mathrm{discr}(f)$ is not a square in k. Then, if we try to apply the absolute formal method (see Section 9.1) with polynomials of degree bounded by 28, we see from the tables given in [21, Annexe 3] or [70] that $[\Gamma]$ can be identified except for the 3 following sets, where we use the names of the groups given in [14]:

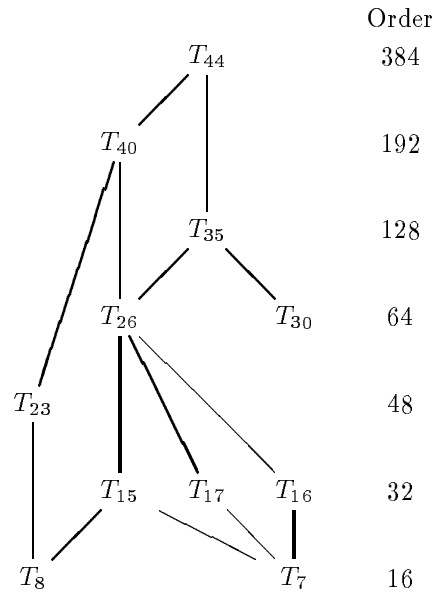
$$\{T_{44}, T_{40}, T_{23}\},\ \{T_{35}, T_{30}, T_{26}, T_{17}, T_{15}, T_8\} \text{ and } \{T_{16}, T_7\}.$$

(the only polynomials to factorize are $\mathcal{L}_{\Theta,\mathbf{x}}$, of degree 28, the same resolvent with f replaced by an irreducible factor of degree 8 of $\mathcal{L}_{\Theta,\mathbf{x}}$, and a few resolvents of degrees 2 or 3 needed to identify the Galois groups of irreducible factors of degree 4)

More precisely, the absolute formal method with resolvents of degrees at most 28 enables to guess to which of these 3 sets Γ belongs (and if it belongs to none of them then we can identify it), but we cannot identify it among one of the 3 sets.

With the absolute formal method, we would need to factorize resolvents of degree up to 56 if we wanted to identify $[\Gamma]$ among one of these sets.

Here is the inclusion diagram (up to conjugacy) of the groups of these 3 sets; it is reproduced from the complete diagram given in [21, Annexe 1]. An arrow $T_i \longrightarrow T_j$ means that T_j is a maximal subgroup of a conjugate of T_i (it is an order relation between the conjugacy classes of subgroups). The thick arrows mark the 3 problematic sets.



Let us suppose for instance that the factorization type of $\mathcal{L}_{\Theta,\mathbf{x}}$ is $(4, 24)$, and that the discriminant of the factor of degree 4 is not a square in k. Then, from the tables given in [70] or [21, Annexe 3], we know that a conjugate of Γ belongs to the set $\{T_{23}, T_{40}, T_{44}\}$. So, Γ is included in a conjugate L of T_{44}. From the graph above, we have to test if a conjugate of T_{44} is included in T_{40}, *i.e.* to factorize a resolvent $\mathcal{L}^L_{\Theta_{T_{40}},\mathbf{x}}$, where $\Theta_{T_{40}}$ is a primitive invariant relative to L of a conjugate H of T_{40} such that $H \subset L$. The coefficients of $\mathcal{L}^L_{\Theta_{T_{40}},\mathbf{x}}$ belong to $k[\mathbf{X}]^L$. We notice that T_{40}, and hence its conjugate L, is a maximal subgroup of $\mathfrak{S}_8$. Therefore, to specialize an element $P \in k[\mathbf{X}]^L$ — for instance a primitive element —, we have to factorize the resolvent $\mathcal{L}_{P,\mathbf{x}}$, whose degree is $[\mathfrak{S}_8 : L] = 105$. It is very bad, because the absolute formal method enables to identify the Galois group by factorizing polynomials of degrees at most 56 only! so on this example the absolute formal method would be better than the formal Stauduhar one.

Let us now explain how the new diagonal method applies here. We take $L = \mathfrak{S}_8$ and $H = \mathfrak{S}_2 \times \mathfrak{S}_6$. As Γ is a subgroup of a conjugate of T_{44}, we can take $G_0 = T_{44}$. Then, the orbit of H under G_0 in $(L/H)_g$ is $\{g_1.H, g_2.H, g_3.H, g_4.H\}$ where $g_1 = Id$, $g_2 = (1,3)(2,4)$, $g_3 = (1,5)(2,6)$ and $g_4 = (1,7)(2,8)$.

The algorithm of [40], implemented into maple by Kemper, yields:

$$k[\mathbf{X}]^{T_{44}} = \bigoplus_{i=1}^{18} k[\Pi_1, \ldots, \Pi_8]\Sigma_i \tag{9.1}$$

(the direct sum is over $k[\Pi_1, \ldots, \Pi_8]$), where: $\Pi_1 = S_1$, $\Pi_2 = S_2$, $\Pi_3 = X_1X_2 + X_3X_4 + X_5X_6 + X_7X_8$, $\Pi_4 = S_3$, $\Pi_5 = X_1^2X_2 + X_1X_2^2 + X_3^2X_4 + X_3X_4^2 + X_5^2X_6 + X_5X_6^2 + X_7^2X_8 + X_7X_8^2$, $\Pi_6 = S_4$, $\Pi_7 = S_6$, $\Pi_8 = S_8$, $\Sigma_1 = 1$, $\Sigma_2 = X_1^3X_2 + X_1X_2^3 + X_3^3X_4 + X_3X_4^3 + X_5^3X_6 + X_5X_6^3 + X_7^3X_8 + X_7X_8^3$, $\Sigma_3 = X_1^2X_2^2 + X_3^2X_4^2 + X_5^2X_6^2 + X_7^2X_8^2$, $\Sigma_4 = S_5$, $\Sigma_5 = X_1^4X_2 + X_1X_2^4 + X_3^4X_4 + X_3X_4^4 + X_5^4X_6 + X_5X_6^4 + X_7^4X_8 + X_7X_8^4$, $\Sigma_6 = X_1^5X_2 + X_1X_2^5 + X_3^5X_4 + X_3X_4^5 + X_5^5X_6 + X_5X_6^5 + X_7^5X_8 + X_7X_8^5$, $\Sigma_7 = S_7$, $\Sigma_8 = \Sigma_2^2$, $\Sigma_9 = \Sigma_2\Sigma_3$, $\Sigma_{10} = \Sigma_2\Sigma_4$, $\Sigma_{11} = \Sigma_2\Sigma_5$, $\Sigma_{12} = \Sigma_2\Sigma_6$, $\Sigma_{13} = \Sigma_2\Sigma_7$, $\Sigma_{14} = \Sigma_4\Sigma_7$, $\Sigma_{15} = \Sigma_5\Sigma_7$, $\Sigma_{16} = \Sigma_6\Sigma_7$, $\Sigma_{17} = \Sigma_2^2\Sigma_4$, $\Sigma_{18} = \Sigma_2\Sigma_6\Sigma_7$ and where $S_k = \sum_{i=1}^8 X_i^k$ (power sums).

Amongst these primary invariants Π_i and secondaries Σ_i, some are symmetric, and some are expressed in terms of others; so that the only ones whose specialization is not obvious are Π_3, Π_5, Σ_2, Σ_3, Σ_5, Σ_6. But there holds: $\Pi_3 = \mathcal{P}(X_1X_2)$, $\Pi_5 = \mathcal{P}(X_1X_2(X_1+X_2))$, $\Sigma_2 = \mathcal{P}(X_1X_2(X_1^2+X_2^2))$, $\Sigma_3 = \mathcal{P}(X_1^2X_2^2)$, $\Sigma_5 = \mathcal{P}(X_1X_2(X_1^3+X_2^3))$, $\Sigma_6 = \mathcal{P}(X_1X_2(X_1^4+X_2^4))$ where

$$\mathcal{P} : \left| \begin{array}{lll} k[\mathbf{X}]^{\mathfrak{S}_2\times\mathfrak{S}_6} & \longrightarrow & k[\mathbf{X}]^{T_{44}} \\ P & \longmapsto & \mathcal{P}(P) = g_1.P + g_2.P + g_3.P + g_4.P \end{array} \right.$$

Now, by looking at the tables of partitions given in [69] or [21], we see that the factorization type of $\mathcal{L}_{\Theta,\mathbf{x}}$ is either $(4,24)$ (when a conjugate of Γ belongs to the first set $\{T_{44}, T_{40}, T_{23}\}$), either $(4,8,16)$ (when it belongs to one of the 2 other problematic sets). Therefore, $\mathcal{L}_{\Theta,\mathbf{x}}$ has always a single factor of degree 4. Therefore, if we compute the factor of degree 4 of $\mathcal{L}_{\Theta,\mathbf{x}}$, let it be $T^4 + aT^3 + bT^2 + cT + d$, then $-a$ is the specialized value of $\mathcal{P}(\Theta)$. Also, by applying this successively to $\Theta = X_1X_2, X_1X_2(X_1 + X_2), X_1^2X_2^2, X_1X_2(X_1^2+X_2^2), X_1X_2(X_1^3+X_2^3)$ and $X_1X_2(X_1^4+X_2^4)$, we get the specialized values of respectively Π_3, Π_5, Σ_2, Σ_3, Σ_5 and Σ_6. So, it results from 9.1 that we can now specialize all the elements of $k[\mathbf{X}]^{T_{44}}$ (indeed, the decomposition (9.1) is algorithmic, and implemented in the package Invar of Maple [2] and in MAGMA [1]. Therefore, we can now compute the resolvents of invariants of T_{35} and T_{40} relative to T_{44} (their generic coefficients belong to $k[\mathbf{X}]^{T_{44}}$), and thus go on with the classical formal Stauduhar method in the graph of subgroups. All the resolvents to factorize will be of degrees 2, 3 or 4. In fact, in all cases, the following resolvents are enough: $\mathcal{L}^{T_{44}}_{\Theta_{40},\mathbf{x}}$, $\mathcal{L}^{T_{44}}_{\Theta_{35},\mathbf{x}}$, $\mathcal{L}^{T_{40}}_{\Theta_{23},\mathbf{x}}$, $\mathcal{L}^{T_{35}}_{\Theta_{30},\mathbf{x}}$, $\mathcal{L}^{T_{35}}_{\Theta_{26},\mathbf{x}}$, $\mathcal{L}^{T_{26}}_{\Theta_{17},\mathbf{x}}$, $\mathcal{L}^{T_{26}}_{\Theta_{15},\mathbf{x}}$, where each Θ_i is a primitive invariant of T_i (relative to the group in exponent).

Therefore, we have proved here that **when the Galois group of an irreducible polynomial of degree 8 is odd and imprimitive, it can be identified thanks to symbolic computation and factorizations of resolvents of degrees at most 28**.

9.4 Results in degrees 8, 9 and 10

In this section, we give the bounds on the degrees of the factorizations needed to identify the Galois groups of irreducible polynomials of degrees 8 to 10 with the diagonal method, and we compare them with those needed with the absolute formal method and with the relative formal method (see the definitions of these methods in Section 9.1). We do not treat the case of intransitive groups, which involves factorizations of lower degrees (see [65]) but a large number of possible groups. The names (T_i) given to the conjugacy classes of transitive subgroups of $\mathfrak{S}_n$ are those of [14].

We begin with the results, and we then explain, in subsections 9.4.1, 9.4.2 and 9.4.3, how we got them.

Degree 8:

	Primitive		Imprimitive	
	Odd	Even	Odd	Even
Absolute	30	30	35	56
Relative	30	15	35	56
Diagonal	30	15	28	28

Degree 9:

	Primitive		Imprimitive	
	Odd	Even	Odd	Even
Absolute	126	280	168	168
Relative	126	126	168	168
Diagonal	84	120	36	36

Degree 10:

	Primitive		Imprimitive	
	Odd	Even	Odd	Even
Absolute	126	126	420	420
Relative	126	126	420	126
Diagonal	126	126	45	45

In the line "Absolute" are the maximal degrees of the polynomials we have to factorize (or at least of which we have to find a root) using the absolute formal method (including the use of the Galois groups of the factors, see Section 9.1).

In the line "Relative", are the maximal degrees with the relative formal method (*i.e.* union of the absolute method and Stauduhar's method, see Section 9.1).

In the line "Diagonal", are the maximal degrees with the method of this article, using relative Lagrange resolvents and diagonal inclusion, without using the Galois groups of the factors (we do not need them, using them would not decrease any degree of a factorization).

Of course, the degrees written in the tables include the tests to decide whether the group is primitive or imprimitive (that is to say, we are not supposed to know *a priori* whether the group is primitive or not). Yet, there exists methods to exhibit imprimitivity (see [15, 36, 42]).

9.4.1 Degree 8

We already treated the odd imprimitive case in Section 9.3. The even imprimitive case is works similarly: indeed, with factorizations of degrees up to 28, we can identify all the Galois groups but these of the 4 following sets:

$$\{T_{45}, T_{45}, T_{41}, T_{34}, T_{33}\}, \{T_{22}, T_{11}\}, \{T_{24}, T_{14}\} \text{ and } \{T_{32}, T_{12}\}.$$

For all these groups, we can choose for H the usual representation of $\mathfrak{S}_2 \times \mathfrak{S}_6$ in $\mathfrak{S}_8$. For G, we can take T_{45} for the first of these sets, and T_{39} for the 3 last ones. From Lemma 9.6, we can compute the orbits on primitive invariants, instead of left cosets. The orbit of the primitive invariant X_1X_2 of H is then $T_{39}.X_1X_2 = \{X_1X_2, X_3X_4, X_5X_6, X_7X_8\}$ under T_{39}, and corresponds to the irreducible factor of degree 4 of the resolvent (there is only one from the tables); and $T_{45}.X_1X_2 = \{X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_2X_4, X_3X_4, X_5X_6, X_5X_7, X_5X_8, X_6X_7, X_6X_8, X_7X_8\}$, and corresponds to the irreducible factor of degree 12 of the resolvent (there is only one). In these cases, there is an improvement of the formal Stauduhar method, which was rather efficient here for the subgroups of T_{45} because $[T_{49} : T_{45}] = 35$, which is better than 56 (the degree needed with the absolute formal method), but not efficient at all for the subgroups of T_{45} which are not subgroups of T_{39} (indeed, T_{45} is a maximal subgroup of $T_{49} \simeq \mathfrak{A}_8$ of index 105, which is worse than the degree (56) needed with the absolute formal method.

As for the primitive case, the diagonal method does not improve the degrees: we need a resolvent of degree 30 (associated to a primitive invariant of T_{48}) to separate T_{43} from T_{50}, and for all the other ones, the formal Stauduhar methods works with resolvents of degrees at most 15.

9.4.2 Degree 9

In degree 9, the resolvent of a primitive invariant of $\mathfrak{S}_2 \times \mathfrak{S}_7$ (for example $\mathcal{L}_{X_1+X_2,\mathbf{x}}$) enables to know whether the group is primitive or not: it is primitive if and only if the factorizing type of this resolvent is either (36) or $(18,18)$ (when it is square-free).

When Γ is primitive: we set $L = \mathfrak{S}_8$ and H equal to the usual representation of $\mathfrak{S}_3 \times \mathfrak{S}_6$ in $\mathfrak{S}_8$. We compute a resolvent (of degree $[\mathfrak{S}_8 : H] = 84$) of a primitive invariant of H, for instance $\mathcal{L}_{X_1X_2X_3,\mathbf{x}}$. We see from the tables that this resolvent splits if and only if T_{26} contains a conjugate of Γ. In this case, it has a single factor of degree 12 (not necessarily irreducible), which enables to specialize all the elements of $k[\mathbf{X}]^{T_{26}}$ (the orbit of H under the action of T_{26} is given in the example following Theorem 9.7). And we can then go on with a formal Stauduhar method amidst the sons of T_{26}, involving resolvents of degrees 2 or 3. The improvement of the diagonal method is obvious here, because as T_{26} is a maximal subgroup of $T_{34} \simeq \mathfrak{S}_9$ of index 840, we would have with Stauduhar's method to begin with the factorization of a resolvent of degree 840.

When T_{26} does not contain a conjugate of Γ (*i.e.* when the resolvent $\mathcal{L}_{X_1X_2X_3,\mathbf{x}}$ is irreducible), the diagonal method allows no improvement, we have to use the formal Stauduhar method with a factorization of degree 120 to separate $T32$ from T_{33}.

When Γ is imprimitive: then, up to conjugation, it is included in $H = T_{31}$. But as T_{31} is a maximal subgroup of index 280 of $\mathfrak{S}_9$, Stauduhar's method requires a factorization of this degree. With the diagonal method, we can take $H = \mathfrak{S}_2 \times \mathfrak{S}_7$. The orbit of $\Theta = X_1X_2$ (primitive invariant of H) under T_{31} is $T_{31}.\Theta = \{X_1X_2, X_1X_3, X_2X_3, X_4X_5, X_4X_6, X_5X_6, X_7X_8, X_7X_9, X_8X_9\}$, whose stabilizer in T_{31} is $G = T_{31}$. Therefore, a factor of degree 9 of $\mathcal{L}_{\Theta,\mathbf{x}}$ enables to specialize all the elements of $k[\mathbf{X}]^{T_{31}}$. The degree of this resolvent is 36, and we can finish with a formal Stauduhar method starting from T_{31}, involving resolvents of degrees 2, 3 and 4.

9.4.3 Degree 10

In degree 10, the principle is the same. Let Θ be a primitive invariant of invariant of $\mathfrak{S}_2 \times \mathfrak{S}_8$ (for instance $\Theta = X_1 + X_2$). Then, Γ is primitive if and only if the factorization type of $\mathcal{L}_{\Theta,\mathbf{x}}$ (supposed square-free) is either (45) or $(30,15)$.

In the primitive case: no improvement is entailed by the diagonal method; indeed, we can identify all the groups with 2 absolute resolvents, of degrees 45 and 126 (associated to $\mathfrak{S}_2 \times \mathfrak{S}_8$ and to T_{43}); as the index of T_{35} in $\mathfrak{S}_{10}$ is 2520, the relative method doesn't improve anything, and we notice that the diagonal method doesn't either.

Whereas in the imprimitive case: Γ is, up to conjugation, included either in T_{43} or in T_{39}, which are maximal subgroups of $\mathfrak{S}_8$ of respective indexes 126 and 945. Therefore, Stauduhar's method is not so good (subgroups of T_{43}) or prohibited (the others); whereas the diagonal method enables to specialize the elements of $k[\mathbf{X}]^G$, thanks to a factor of degree 5 of $\mathcal{L}_{\Theta,\mathbf{x}}$ (case $G = T_{39}$) or of degree 20 (case $G = T_{43}$). Therefore, factorizations of degree at most 45 (the degree of $\mathcal{L}_{\Theta,\mathbf{x}}$) are enough in the imprimitive case. With the absolute method, we had to factorize a resolvent of degree at least 420 (for example, we could identify all the groups with absolute resolvents associated to $\mathfrak{S}_2 \times \mathfrak{S}_8$, $(\mathfrak{S}_2 \times \mathfrak{S}_8) \cap \mathfrak{A}_{10}$, $\mathfrak{S}_5^2$, T_{41}, $\mathfrak{S}_4 \times \mathfrak{A}_6$,

$\mathfrak{S}_6 \times \mathfrak{A}_4$, whose indexes are respectively 45, 90, 252, 252, 420 and 420) as we can see from the tables given in [21], so 420 was the best.

9.4.4 Higher degrees

From the examples of degrees 8 to 10, we can induce that in the case of an imprimitive group G, the improvement given by the diagonal method is usually good. The reason for this fact is that in Theorem 9.7, we can then choose for Θ an invariant depending only on the variables belonging to a block of imprimitivity of G. Therefore, in the imprimitive case, the method will generalize to higher degrees. But with primitive groups, it is more difficult to guess. We showed that in degree 9 there is an improvement for primitive groups too; but in degrees 10 and 11, it is not the case.

Troisième partie

Systèmes d'équations algébriques présentant des symétries

Chapitre 10

Résolution d'un système d'équations algébriques présentant des symétries

Résumé

We propose a method to solve some polynomial systems whose equations are invariant by the action of a finite matrix multiplicative group G. It consists in expressing the polynomial equations in terms of some *primary invariants* Π_1, ..., Π_n (*e.g.* the elementary symmetric polynomials), and either one single "primitive" invariant, or a familly of *secondary invariants*. The primary invariants are a transcendence basis of the algebra of the invariants of the group G over the ground field k, and the powers of the primitive invariant, or the secondary invariants, give a basis of the algebra of invariants considered as a module over over $k[\mathbf{\Pi}]$ or $k(\mathbf{\Pi})$. The solutions of the system are given as roots of polynomials whose coefficients themselves are given as roots of some other polynomials: the representation of the solutions $(x_1, \ldots, x_n)$ breaks the field extension $k(x_1, \ldots, x_n) : k$ in two parts (or more).

10.1 Introduction

Let $(\mathcal{F})$ be a system of p polynomial equations $F_i(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ where k is a commutative field. Solving $(\mathcal{F})$ can mean many different things. For the numericians it means to find approximated values of the isolated points of the variety defined by $(\mathcal{F})$. Our point of view is computer algebra and we shall not here deal with the numericians' point of view; we just quote [71], where is shown how the symmetries can be taken into account in the numerical methods using homotopies.

In computer algebra, by solving $(\mathcal{F})$, it is usually meant to find a "convenient" system of generators of the ideal $\mathcal{I} = (F_1, \ldots, F_p)$, or of any ideal that has the same radical as $\mathcal{I}$ (and hence defines the same sub-variety of $\hat{k}^n$, where $\hat{k}$ is an algebraic closure of k). By a "convenient" system of generators, it is usually understood a triangular system with degrees as low as possible. The standard basis (see [20, chap. 2]) are such systems, but they break the symmetries of the system. Yet, Karin Gatermann is working on decreasing the complexity of standard basis by using the symmetries (see [24] and [25]).

Here, we shall not try to give generators of the ideal $\mathcal{I}$. We shall try to express the points of the variety defined by $\mathcal{I}$ in k^n in successive steps, by introducing some intermediate field extensions between k and the extension of k generated by the coordinates of the solutions of $(\mathcal{F})$.

For this, we shall use the symmetries of $(\mathcal{F})$ and express the polynomials F_i of our system $(\mathcal{F})$ as algebraic elements over a transcendental extension of k. The way we express the F_i in terms of other polynomials using the symmetries of $(\mathcal{F})$ can be seen as an application of a more general problem: how to express the invariants of a group in terms of a small number of them, in fact thanks to a primitive element.

This idea was developed in [17], where it was used to compute relative resolvents, in computational Galois theory.

Invariant theory is what we begin with, in § 10.3. In § 10.4 and § 10.5, we apply invariant theory to solve algebraic systems with symmetries: in § 10.4 we use the field theory point of view of §10.3.2, whereas in § 10.5, we use the Cohen-Macaulay algebra point of view of § 10.3.1.

Then in § 10.7, we compute a few examples using different variants of the method.

10.2 Preliminaries

10.2.1 A few Definitions

Let k be a commutative field. Let $n \in \mathbb{N}^*$ be a positive integer, $X_1, \ldots, X_n$ some indeterminates on k, and $\mathbf{X} = (X_1, \ldots, X_n)$.

The general linear group $\mathbf{GL}_n(k)$ acts faithfully on the left on $k[\mathbf{X}]$ (and $k(\mathbf{X})$) as follows: if $A = (a_{i,j})_{i,j \in \mathbb{N}_n^*} \in \mathbf{GL}_n(k)$ and $P \in k[\mathbf{X}]$ (or $P \in k(\mathbf{X})$) are given, we define $A.P(\mathbf{X}) = P(a_{1,1}X_1 + \ldots + a_{1,n}X_n, \ldots, a_{n,1}X_1 + \ldots + a_{n,n}X_n)$. We denote by $\mathcal{S}tab_L(P)$ the stabilizer of an element P in a subgroup L of $\mathbf{GL}_n(k)$, and by $L.P$ the L-orbit of P.
In particular, the symmetric group $\mathfrak{S}_n$ can be identified to a subgroup of $\mathbf{GL}_n(k)$ by associating the matrix $A_\tau = (\delta_{i,\tau(j)})_{(i,j) \in (\mathbb{N}_n^*)^2}$ (where δ is Kronecker's symbol) to a permutation $\tau \in \mathfrak{S}_n$. By the induced action, $\mathfrak{S}_n$ acts on $k[\mathbf{X}]$ and on $k(\mathbf{X})$ with $\tau.X_i = X_{\tau(i)}, i \in \mathbb{N}_n^* = \{1, \ldots, n\}, \tau \in \mathfrak{S}_n$.

Definition 10.1 *Let G be a subgroup of $\mathbf{GL}_n(k)$. We say that a polynomial $P \in k[\mathbf{X}]$ (resp. a fraction $P \in k(\mathbf{X})$) is* an invariant of G *if and only if for all $A \in G$, we have $A.P = P$. We denote by $k[\mathbf{X}]^G$ (resp. $k(\mathbf{X})^G$) the algebra of polynomial (resp. fractional) invariants of G.*
If L is another subgroup of $\mathbf{GL}_n(k)$ such that $G \subset L$, P is called a primitive invariant of G relative to L *if and only if $\mathcal{S}tab_L(P) = G$ (see Th. 3.1 for the explanation of this terminology).*

10.2.2 What is a System with Symmetries?

Let $\hat{k}$ be an algebraic closure of k. Let us consider a system of p, $p \in \mathbb{N}^*$, polynomial equations

$$(\mathcal{F}): \qquad \forall i \in \mathbb{N}_p^*, \qquad F_i(X_1, \ldots, X_n) = 0$$

with $F_i \in k[\mathbf{X}]$, for all $i \in \mathbb{N}_p^*$. Let us define the ideal $\mathcal{I}(\mathcal{F}) = (F_1, \ldots, F_p)$ of $k[\mathbf{X}]$, its radical $\mathcal{J}(\mathcal{F})$, the ideal $\hat{\mathcal{I}}(\mathcal{F}) = \hat{k} \otimes_k \mathcal{I}(\mathcal{F})$ of $\hat{k}[\mathbf{X}]$ generated by the polynomials $1 \otimes_k F_i$, and the manifold $\mathcal{V}(\mathcal{F})$ defined in $\hat{k}^n$ by $\hat{\mathcal{I}}(\mathcal{F})$.

Definition 10.2 *We define the following subgroups of $\mathbf{GL}_n(k)$:*

- *The* symmetry group *of the system:* $G_{(\mathcal{F})} = \bigcap_{i=1}^p \mathcal{S}tab_{\mathbf{GL}_{n(k)}}(F_i)$
- *The* vector space symmetry group *of $(\mathcal{F})$ as the group associated to the vector space $\mathcal{L}(\mathcal{F}) = \bigoplus_{i=1}^n k.F_i$:* $G_{\mathcal{L}(\mathcal{F})} = \mathcal{S}tab_{\mathbf{GL}_{n(k)}}(\mathcal{L}(\mathcal{F}))$
- *The* ideal symmetry group *of $(\mathcal{F})$ as the group associated to the ideal $\mathcal{I}(\mathcal{F})$:*
  $G_{\mathcal{I}(\mathcal{F})} = \mathcal{S}tab_{\mathbf{GL}_{n(k)}}(\mathcal{I}(\mathcal{F})) = \{A \in \mathbf{GL}_n(k) \ / \ \forall P \in \mathcal{I}(\mathcal{F}), A.P \in \mathcal{I}(\mathcal{F})\}$
- *The* manifold symmetry group $G_{\mathcal{V}(\mathcal{F})}$ *of $(\mathcal{F})$ as the group associated to the radical ideal $\mathcal{J}(\mathcal{F})$ of $\mathcal{I}(\mathcal{F})$:* $G_{\mathcal{V}(\mathcal{F})} = \mathcal{S}tab_{\mathbf{GL}_{n(k)}}(\mathcal{J}(\mathcal{F}))$.

For each of the different groups G above, we can define the associated permutation group as $\mathfrak{S}_n \bigcap G$. The following obviously holds:

$$G_{(\mathcal{F})} \subset G_{\mathcal{L}(\mathcal{F})} \subset G_{\mathcal{I}(\mathcal{F})} \subset G_{\mathcal{V}(\mathcal{F})} \ .$$

Instead of solving $(\mathcal{F})$, we could solve any system $(\mathcal{F}')$ such that $\mathcal{V}(\mathcal{F}') = \mathcal{V}(\mathcal{F})$ (or $\mathcal{I}(\mathcal{F}) = \mathcal{I}(\mathcal{F}')$ if we pay attention to the multiplicities). And we may choose $(\mathcal{F}')$ such that $G_{(\mathcal{F}')}$ be bigger than $G_{(\mathcal{F})}$ (the more symmetries we have is the best: see Th. 3.1). The best we could hope would be $G_{(\mathcal{F}')} = G_{\mathcal{V}(\mathcal{F})}$.

We shall not deal here with the problem of finding such a system $(\mathcal{F}')$. We just mention the notion of *equivariant*, more general than that of invariants (see [25] or [72]); equivariants can take into account some group action on the image space k^n. **In all the following**, the system $(\mathcal{F})$ is given; and as symmetries, we shall consider the only permutations belonging to a fixed finite subgroup G of $G_{(\mathcal{F})}$.

10.3 Description of the invariants of a group

Here we describe the algebra of the invariants of the finite group G that leaves invariant the equations of $(\mathcal{F})$, *i.e.* we study how to express these invariants in terms of a small number of them.

10.3.1 The Cohen-Macaulay algebra point of view

We refer to chapter 4, where this point of view was already studied, and we assume $caract(k) = 0$. **In all this chapter,** we shall bound ourselves to the case when the ring $k[\Pi_1, \ldots, \Pi_n]$ generated by the primary invariants of the finite group $G \subset \mathbf{GL}_n(k)$ is the invariant ring $k[\mathbf{X}]^L$ of a finite reflexion group $L \supset G$. Therefore, we have:

$$k[\mathbf{X}]^G = \bigoplus_{i=1}^{e} k[\mathbf{\Pi}]\Sigma_i \qquad \text{(direct sum over} k[\mathbf{\Pi}]) \qquad \text{and} \qquad k[\mathbf{\Pi}] = k[\mathbf{X}]^L, \qquad e = [L : G].$$

Therefore, we can use the algorithm of Prop. 4.11, as well as Theorem 4.12 and Theorem 4.14.

This point of view gives a very accurate description of polynomial invariants. It is in some way similar to the description of fractional invariants in Th. 3.1. But it involves usually more fundamental invariants than the description of Th. 3.1 does, except for groups of index 2.

Remark 10.3 *Yet, there are some other exceptions. For instance,*

$$k[\mathbf{X}]^{\mathfrak{D}_4} = k[\mathbf{E}] \ \oplus \ k[\mathbf{E}]\Theta \ \oplus \ k[\mathbf{E}]\Theta^2 \qquad \textit{(direct sum over } k[\mathbf{E}]\textit{)}$$

where $\Theta = X_1X_2 + X_3X_4$, $\mathfrak{D}_4 = \mathcal{S}tab_{\mathfrak{S}_4}(\Theta)$ *is the dihedral group, and* $\mathbf{E}$ *is the familly of elementary symmetric polynomials.*

On this example, we have the advantages of a single primitive element, as in § 3.1, without the inconvenients (we have no denominators). But it happens very seldom.

10.3.2 The Field theory point of view

Here, k is a commutative field (no hypothesis on its characteristic). We refer to chapter 3, where this point of view was developped. **In all this chapter,** we shall bound ourselves to the case when L satisfies Noether's problem. We then have $G \subset L \subset \mathbf{GL}_n(k)$ (finite subgroups), Θ an L-relative primitive G-invariant and $\Pi_1, \ldots, \Pi_n \in k[\mathbf{X}]^L$ such that

$$k(\mathbf{X})^G = \bigoplus_{i=1}^{e} k(\mathbf{\Pi})\Theta^i \qquad \text{(direct sum over } k(\mathbf{\Pi})) \qquad \text{and} \qquad k(\mathbf{\Pi}) = k(\mathbf{X})^L, \qquad e = [L : G].$$

Besides, we refer to the algorithms of chapter 3 to express an invariant of G in terms of the Π_i and Θ.

Iterating the Th. 3.1 and Prop. 3.10, we get the following propositions that we will need later (see § 10.7.5):

Proposition 10.4 *Let $(L = G_0, \ldots, G_r = G)$ be a family of finite subgroups of $\mathbf{GL}_n(k)$ such that $L = G_0 \supset G_1 \supset \ldots \supset G_r = G$, and for all $i \in \mathbb{N}_r^*$, Θ_i an invariant of G_i relative to G_{i-1}. Then we have $k(\mathbf{X})^L[\Theta_1, \ldots, \Theta_r] = k(\mathbf{X})^G$; and if we let $e_i = [G_{i-1} : G_i]$, then $(\prod_{j=1}^r \Theta_j^{i_j})_{1 \le i_j \le e_j, \forall j \in \mathbb{N}_r^*}$ is a basis of $k(\mathbf{X})^G$ as a vector space over $k(\mathbf{X})^L$. Its dimension is $e = [L : G] = \prod_{j=1}^r e_j$.*

Proposition 10.5 *With the hypothesis of Prop. 10.4, we have an algorithm, based on linear algebra, to compute the coordinates of an $F \in k(\mathbf{X})^G$ in the $k(\mathbf{X})^L$-basis $(\prod_{j=1}^r \Theta_j^{i_j})_{1 \le i_j \le e_j, \forall j \in \mathbb{N}_r^*}$.*

Proof – We iterate r times the algorithm of Prop. 3.10. More accurately, at the level r, if we look for the decomposition $F = \sum_{j=0}^{e_r-1} A_j \Theta_r^j$ of an $F \in k(\mathbf{X})^G$, with $A_j \in k(\mathbf{X})^L[\Theta_1, \ldots, \Theta_{r-1}]$, we just need to write the linear system:

$$\forall i \in \mathbb{N}_{e_r-1}, \qquad < F, \Theta_r^i >_r = \sum_{j=0}^{e_r-1} A_j < \Theta_r^j, \Theta_r^i >_r$$

where $< ., . >_r$ denotes the function bilinear symmetric $k(\mathbf{X})^{G_{r-1}}$-form on $k(\mathbf{X})^{G_r}$ defined in Prop. 3.5, *i.e.* $< P, Q >_r = \mathrm{Tr}_r(PQ)$ where Tr_r is the trace function associated to the field extension $k(\mathbf{X})^{G_r} : k(\mathbf{X})^{G_{r-1}}$ and before solving this system, to use the algorithm at level $r-1$ to express its coefficients $< \Theta_r^i, \Theta_r^j >_r$ (with $0 < i + j \le e$; it's enough because the coefficients $\mathrm{Tr}_r(\Theta^k)$ with $e < k \le 2e-2$ can be deduced from the $\mathrm{Tr}_r(\Theta^k)$ with $1 \le k \le e$ thanks to Newton's formulae) and $< F.\Theta^i >$ as polynomials in $\Theta_1, \ldots, \Theta_{r-1}$ with coefficients in $k(\mathbf{X})^L$. By induction, we are reduced to $r = 1$, in which case we apply Prop. 3.10. □

10.4 Principle of the method with a primitive element

Let us consider the system $(\mathcal{F})$ defined in § 10.2.2. As we said in that section, the equations $F_i = 0$ in $(\mathcal{F})$ satisfy $A.F_i = F_i$ for every $A \in G$. Let L be a subgroup of $\mathbf{GL}_n(k)$ such that $G \subset L$ and that $k(\mathbf{X})^L$ be a purely transcendental extension of k, $\Pi_1, \ldots, \Pi_n$ polynomials such that $k(\mathbf{X})^L = k(\Pi_1, \ldots, \Pi_n)$, and $\Theta \in k[\mathbf{X}]^G$ a primitive polynomial invariant of G relatively to L. When it is possible, it is convenient to choose Θ among the polynomials F_i of the system.

Then thanks to the algorithm of Prop. 3.10, we can express each polynomial F_i as an algebraic fraction in $\Pi_1, \ldots, \Pi_n$ and Θ, polynomial in Θ:

$$\forall i \in \mathbb{N}_p^*, \qquad F_i(\mathbf{X}) = H_i(\Pi_1, \ldots, \Pi_n, \Theta).$$

Now, let $\mathcal{L}$ be the minimal polynomial of Θ over $k[\mathbf{X}]^L$; we have:

$$\mathcal{L}(\mathbf{X}, T) = \prod_{\Theta' \in L.\Theta} (T - \Theta') \in k[\mathbf{X}]^L[T]$$

(When $L \subset \mathfrak{S}_n$, $\mathcal{L}$ is the generic Lagrange resolvent of Θ, see Def. 6.1).

As $k(\Pi_1, \ldots, \Pi_n) = k(\mathbf{X})^L$, we can write:

$$\mathcal{L}(\mathbf{X}, T) = H_0(\Pi_1, \ldots, \Pi_n, T)$$

where H_0 is some rational fraction. The equation $H_0(\Pi_1,\ldots,\Pi_n,\Theta)=0$ is always satisfied because Θ is a root of $\mathcal{L}$. Then, we solve the system of $(p+1)$ algebraic equations $\forall i\in\mathbb{N}_p, H_i(\Pi_1,\ldots,\Pi_n,\Theta)=0$, in $\Pi_1,\ldots,\Pi_n,\Theta$ seen as indeterminates.

The following theorem is then obvious:

Theorem 10.6 *Let $D\in k[\Pi_1,\ldots,\Pi_n]$ be the L.C.M. of the denominators of all the fractions H_i, $i\in\mathbb{N}_p$, and let $H'_i=DH_i$. For every solution $(x_1,\ldots,x_n)$ of the system $(\mathcal{F}):\forall i\in\mathbb{N}_p^*, F_i(\mathbf{X})=0$, there exists a solution $(\pi_1,\ldots,\pi_n,\theta)$ of the system $(\mathcal{H}'):\forall i\in\mathbb{N}_p, H'_i(\Pi_1,\ldots,\Pi_n,\Theta)=0$ such that $(x_1,\ldots,x_n)$ be a solution of the system $(\mathcal{P}_\pi)$: $\forall i\in\mathbb{N}_n^*,\Pi_i(\mathbf{X})=\pi_i$ and of the equation $\Theta(\mathbf{X})=\theta$. Conversely, for any solution $(\pi_1,\ldots,\pi_n,\theta)$ of the system $(\mathcal{H}')$ such that $D(\pi_1,\ldots,\pi_n)\neq 0$, if $\mathbf{x}=(x_1,\ldots,x_n)$ is a solution of the system $(\mathcal{P}_\pi)$ relative to $(\pi_1,\ldots,\pi_n)$, then there exists some $A\in L$ such that $\Theta(A.\mathbf{x})=\theta$, and then for all $B\in G$, $BA.\mathbf{x}$ is a solution of the system $(\mathcal{F})$.*

Proof – If $\mathbf{x}=(x_1,\ldots,x_n)$ is a solution of $(\mathcal{F})$, then let $\pi_i=\Pi_i(\mathbf{x})$ for all $i\in\mathbb{N}_n^*$ and $\theta=\Theta(\mathbf{x})$. For all $i\in\mathbb{N}_n^*$, $F_i(\mathbf{x})=0$ implies: $D(\pi_1,\ldots,\pi_n)F_i(\mathbf{x})=0$, and as $D(\Pi_1(\mathbf{X}),\ldots,\Pi_n(\mathbf{X}))F_i(\mathbf{X})=H'_i(\Pi_1,\ldots,\Pi_n,\Theta)$ in $k[\mathbf{X}]$, we have $H'(\pi_1,\ldots,\pi_n,\theta)=0$. And for $i=0$, $H_0(\pi_1,\ldots,\pi_n,\theta)=\mathcal{L}(\mathbf{x},\theta)=\prod_{\Theta'\in L.\Theta}(\theta-\Theta'(\mathbf{x}))=0$. So, $\mathbf{x}$ is solution of $(\mathcal{P}_\pi)$ and $(\pi_1,\ldots,\pi_n,\theta)$ is a solution of $(\mathcal{H}')$.

Conversely, if $(\pi_1,\ldots,\pi_n,\theta)$ is a solution of $(\mathcal{H}')$ and $\mathbf{x}$ is a solution of $(\mathcal{P}_\pi)$, then

$$\prod_{\Theta'\in L.\Theta}(\theta-\Theta'(\mathbf{x}))=\mathcal{L}(\mathbf{x},\theta)=H_0(\pi_1,\ldots,\pi_n,\theta)=0.$$

So, there exists $\Theta'\in L.\Theta$ such that $\Theta'(\mathbf{x})=\theta$. There exists $A\in\mathbf{GL}_n(k)$ such that $\Theta'=\Theta$; then, $\Theta(A\mathbf{x})=\theta$. Now, for all $i\in\mathbb{N}_p^*$ and for all $B\in G$, we have:

$$D(\pi_1,\ldots,\pi_n)F_i(BA\mathbf{x})=D(\pi_1,\ldots,\pi_n)H_i(\pi_1,\ldots,\pi_n,\theta)=H'_i(\pi_1,\ldots,\pi_n,\theta)=0\ ;$$

so if we assume that $D(\pi_1,\ldots,\pi_n)\neq 0$, then $F_i(BA\mathbf{x})=0$. □

Remark 10.7 *If we choose for Θ one of the F_i (when it is possible), then we can substitute $\Theta=0$ in the H_i and get a system in the only indeterminates $\Pi_1,\ldots,\Pi_n$. Then, the polynomial $H_0(\Pi_1,\ldots,\Pi_n,0)$ is reduced to $\prod_{\Theta'\in L.\Theta}\Theta'\in k[\mathbf{X}]^L$,* i.e. *the norm of Θ over $k(\mathbf{X})^L$, in terms of Π_1, ..., Π_n.*

Using Proposition 10.4 instead of Theorem 3.1

Theorem 10.6 is based on Th. 3.1, where we use a primitive element of $k(\mathbf{X})^G:k(\mathbf{X})^L$. We can break this extension of fields, as in Prop. 10.4, whose notations we keep, and modify consequently Theorem 10.6.

So, we define fractions F_i that are polynomial in $\Theta_1,\ldots,\Theta_r$ such that

$$\forall i\in\mathbb{N}_p^*,\qquad F_i(\mathbf{X})=H_i(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_r).$$

We define, for all $j\in\mathbb{N}_r^*$, the polynomial $\mathcal{L}_j(\mathbf{X},T)=\prod_{\Theta'\in G_{j-1}.\Theta_j}(T-\Theta')$. It belongs to $k[\mathbf{X}]^{G_{j-1}}[T]\subset k(\Pi_1,\ldots,\Pi_n)[\Theta_1,\ldots,\Theta_{j-1}][T]$. Let N_j be defined by: $\mathcal{L}_j(\mathbf{X},T)=N_j(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_{j-1},T)$, polynomial in $\Theta_1,\ldots,\Theta_r,T$ and fractional in the Π_i. Then, we get the following variant of Theorem 10.6:

Theorem 10.8 *Let $D\in k[\Pi_1,\ldots,\Pi_n]$ be the L.C.M. of the denominators of all the fractions H_i, $i\in\mathbb{N}_p^*$, and N_j, $j\in\mathbb{N}_r^*$. Let $H'_i=DH_i$ for all i and $N'_j=DN_j$ for all j. For every solution $\mathbf{x}=(x_1,\ldots,x_n)$ of the system $(\mathcal{F}):(\forall i\in\mathbb{N}_p^*, F_i(\mathbf{X})=0)$, there exists a solution $(\pi_1,\ldots,\pi_n,\theta_1,\ldots,\theta_r)$ of the system $(\mathcal{H}',N'):(\forall i\in\mathbb{N}_p^*, H'_i(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_r)=0$ and $\forall j\in\mathbb{N}_r^*, N_j(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_j)=0)$ such that $\mathbf{x}$ be a solution of the system $(\mathcal{P}_\pi)$: $\forall i\in\mathbb{N}_n^*,\Pi_i(\mathbf{X})=\pi_i$ and of the equations $\Theta_1(\mathbf{X})=\theta_1,\ldots,\Theta_r(\mathbf{X})=\theta_r$. Conversely, for any solution $(\pi_1,\ldots,\pi_n,\theta_1,\ldots,\theta_r)$ of the system $(\mathcal{H}',N')$ such that $D(\pi_1,\ldots,\pi_n)\neq 0$, if $\mathbf{x}$ is a solution of the system $(\mathcal{P}_\pi)$ relative to $(\pi_1,\ldots,\pi_n)$, then there exists $A\in\mathbf{GL}_n(k)$ such that $\forall j\in\mathbb{N}_r^*,\Theta_j(A.\mathbf{x})=\theta_j$, and then for every $B\in G$, $BA.\mathbf{x}$ is a solution of the system $(\mathcal{F})$.*

Proof – It is roughly the same as that of Theorem 10.6. □

10.5 Principle with a Hironaka decomposition

When caract$(k) = 0$ and when L is a reflexion group, we can translate all the § 10.4 in the language of polynomials, by using the Cohen-Macaulay algebra point of view and Hironaka decomposition of § 10.3.1 and chap. 4 instead of the field theory point of view and primitive element decomposition of § 10.3.2 and chap. 3.

So, we compute fundamental invariants $(\mathbf{\Pi}, \mathbf{\Sigma}) = (\Pi_1, \ldots, \Pi_n, \Sigma_1, \ldots, \Sigma_e)$ such that

$$k[\mathbf{X}]^G = \bigoplus_{i=1}^{e} k[\mathbf{\Pi}]\Sigma_i.$$

Then, whe write

$$\forall i \in \{1, \ldots, p\}, F_i(\mathbf{X}) = H_i(\mathbf{\Pi}, \mathbf{\Sigma}) \qquad \text{with} \qquad H_i \in k[Y_1, \ldots, Y_n, Z_1, \ldots, Z_e].$$

Now, we consider generators $S_1, \ldots, S_s$ of the ideal of syzygies over $k[\mathbf{\Pi}]$ between $\Sigma_1, \ldots, \Sigma_e$ (for instance, the elements of the standard basis given in § 4.4.1). So, translating Theorem 10.6 in the language of polynomials, we get the following theorems:

Theorem 10.9 *For every solution* $\mathbf{x} = (x_1, \ldots, x_n)$ *of the system*

$$(\mathcal{F}): \qquad \forall i \in \{1, \ldots, p\}, F_i(\mathbf{X}) = 0,$$

there exists a solution $(\pi, \sigma) = (\pi_1, \ldots, \pi_n, \sigma_1, \ldots, \sigma_e)$ *of the systems*

$$(\mathcal{H}): \qquad \forall i \in \{1, \ldots, n\}, \quad H_i(\pi, \sigma) = 0$$

$$\textit{and} \qquad (\mathcal{S}): \qquad \forall j \in \{1, \ldots, s\}, \ S_j(\pi, \sigma) = 0$$

such that $\mathbf{x}$ *be a solution of the system*

$$(\mathcal{P}_{\pi,\sigma}): \qquad \forall i \in \{1, \ldots, n\}, \ \forall j \in \{1, \ldots, e\}, \ \Pi_i(X_1, \ldots, X_n) = \pi_i \ \textit{ and } \ \Sigma_j(X_1, \ldots, X_n) = \sigma_j.$$

Conversely, for any solution $(\pi_1, \ldots, \pi_n, \sigma_1, \ldots, \sigma_e)$ *of* $(\mathcal{H})$ *and for any solution* $\mathbf{x} = (x_1, \ldots, x_n)$ *of the system* $(\mathcal{P}_{\pi,\sigma})$ *defined by this solution* (π, σ) *of* $(\mathcal{H})$, $\mathbf{x}$ *is a solution of* $(\mathcal{F})$.

Proof – If $\mathbf{x} = (x_1, \ldots, x_n)$ is a solution of $(\mathcal{F})$, we let $\pi_i = \Pi_i(\mathbf{x})$ and $\sigma_j = \Sigma_j(\mathbf{x})$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, e\}$. Then $\mathbf{x}$ is a solution of $(\mathcal{P}_{\pi,\sigma})$, and for all $i \in \{1, \ldots, p\}$, $0 = F_i(\mathbf{x}) = H_i(\pi, \sigma)$ so that $\mathbf{x}$ is a solution of $(\mathcal{H})$; and $S_j(\mathbf{\Pi}, \mathbf{\Sigma}) = 0$ implies $S_j(\pi, \sigma) = 0$ for all $j \in \{1, \ldots, s\}$ so that (π, σ) is a solution of $(\mathcal{S})$.

Conversely, if (π, σ) is a solution of $(\mathcal{H})$ and $\mathbf{x}$ is a solution of $(\mathcal{P}_{\pi,\sigma})$, then $F_i(\mathbf{x}) = H_i(\pi, \sigma) = 0$ for all $i \in \{1, \ldots, p\}$ so that $\mathbf{x}$ is a solution of $(\mathcal{F})$. □

If now we assume that there exists a reflexion group $L \subset \mathbf{GL}_n(k)$ such that $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$, then we can be more specific:

Theorem 10.10 *Here we assume* $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$. *Then for every solution* $\mathbf{x} = (x_1, \ldots, x_n)$ *of the system*

$$(\mathcal{F}): \qquad \forall i \in \{1, \ldots, p\}, F_i(\mathbf{X}) = 0,$$

there exists a solution $(\pi, \sigma) = (\pi_1, \ldots, \pi_n, \sigma_1, \ldots, \sigma_e)$ *of the system*

$$(\mathcal{H}, \mathcal{S}): \qquad \forall i \in \{1, \ldots, n\}, \ \forall j \in \{1, \ldots, s\}, \quad H_i(\pi, \sigma) = 0 \ \textit{ and } \ S_j(\pi, \sigma) = 0$$

such that $\mathbf{x}$ *be a solution of the system*

$$(\mathcal{P}_{\pi,\sigma}): \qquad \forall i \in \{1,\ldots,n\},\ \forall j \in \{1,\ldots,e\},\ \Pi_i(X_1,\ldots,X_n) = \pi_i \ \text{ and } \ \Sigma_j(X_1,\ldots,X_n) = \sigma_j.$$

Conversely, for any solution $(\pi_1,\ldots,\pi_n,\sigma_1,\ldots,\sigma_e)$ *of* $(\mathcal{H},\mathcal{S})$ *and for any solution* $\mathbf{x} = (x_1,\ldots,x_n)$ *of the system*

$$(\mathcal{P}_{\pi}): \qquad \forall i \in \{1,\ldots,n\},\ \Pi_i(X_1,\ldots,X_n) = \pi_i$$

defined by this solution (π,σ) *of* $(\mathcal{H})$*, there exists* $A \in L$ *such that* $A.\mathbf{x}$ *be a solution of* $(\mathcal{F})$*.*

Proof – The direct part results from Theorem 10.9. As for the converse, the syzygies S_j cancel on $\mathbf{x}$, therefore from Theorem 4.14 there exists an element $A \in L$ such that $\Sigma_i(A.\mathbf{x}) = 0$ for all i. The result follows then from Theorem 10.9. □

Of course, Remark 10.7 still applies here: it is convenient to choose (when it is possible) some of the F_i's as fundamental invariants.

10.6 The algorithm

Here, we recall the different steps of the general algorithm, either by using the Cohen-Macaulay algebra point of view (denoted *infra* by (CMA)) or by using field theory (denoted *infra* by (FT)). With the aim to simplify, we consider here Th. 10.6, not Th. 10.8 (see in § 10.7.5 an example with Th. 10.8).

Input: a system $(\mathcal{F}):\ \forall i \in \mathbb{N}_p^*,\ F_i(X_1,\ldots,X_n) = 0$, and a finite subgroup G of $\mathbf{GL}_n(k)$ such that $\forall i \in \mathbb{N}_p^*, F_i \in k[\mathbf{X}]^G$.

Successive Steps:

i. Choose to use the Cohen-Macaulay algebra point of view (CMA), which works only if caract$(k) = 0$, or the Field theory point of view (FT), which always works.

ii. Find (if possible) a finite subgroup L of $\mathbf{GL}_n(k)$ such that $G \subset L$ and that either L be a reflexion group (case (CMA), see Definition 4.1) either L satisfy Noether's problem, (case (FT), see Noether's problem in § 3.1).

iii. Compute a pure transcendent basis $(\Pi_1,\ldots,\Pi_n)$ of $k[\mathbf{X}]^L$ (case (CMA)) or of $k(\mathbf{X})^L$ (case (FT)), and then the whole Hironaka decomposition $\bigoplus_{i=1}^{e} k[\Pi_1,\ldots,\Pi_n]\Sigma_i$ of $k[\mathbf{X}]^G$ (case (CMA), see the algorithms in chapter 4) or $\bigoplus_{i=0}^{e-1} k(\Pi_1,\ldots,\Pi_n)\Theta^i$ of $k(\mathbf{X})^G$ (case (FT), see chapter 3).

iv. Express the polynomials F_i, $1 \leq i \leq p$, in terms of the fundamental invariants $(\Pi_1,\ldots,\Pi_n)$ and $(\Sigma_1,\ldots,\Sigma_e)$ thanks to Prop. 4.11 (case (CMA)), resp. $(\Pi_1,\ldots,\Pi_n,1,\Theta,\ldots,\Theta^{e-1})$ thanks to Prop. 3.10 (case (FT)).

v. Compute the minimal polynomial of Θ over $k[\mathbf{X}]^L$ (case (FT)) or a family of generators of the ideal of syzygies over $k[\mathbf{\Pi}]$ between the Σ_i (case (CMA))

vi. Solve the system $(\mathcal{H}')$ (see Theorem 10.6) in the variables $\Pi_1,\ldots,\Pi_n,\Theta$ in the case (FT), or the system $(\mathcal{H})$ in the variables $\Pi_1,\ldots,\Pi_n,\Sigma_1,\ldots,\Sigma_e$ (see Theorem 10.10) in the case (FT).

vii. For each solution $(\pi_1, \ldots, \pi_n, \theta)$ of $(\mathcal{H}')$, in the case (FT) (resp. $(\pi_1, \ldots, \pi_n, \sigma_1, \ldots, \sigma_e)$ of $(\mathcal{H})$ in the case (CMA)), solve the corresponding system $(\mathcal{P}_\pi) : \forall i \in \{1, \ldots, n\}, \Pi_i(\mathbf{X}) = \pi_i$, and in each (finite) orbit under L in the set of the solutions of $(\mathcal{P}_\pi)$, keep one solution $\mathbf{x} = (x_1, \ldots, x_n)$ such that $\Theta(\mathbf{x}) = \theta$ in the case (FT) (resp. such that $\forall i \in \{1, \ldots, e\}, \Sigma_i(\mathbf{x}) = \sigma_i$ in the case (CMA)): it costs at most $[L : G]$ tries for each orbit. Let $\mathcal{S}$ be the set of all these solutions $\mathbf{x}$.

Remark 10.11 *Solving $(\mathcal{P}_\pi)$ when L is a product of symmetric groups is particuliarly easy. For instance, when $L = \mathfrak{S}_n$, we can choose $\Pi_i = E_i$ for every $i \in \mathbb{N}_n^*$, so that the solutions of $(\mathcal{P}_\pi)$ are exactly the families of roots, taken in some order, of the polynomial $T^n + \sum_{i=1}^n (-1)^i \pi_i T^{n-i}$.*

viii. In the case (CMA), we take $\mathcal{S}' = \mathcal{S}$ and the algorithm is finished. In the case (FT): for every $\mathbf{x}$ in $\mathcal{S}$, check whether D cancells on $\mathbf{x}$. If it doesn't, we can keep $\mathbf{x}$; if it does, we have to check that $\mathbf{x}$ satisfies $(\mathcal{F})$, and we throw it if it doesn't. Let $\mathcal{S}'$ be the set of all the $\mathbf{x}$ we have kept.

Output: The set of all solutions of $(\mathcal{F})$ is $\{A.\mathbf{x} \ / \ A \in G, \ \mathbf{x} \in \mathcal{S}'\}$.

Implementation The algorithm is implemented in the AXIOM computer algebra language (see [37]), when $L = \mathfrak{S}_n$ and the principal invariants are the elementary symmetric polynomials E_1, ..., E_n. We implemented a domain that computes on symmetric polynomials, represented either as polynomials in the E_i, or as linear combinations of the polynomials $A_{\mathbf{i}} = \sum_{\tau \in \mathfrak{S}_n} \prod_{j=1}^n X_j^{i_{\tau(j)}}$. Then, we implemented the algorithms of Propositions 3.10 and 10.5. Besides, computation in $k[\mathbf{X}]^{\mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}}$ is implemented in SYM (see [67]), with many operations on symmetric polynomials.

10.7 Examples

10.7.1 A very simple example

Let us consider the system:

$$(\mathcal{S}_4) \begin{cases} X_1 + X_2 + X_3 + X_4 & = & 0 \\ X_1X_2 + X_2X_3 + X_3X_4 + X_4X_1 & = & 0 \\ X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_1 + X_4X_1X_2 & = & 0 \\ X_1X_2X_3X_4 - 1 & = & 0 \end{cases}$$

We notice that $G = \mathcal{D}_4 = < (1234), (13) >$. We take $L = \mathcal{S}_4$, $\Pi_i = E_i$, and $\Theta = (X_1 + X_3)(X_2 + X_4)$. Then the system can be written: $(E_1 = 0, \ E_3 = 0, \ E_4 = 1, \ \Theta = 0)$; and Θ satisfies $\Theta\Theta'\Theta'' = 0$, where $\Theta' = (X_1 + X_2)(X_3 + X_4)$ and $\Theta'' = (X_1 + X_4)(X_2 + X_3)$. We can compute that $\Theta\Theta'\Theta'' = E_3E_2E_1 - E_4E_1^2 - E_3^2$.

The equation $E_3E_2E_1 - E_4E_1^2 - E_3^2 = 0$ is always satisfied, when $E_1 = E_3 = 0$. So, from theorem 10.6, the solutions of $\mathcal{S}_4$ are the famillies (x_1, x_2, x_3, x_4) of roots of the equation $T^4 + \sigma_2 T^2 + 1$, for any scalar $\sigma_2 \in k$, with the x_i well numbered. For each value of $\sigma_2 \in k$, we have 8 solutions, *i.e.* $\{(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)}) / \tau \in \mathcal{D}_4\}$ where the x_i's are the roots of $T^4 + \sigma_2 T^2 + 1$ numbered so that $(x_1 + x_3)(x_2 + x_4) = 0$.

Of course, this example could be solved easier: the two first equations are equivalent to $(X_3 = -X_1$ and $X_4 = -X_2)$; then the third equation is satisfied, and the fourth equation can be written: $(X_1X_2)^2 = 1$. Yet, if we compute a standard basis of the ideal defined by this system, it will not factorize anything and will be complicated.

We notice on this easy example that the representation of the solutions that we get is not at all the same than the usual one (see the introduction).

10.7.2 If G is a Reflexion Group

Here, we shall use the representation of the invariants of a reflexion group G given by Chevalley's theorem (see Th. 4.2) to solve an algebraic system whose equations are invariant by the action of G. We apply here in fact the general algorithm of § 10.6 to a particular case. The following system is quoted by K. Gatermann from [55]:

$$(\text{Noo}) \left\{ \begin{array}{rcl} P_1 & = & 1 - X_1(\alpha + X_2^2 + X_3^2) = 0 \\ P_2 & = & 1 - X_2(\alpha + X_3^2 + X_1^2) = 0 \\ P_3 & = & 1 - X_3(\alpha + X_1^2 + X_2^2) = 0 \end{array} \right.$$

where α is an independent parameter. The system (Noo) is equivalent to the following:

$$(\text{Noo}') \left\{ \begin{array}{rcl} Q_1 & = & P_1 + P_2 + P_3 = 0 \\ Q_2 & = & P_1P_2 + P_2P_3 + P_3P_1 = 0 \\ Q_3 & = & P_1P_2P_3 = 0 \end{array} \right.$$

Each equation of this new system is invariant by the action of the symmetric group $\mathfrak{S}_3$, hence can be expressed in terms of $E_3 = X_1X_2X_3$, $E_2 = X_1X_2 + X_2X_3 + X_3X_1$ and $E_1 = X_1 + X_2 + X_3$: we get

$$Q_1 = 3E_3 - (E_2 + \alpha)E_1 + 3 = 0$$

which gives E_3 in terms of E_1 and E_2. We use this equation to eliminate E_3 in Q_2 and Q_3: we get respectively polynomials $R_2(E_1, E_2)$ and $R_3(E_1, E_2)$. We then eliminate E_2 between R_2 and R_3 by computing a resultant; we get the following 3 families of solutions:

$$(\text{Noo1}) \left\{ \begin{array}{rcl} E_1 & = & 0 \\ E_2 & = & \alpha \\ E_3 & = & -1 \end{array} \right. \qquad (\text{Noo2}) \left\{ \begin{array}{rcl} 0 & = & 2E_1^3 + 9\alpha E_1 - 27 \\ E_2 & = & (1/3)E_1^2 \\ E_3 & = & (1/2) - (\alpha/6)E_1 \end{array} \right.$$

$$(\text{Noo3}) \left\{ \begin{array}{rcl} 0 & = & 2\alpha E_1^4 - 2E_1^3 + 9\alpha^2 E_1^2 - 36\alpha E_1 + 4\alpha^3 + 27 \\ (98\alpha^3 - 54)E_2 & = & (42\alpha^3 - 18)E_1^2 + 93\alpha^2 E_1 + 70\alpha^4 - 243\alpha \\ E_3 & = & (1/3)(E_2 + \alpha)E_1 - 1 \end{array} \right.$$

For each solution $(\sigma_1, \sigma_2, \sigma_3)$ of one of the systems (Noo1), (Noo2) or (Noo3), we get corresponding solutions (x_1, x_2, x_3) of (Noo): x_1, x_2 and x_3 are the 3 roots, sorted in any order, of the polynomial $T^3 - \sigma_1 T^2 + \sigma_2 T - \sigma_3$. And by this process, we get all the solutions of (Noo) (it follows from Th. 10.6).

10.7.3 With a Group of Matrices, Using the CMA Point of View

Let us consider the following system:

$$(\text{Rot}) \left\{ \begin{array}{rcl} P_1 = X_1^4 + X_2^4 - 1 & = & 0 \\ P_2 = X_1^3X_2^3(X_1^6 - X_2^6) - 2 & = & 0 \end{array} \right.$$

If we try to eliminate X_2 between the two equations thanks to a resultant, we get the big following irreducible polynomial in X_1 of degree 48, which depends only on X_1^4:

$$4\ X_1^{48} - 24\ X_1^{44} + 69\ X_1^{40} - 125\ X_1^{36} + 156\ X_1^{32} - 138\ X_1^{28} + 70\ X_1^{24} + 12\ X_1^{20} - 39\ X_1^{16} + 15\ X_1^{12} + 16$$

so, we have to find the roots of an irreducible polynomial of degree 12 and then to extract their fourth roots. Using the symmetries, we will show that we are reduced to a polynomial of degree 6 and extracting fourth roots.

Each equation of the system is invariant by the matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, hence by the action of the cyclic group $G = \{Id, A, -Id, -A\}$ generated by A. Now, G is a subgroup of the following finite reflexion group of order 8: $L =< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} >$, which satisfies the conditions of Chevalley's theorem. We compute the following pure basis of $k[\mathbf{X}]^L$: $\Pi_1 = X_1^2 + X_2^2$ and $\Pi_2 = (X_1X_2)^2$, so that $k[\mathbf{X}]^L = k[\Pi_1, \Pi_2]$. Then, (Π_1, Π_2) is a familly of primary invariants of G, and we have the corresponding single secondary invariant $\Sigma = X_1X_2(X_1^2 - X_2^2)$ (they are given in [62, Example 2.2.4]), so that $k[\mathbf{X}]^G = k[\Pi_1, \Pi_2] \bigoplus k[\Pi_1, \Pi_2]\Sigma$. Then, we express the system in terms of the fundamental invariants, thanks to the algorithm of Prop. 4.11. We get: $P_1 = \Pi_1^2 - 2\Pi_2 - 1$ and $P_2 = (\Pi_1^2\Pi_2 - \Pi_2^2)\Sigma - 2$. Besides, we compute $\Sigma^2 - \Pi_1^2\Pi_2 + 4\Pi_2^2 = 0$ (minimal polynomial of Σ over $k[\Pi_1, \Pi_2]$). So, (Rot) is equivalent to:

$$(\text{Rot}') \begin{cases} (\Pi_1^2 - \Pi_2)\Sigma\Pi_2 - 2 &= 0 \\ \Pi_1^2 - 2\Pi_2 - 1 &= 0 \\ \Sigma^2 - \Pi_1^2\Pi_2 + 4\Pi_2^2 &= 0 \\ \Sigma - X_1X_2(X_1^2 - X_2^2) &= 0 \end{cases}$$

We eliminate Π_1 in the first and the third equations thanks to the second one, and then we eliminate Π_2, getting:

$$\Sigma^6 + 3\Sigma^4 + 8\Sigma^3 - 6\Sigma + 16 = 0 \ .$$

For each solution s of this equation of degree 6, we compute the values π_1 and π_2 of Π_1 and Π_2 s.t. (s, π_1, π_2) satisfy (Rot'). Then, the solutions (x_1, x_2) of (Rot) must satisfy $(x_1^2 - x_2^2)^2 = \frac{s^2}{\pi_2}$. So, we know $x_1^2 - x_2^2$ up to the sign and $x_1^2 + x_2^2 = \pi_1$, from which we deduce all the solutions (x_1, x_2) of (Rot).

Therefore, we have reduced the problem from degree 12 to degree 6.

10.7.4 Using (FT) with a simple extension of $k(\mathbf{X})^{\mathfrak{S}_n}$

Cyclic roots systems come from the problem of finding bi-equimodular vectors (see [8] and [12], where these systems are solved for $n = 4, 5, 6, 7$).
In this paragraph, we apply Theorem 10.6 to the following 5^{th}-cyclic roots system, with $L = \mathfrak{S}_5$, $\Pi_i = E_i, \forall i \in \mathbb{N}_5^*$, and $G = \mathcal{D}_5 =< (1\ 2\ 3\ 4\ 5), (2\ 5)(3\ 4) >$:

$$(S_5) \begin{cases} X_1 + X_2 + X_3 + X_4 + X_5 &= 0 \\ X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 &= 0 \\ X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_1 + X_5X_1X_2 &= 0 \\ X_1X_2X_3X_4 + X_2X_3X_4X_5 + X_3X_4X_5X_1 + X_4X_5X_1X_2 + X_5X_1X_2X_3 &= 0 \\ X_1X_2X_3X_4X_5 - 1 &= 0 \end{cases}$$

Let $\Theta = X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1$. Then (S_5) is equivalent to

$$(S_5') : \qquad (E_1 = 0, \Theta = 0, P = 0, E_4 = 0, E_5 - 1 = 0)$$

where $P = X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_1 + X_5X_1X_2$.

Let us use Remark 10.7: as $\Theta = 0$ is one of the equations of (S_5), we can compute, instead of the polynomial $\mathcal{L}$, the norm $C(E_1, \ldots, E_5)$ of Θ over $k(\mathbf{E})$, *i.e.* the product of the 12 elements of $\mathfrak{S}_5.\Theta$.
Now, thanks to the algorithm of § 10.3.2, we find the polynomials A_i and B_i with $\gcd(A_i, B_i) = 1$, $0 \leq i \leq 11$, such that:

$$P = \sum_{i=0}^{11} \frac{A_i(E_1, E_2, E_3, E_4, E_5)}{B_i(E_1, E_2, E_3, E_4, E_5)} \Theta^i.$$

Let $D(\mathbf{E}) = \prod_{i=0}^{11} B_i(\mathbf{E})$. Replacing E_1 and E_4 by 0 and E_5 by 1, we get $\bar{A}_0(E_2, E_3) = A_0(0, E_2, E_3, 0, 1)$, $\bar{B}_0(E_2, E_3) = B_0(0, E_2, E_3, 0, 1)$, $\bar{C}(E_2, E_3) = C(0, E_2, E_3, 0, 1)$ and $\bar{D}(E_2, E_3) = D(0, E_2, E_3, 0, 1)$. We compute:

$$\begin{array}{rcl}
\bar{A}_0 & = & 2E_2^2E_3^7 + 89E_2E_3^6 + 125E_3^5 + 41E_2^4E_3^4 + 550E_2^3E_3^3 - 5^5E_2^2E_3^2 + (189E_2^6 - 6250E_2)E_3 - 1125E_2^5 \\
\bar{B}_0 & = & 2E_2^2E_3^6 + 58E_2E_3^5 + 31E_2^4E_3^3 + 325E_2^3E_3^2 - 625E_2^2E_3 + 108E_2^6 + 5^5E_2 \\
\bar{C} & = & -27E_2^7 - 4E_3^3E_2^5 - 150E_3^2E_2^4 + \left(-12E_3^5 + 5^5\right)E_2^2 - 125E_3^4E_2 + E_3^8
\end{array}$$

$$\mathcal{R}\mathrm{es}_{E_3}(\bar{A}_0, \bar{C}) = -E_2^{10}(E_2^5 + 5^5)^6(24(6E_2)^5 - 5^5)(27E_2^{10} + 7974E_2^5 - 5^5)^2.$$

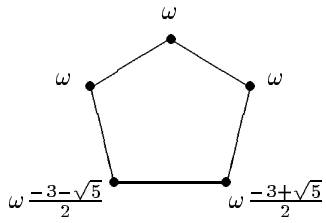
From Theorem 10.6, we know that a necessary condition satisfied by a solution $\mathbf{x}$ of (S_5) is that $\bar{A}_0\bar{D}(\sigma_2, \sigma_3) = \bar{C}(\sigma_2, \sigma_3) = 0$, where $\sigma_2 = E_2(\mathbf{x})$ and $\sigma_3 = E_3(\mathbf{x})$, which implies that σ_2 be a root of $\mathcal{R}\mathrm{es}_{E_3}(\bar{A}_0\bar{D}, \bar{C}) = \mathcal{R}\mathrm{es}_{E_3}(\bar{A}_0, \bar{C})\mathcal{R}\mathrm{es}_{E_3}(\bar{D}, \bar{C})$. Now, this condition is not sufficient, because the solutions cancel the denominator D, as shows the following resultant:

$$\mathcal{R}\mathrm{es}_{E_3}(\bar{B}_0, \bar{C}) = -E_2^8(E_2^5 + 5^5)^5(24(6E_2)^5 - 5^5)(27E_2^{10} + 7974E_2^5 - 5^5)^2$$

In fact, the roots of $\mathcal{R}\mathrm{es}_{E_3}(\bar{D}, \bar{C})$ give no solution of (S_5') that be not already a solution coming from $\mathcal{R}\mathrm{es}_{E_3}(\bar{A}_0, \bar{C})$; and in $\mathcal{R}\mathrm{es}_{E_3}(\bar{A}_0, \bar{C})$, the only factors that lead to solutions of (S_5') are E_2 and $E_2^5 + 5^5$: we could prove this by an argument of multiplicity (see a forthcoming paper), but we can also simply verify it by computing all those candidate-solutions and see that they do not satisfy (S_5'). So, the only solutions are given by $E_2 = 0$ or $E_2^5 = (-5)^5$.

Case Number 1: $E_2^5 = (-5)^5$.–

The solutions for E_2 are: $\sigma_2 = -5\omega^2$, where ω is a fifth root of unity. To each solution σ_2 for E_2 corresponds a single solution for E_3: $\sigma_3 = -5\omega^3$; and we know that the only values for E_1, E_4, E_5 are $\sigma_1 = 0$, $\sigma_4 = 0$ and $\sigma_5 = 1$. The corresponding values x_i for the X_i are the solutions of the system: $E_i(X_1, X_2, X_3, X_4, X_5) = \sigma_i$, for $i = 1, 2, 3, 4, 5$ (which are of course the roots of the polynomial $T^5 - 5\omega^2T^3 + 5\omega^3T^2 - 1$), *i.e.* ω, ω, ω, $\omega\frac{-3-\sqrt{5}}{2}$, $\omega\frac{-3+\sqrt{5}}{2}$, ordered so that $\Theta(x_1, x_2, x_3, x_4, x_5) = 0$. For each of the 5 values of ω, 10 different orders are allowed. It leads to the following 50 solutions:

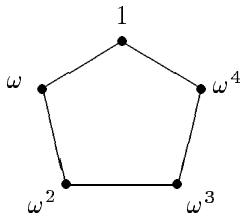


where ω is one of the five fifth roots of unity, and the vertices of the pentagon denote the roots, in the order x_1, x_2, x_3, x_4, x_5, beginning with any vertex and going along either clockwise or anticlockwise.

Case Number 2: $E_2 = 0$.–

If we replace E_2 by $\sigma_2 = 0$ in $C(E_2, E_3)$, we get $E_3 = 0$. The corresponding values x_i for the X_i are the roots of $T^5 - 1$, *i.e.* the fifth roots of unity, ordered so that $\Theta(x_1, x_2, x_3, x_4, x_5) = 0$; we get the

following 20 solutions:



where ω is either $e^{\frac{2i\pi}{5}}$ or $e^{\frac{4i\pi}{5}}$ (the values $e^{\frac{8i\pi}{5}}$ and $e^{\frac{6i\pi}{5}}$ of ω would lead to the same solutions up to a symmetry).

Hence, **we proved that (S_5) has exactly the 50 + 20 = 70 solutions written above**.

10.7.5 Breaking the simple extension of $k(\mathbf{X})^{\mathfrak{S}_n}$

Here, we look for an improvement of the method of § 10.7.4, whose notations we keep: we study the same system (S_5). But we use Theorem 10.8 instead of Theorem 10.6.

We notice that the alternating group $G_1 = \mathcal{A}_5 =< (1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5) >$ satisfies:

$$G \subset G_1 \subset G_0 = \mathfrak{S}_5.$$

From Prop. 10.4, to this groups corresponds the following field extension:

$$k(\mathbf{X})^{\mathfrak{S}_5} = k(\mathbf{E}) \subset k(\mathbf{X})^{\mathcal{A}_5} = k(\mathbf{E})[V] \subset k(\mathbf{X})^{G} = k(\mathbf{E})[\Theta] = k(\mathbf{E})[V][\Theta]$$

where V is the following (primitive) invariant of $\mathcal{A}_5$: $V = \prod_{i<j}(X_j - X_i)$.

Then we do as in § 10.7.4; the only difference is the way we express P. Here, we use the algorithm of Prop. 10.5 to express P as:

$$P = \sum_{i=0}^{5} \frac{A_i(E_1, E_2, E_3, E_4, E_5)V + A'_i(E_1, E_2, E_3, E_4, E_5)}{B_i(E_1, E_2, E_3, E_4, E_5)}\Theta^i.$$

where the A_i, A'_i and B_i are polynomials. Let $\bar{A}_0(E_2, E_3)$, $\bar{A}'_0(E_2, E_3)$ and $\bar{B}_0(E_2, E_3)$ be the evaluations of respectively A_0, A'_0 and B_0 on $(0, E_2, E_3, 0, 1)$. We compute:

$$\begin{aligned}
\bar{A}_0 &= 210E_2E_3^7 + 6000E_3^6 + 30E_2^4E_3^5 + 2375E_2^3E_3^4 + 25000E_2^2E_3^3 + (270E_2^6 + 250000E_2)E_3^2 + (-1125E_2^5 - 390625)E_3 + 140625E_2^4\\
\bar{A}'_0 &= 216E_3^{11} + 86E_2^3E_3^9 + 7590E_2^2E_3^8 + (8E_2^6 - 48000E_2)E_3^7 + (1990E_2^5 + 175000)E_3^6 + 42075E_2^4E_3^5 + (144E_2^8 - 71875E_2^3)E_3^4\\
&\quad + (8730E_2^7 - 3531250E_2^2)E_3^3 + (138375E_2^5 + 12890625E_2)E_3^2 + (486E_2^{10} - 1406250E_2^5 - 9765625)E_3 + 12150E_2^9 + 703125E_2^4\\
\bar{B}_0 &= 1458E_2^{10} + 216E_2^3E_2^8 + 24300E_2^2E_2^7 + 8E_2^8E_2^6 + (3168E_3^5 + 1856250)E_2^5 + 120000E_2^4E_2^4 + (118E_3^8 + 450000E_3^3)E_2^3\\
&\quad + (11400E_3^7 + 3750000E_3^2)E_2^2 + 187500E_3^6E_2 + 432E_3^{10} + 350000E_3^5 - 19531250.
\end{aligned}$$

Now, we apply Theorem 10.8. We compute (notations of Theorem 10.8) the polynomials $N_1(\mathbf{E}, V)$ and $N_2(\mathbf{E}, V, \Theta)$. Let C_1 and C_2 denote the residues of these polynomials modulo $(E_1 = 0,\ E_4 = 0,\ E_5 = 1,\ \Theta = 0)$. We find: $\begin{array}{rcl} C_1 &=& V^2 - 108E_3^5 - 16E_2^3E_3^3 - 825E_2^2E_3^2 + 3750E_2E_3 - 108E_2^5 - 3125\\ C_2 &=& E_2V - 2E_3^4 - 15E_2^2E_3 + 125E_2 \end{array}$.

Then, we compute:

$$\mathcal{R}es_{E_3}(\mathcal{R}es_V(\bar{A}_0V + \bar{A}'_0, C_2), \mathcal{R}es_V(C_1, C_2)) = E_2^{10}(E_2^5 + 5^5)^7 f_1 f_2^2 f_3 f_4$$

$$\mathcal{R}es_{E_3}(\bar{B}_0, \mathcal{R}es_V(C_1, C_2)) = (E_2^5 + 5^5)^6 f_1 f_2^2 f_3 f_4$$

where $f_1 = 27E_2^5 - 1$, $f_2 = 27E_2^{10} + 7974E_2^5 - 3125$, $f_3 = 256E_2^{15} + 21089952E_2^{10} + 1587890625E_2^5 + 30517578125$, $f_4 = 5038848E_2^{20} + 1941472800000E_2^{15} + 81696996562500000E_2^{10} + 9100772094726562500000E_2^5 - 298023223876953125$.
We conclude like in § 10.7.4: $E_2 = 0$ or $E_2^5 = (-5)^5$.

BEWARE.–The polynomial C_2 in § 10.7.5 is the norm of Θ over $k(\mathbf{X})^{\mathcal{A}_5}$, whereas in § 10.7.4 we used the norm C of Θ over $k(\mathbf{X})^{\mathfrak{S}_5}$. If we had used here the norm over $k(\mathbf{X})^{\mathfrak{S}_5}$, a big irreducible parasite factor of degree 60 would have appeared in the resultant $\mathcal{R}es_{E_3}(\mathcal{R}es_V(\bar{A}_0V + \bar{A}'_0, C_1), C)$. Indeed, the polynomials $E_1, \ldots, E_5, V, \Theta$ are not algebraically independent; if we want to lift the solutions in $E_1, \ldots, E_5, V, \Theta$ back to solutions in $X_1, \ldots, X_n$, we need to check that they satisfy the algebraic relations between these polynomials. It is sufficient that they satisfy (C_1 and C_2), but (C_1 and C) is not enough. This is implicit in Theorem 10.8. I would like to thank Marc Giusti here for pointing out to me this difficulty.

10.7.6 Using (CMA) with $L = \mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_s}$

A) Cyclic 5^{th}-Roots System

In this approach, the system is transformed, which destroys some of its symmetries but yet simplifies its resolution. This idea and the following computation are due to Daniel Lazard [48], whom I would like to thank for his help.

The solutions of (S_5) can be deduced by homogenization from those of the following system:

$$(S'_5)\begin{cases} X_1 + X_2 + X_3 + X_4 + 1 = 0 \\ X_1X_2 + X_2X_3 + X_3X_4 + X_4 + X_1 = 0 \\ X_1X_2X_3 + X_2X_3X_4 + X_3X_4 + X_4X_1 + X_1X_2 = 0 \\ X_1X_2X_3X_4 + X_2X_3X_4 + X_3X_4X_1 + X_4X_1X_2 + X_1X_2X_3 = 0 \end{cases}$$

A 5-tuple $(x_1, x_2, x_3, x_4, x_5)$ is a solution of (S_5) if and only if ($x_5 \neq 0$, $(x_1/x_5, x_2/x_5, x_3/x_5, x_4/x_5)$ is a solution of (S'_5) and $x_5^5(x_1/x_5)(x_2/x_5)(x_3/x_5)\ (x_4/x_5) = 1$).

The permutation group corresponding to (S'_5) is $G = \{Id, (1\ 4)(2\ 3)\}$. Let L be the following subgroup of $\mathfrak{S}_4$: $L = \{Id, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}$. We have $G \subset L$ and $L \simeq \mathfrak{S}_2 \times \mathfrak{S}_2$. So, from Example 1.2, we know that $k[\mathbf{X}]^L = k[S, T, P, Q]$ where

$$S = X_1 + X_4, \qquad T = X_2 + X_3, \qquad P = X_1X_4, \qquad Q = X_2X_3.$$

and from Th. 3.1 that $k(\mathbf{X})^G = k(S, T, P, Q)[\Theta]$ where $\Theta = X_1X_2 + X_3X_4$. In fact, we even have: $k[\mathbf{X}]^G = k[S, T, P, Q][\Theta]$.

So, we can rewrite the system (S'_5) in terms of S, T, P, Q and Θ:

$$(S''_5)\begin{cases} S + T + 1 = 0 & (1) \\ Q + S + \Theta = 0 & (2) \\ QS + P + \Theta = 0 & (3) \\ PQ + PT + QS = 0 & (4) \end{cases}.$$

We have: $L.\Theta = \{\Theta, \Theta'\}$, where $\Theta' = X_1X_3 + X_2X_4 = (2\ 3).\Theta = (1\ 4).\Theta$. So, as we have $\Theta + \Theta' = ST$ and $\Theta\Theta' = S^2Q + T^2P - 4PQ$, we know that

$$\Theta^2 - ST\,\Theta + S^2Q + T^2P - 4PQ = 0 \qquad (5).$$

As there is no denominator, we know from Theorem 10.6 that the solutions of (S''_5) and (5) will give us exactly the solutions of (S'_5). So, let us solve (S''_5).

Thanks to (1), (2) and (3), we eliminate T, Θ and P in (4) and (5). We get:

$$(Q - 1)(Q + S^2 - SQ + S) = 0 \qquad (4')$$

$$-QS^3 + (2 - Q)S^2 + (4Q^2 - 2Q + 1)S + Q - 3Q^2 = 0 \qquad (5').$$

As the equation (4′) has two factors, we can simplify the elimination of Q:

Case Number 1: $Q-1=0$.–

By eliminating Q, $(5')$ becomes: $(S-2)(S^2+S-1)=0$.

Case Number 1a: $Q-1=0$ **and** $S-2=0$.– We get the following roots of (S'_5):

$$x'_1=x'_4=1, \qquad \{x'_2,x'_3\}=\{\frac{-3+\sqrt{5}}{2},\frac{-3-\sqrt{5}}{2}\}.$$

As $x'_1x'_2x'_3x'_4=1$, $(x'_1\omega,x'_2\omega,x'_3\omega,x'_4\omega,\omega)$ is a corresponding solution of (S_5) if and only if $\omega^5=1$.

So, we get the $10\times 5=50$ solutions of (S_5) that are written in paragraph 10.7.4, case number 1.

Remark.– Permuting the x_i, we get other values for s and q. For example, $(x_1,x_2,x_3,x_4,x_5)=(\frac{-3-\sqrt{5}}{2},\frac{-3+\sqrt{5}}{2},1,1,1)$ is another solution of (S_5); and it leads to $q=x'_2x'_3=\frac{-3+\sqrt{5}}{2}$ and $s=x'_1+x'_4=\frac{-1-\sqrt{5}}{2}$. They satisfy s^2+s-1 and $q+s^2-sq+s=0$. An other solution of (S_5) is $(x_1,x_2,x_3,x_4,x_5)=(\frac{-3-\sqrt{5}}{2},1,1,1,\frac{-3+\sqrt{5}}{2})$. The associated solution of (S'_5) is $(x'_1,x'_2,x'_3,x'_4)=(\frac{7+3\sqrt{5}}{2},-\frac{3+\sqrt{5}}{2},-\frac{3+\sqrt{5}}{2},-\frac{3+\sqrt{5}}{2})$. We compute the corresponding s and q: they satisfy $s^2-4s-1=0$ and $(1-s)q+s(s+1)=0$.

Case Number 1b: $Q-1=0$ **and** $S^2+S-1=0$.– If ω denotes a primitive fifth root of unity, then $\alpha=\omega+\omega^4$ and $\beta=\omega^2+\omega^3$ satisfy: $\alpha+\beta=\alpha\beta=-1$. So, we must have $\{s,t\}=\{\alpha,\beta\}$; and $p=q=1$. Now, we have $x'_1x'_2+x'_3x'_4=\theta$, with $\theta=-q-s=-1-s$. The only solution is: $(x'_1,x'_2,x'_3,x'_4)=(\omega^\epsilon,\omega^{2\epsilon},\omega^{3\epsilon},\omega^{4\epsilon})$ with $\epsilon=\pm 1$. As $x'_1x'_2x'_3x'_4=1$, the corresponding solutions of (S_5) satisfy $x_5^5=1$; and we get the $10\times 2=20$ solutions of (S_5) written in paragraph 10.7.4, case number 2.

Case Number 2: $Q+S^2-SQ+S=0$.–

By eliminating Q, $(5')$ becomes: $S^2(S^2+S-1)(S^2-4S-1)=0$. Now, $S=0$ leads to $Q=0$, which gives no solution of (S_5) (we must have $PQ\neq 0$); and the cases $S^2+S-1=0$ and $S^2-4S-1=0$ lead to the same solutions as the case number 1a ($S-2=0$, $Q-1=0$): see the Remark in case 1a.

B) Cyclic 6^{th}-Roots System

Here, we solve the following system (S_6) with the same method:

$$(S_6)\quad\begin{cases} X_1+X_2+X_3+X_4+X_5+X_6 &= 0\\ X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_6+X_6X_1 &= 0\\ X_1X_2X_3+X_2X_3X_4+X_3X_4X_5+X_4X_5X_6+X_5X_6X_1+X_6X_1X_2 &= 0\\ X_1X_2X_3X_4+X_2X_3X_4X_5+X_3X_4X_5X_6+X_4X_5X_6X_1+X_5X_6X_1X_2+X_6X_1X_2X_3 &= 0\\ X_1X_2X_3X_4X_5+X_2X_3X_4X_5X_6+X_3X_4X_5X_6X_1+X_4X_5X_6X_1X_2+X_5X_6X_1X_2X_3+X_6X_1X_2X_3X_4 &= 0\\ X_1X_2X_3X_4X_5X_6-1 &= 0 \end{cases}$$

By deshomogenizing through the variable X_4, (S_6) becomes:

$$(S'_6)\quad\begin{cases} X_1+X_2+X_3+X_5+X_6+1 &= 0\\ X_1X_2+X_2X_3+X_3+X_5+X_5X_6+X_6X_1 &= 0\\ X_1X_2X_3+X_2X_3+X_3X_5+X_5X_6+X_5X_6X_1+X_6X_1X_2 &= 0\\ X_1X_2X_3+X_2X_3X_5+X_3X_5X_6+X_5X_6X_1+X_5X_6X_1X_2+X_6X_1X_2X_3 &= 0\\ X_1X_2X_3X_5+X_2X_3X_5X_6+X_3X_5X_6X_1+X_5X_6X_1X_2+X_5X_6X_1X_2X_3+X_6X_1X_2X_3 &= 0 \end{cases}$$

The permutation group corresponding to (S'_6) is $G=\{Id,(2\,6)(3\,5)\}$. We choose $L=\{Id,(2\,6),(3\,5),(2\,6)(3\,5)\}$. Then $G\subset L$, and a system of principal invariants of L is:

$$S=X_2+X_6,\ T=X_3+X_5,\ P=X_2X_6,\ Q=X_3X_5,\ X=X_1.$$

Then, $k[\mathbf{X}]^L = k[S,T,P,Q,X]$. The polynomial $\Theta = X_2X_3 + X_5X_6$ is a primitive invariant of G relative to L. Its orbit under L is $L.\Theta = \{\Theta, \Theta'\}$, where $\Theta' = X_2X_5 + X_3X_6$. So, the equation "$H_0$" of Theorem 10.6 is $\Theta^2 - (\Theta + \Theta')\Theta + \Theta\Theta' = 0$, where

$$\Theta + \Theta' = ST,\ \Theta\Theta' = Q(S^2 - 2P) + P(T^2 - 2Q).$$

So, we compute easily the system $(\mathcal{H}')$ of Theorem 10.6:

$$(S_6'') \begin{cases} S+T+X+1 & = & 0 \\ XS+T+\Theta & = & 0 \\ Q+XP+(X+1)\Theta & = & 0 \\ QS+X\Theta+XPT & = & 0 \\ (X+1)PQ+X(QS+PT) & = & 0 \\ \Theta^2 - ST\Theta + QS^2 + PT^2 - 4PQ & = & 0 \end{cases}$$

As there is no denominator, Theorem 10.6 proves that solving (S_6'') will give us exactly the solutions of (S_6'). Now, the 3 first equations in (S_6'') give T, Θ and Q in terms of P, S and X. So, (S_6'') is equivalent to:

$$\begin{cases} -S-X-1 & = & T \\ S+X+1-XS & = & \Theta \\ S(X^2-1) - XP - X^2 - 2X - 1 & = & Q \\ (-2XS - X^2 - X)P + (X^2-1)S^2 - (2X^2+X+1)S + X^2 + X & = & 0 \\ (X+1)((X^2-X)S^2 + ((X^2-X-1)P - X^2 - X)S - XP^2 - (X^2+3X+1)P) & = & 0 \\ (X^2-X)S^3 + ((1-X)P - X^2 - 3X + 2)S^2 + ((6+2X-4X^2)P - X^2 + 2X + 3)S + 4XP^2 + (5P+1)(X+1)^2 & = & 0 \end{cases}$$

The fifth equation has two factors; it leads to two different cases. In each one, we eliminate thanks to resultants the remaining variable. We get the following 5 solutions:

i. $T = 1,\ \Theta = -2,\ Q = 1,\ P = 1,\ S = -1,\ X = -1$

ii. $T = -S,\ \Theta = 2S,\ Q = 1,\ P = 1,\ S^2 + 2S - 2 = 0,\ X = -1$

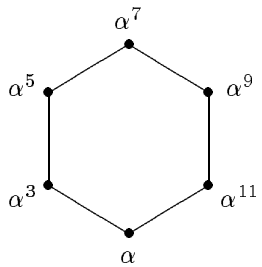
iii. $T = -S - 2,\ \Theta = 2,\ Q = -S - 3,\ P = S - 1,\ S^2 + 2S - 2 = 0,\ X = 1$

iv. $T = -X - S - 1,\ \Theta = (1-S)X + S + 1,\ Q = (1-2S)X - S,\ P = SX + 2S + 1,$
$S^2 + (3-X)S + 2X + 2 = 0,\ X^2 + 4X + 1 = 0$

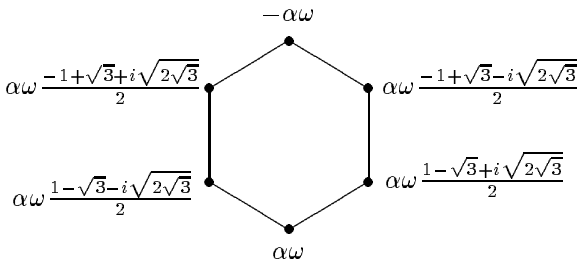
v. $T = X^3 + 5X^2 - 3X - 3,\ 2\Theta = X^2 + 1,\ 4Q = -X^3 - 5X^2 + 3X) - 1,\ 4P = X^3 + 3X^2 - 3X - 1,$
$4S = -X^3 - 5X^2 - X - 1,\ X^4 + 4X^3 - 6X^2 + 4X + 1$

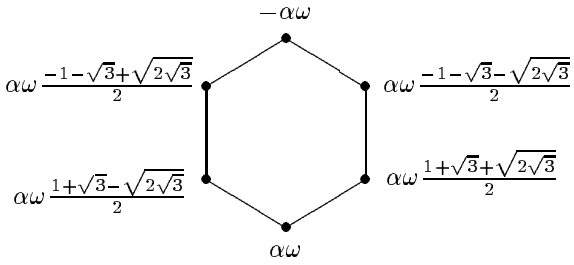
Now, we study successively these 5 cases.

Case Number (i).– We find the following 12 solutions, where $\alpha = e^{\frac{i\pi}{6}}$.



Case Number (ii).– We find 72 solutions partitioned in 2 families:

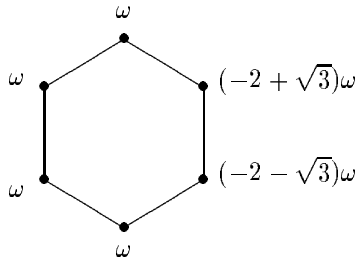




where we let still $\alpha = \frac{\sqrt{3}+i}{2}$, and where ω is one of the elements $1, -j^2 = \alpha^2, j = \alpha^4$. We do not let ω run along all the sixth roots of 1, because the 3 other values correspond to the 3 given ones up to a symmetry on the x_i.

Besides, we notice that by permuting circularly the x_i, we find the values of S, T, P, Q, X, Θ corresponding to the case number (v). So, case number (v) yields no other solution.

Case Number (iii).– We find these $12 \times 6 = 72$ solutions, where ω runs along the six sixth roots of unity:



Besides, we notice that by permuting circularly the x_i, we find the values of S, T, P, Q, X, Θ corresponding to the case number (iv).

So, we have found all the solutions of (S_6): **we proved that (S_6) has exactly 156 solutions, written *supra*.**

Acknowledgements. The notions of invariant theory that I use here were partially developed in [17]. After the congress AAECC'95, François Ollivier suggested to me that they could be applied to solve systems like the "cyclic roots systems". Besides, this paper has benefited from fruitful conversations with Marc Chardin, Vincent Cossart, Marc Giusti, Daniel Lazard, Olivier Piltant and Annick Valibouze. This paper was also enriched thanks to detailed comments, questions and references from the anonymous referees. The author thanks all of them.

Conclusion

La méthode de résolution des systèmes algébriques ayant des symétries que nous avons présentée au chapitre 10 présente certaines analogies avec la résolution par radicaux d'une équation algébrique dont le groupe est résoluble. En effet, la méthode du chapitre 10 consiste aussi en un scindage de l'extension de corps dans laquelle vivent les solutions du système d'équations, et c'est aussi une considération sur un groupe de symétries qui permet ce scindage. Cependant le rapprochement s'arrête là pour le moment; nous sommes en effet très loin d'avoir trouvé un analogue du théorème de dualité de Galois pour les systèmes d'équations algébriques. Par exemple, les deux approches présentées (théorie des corps, avec un seul invariant primitif donc une seule inconnue et une seule équation supplémentaire — son polynôme minimal — mais des dénominateurs ; ou propriété de Cohen-Macaulay, avec plusieurs invariants secondaires, donc plusieurs inconnues et plusieurs équations — les syzygies — supplémentaires, mais sans dénominateurs) nécessitent des hypothèses bien distinctes (dans le premier cas, le groupe G doit être inclus dans un groupe fini L qui satisfait le problème de Noether ; dans le second, k doit être de caractéristique nulle et L être un groupe de réflexions). Nous avons donc des techniques permettant dans certains cas de résoudre par radicaux les systèmes (voir par exemple le § 10.7.6), mais certainement pas une condition nécessaire et suffisante de résolubilité par radicaux.

Notons d'ailleurs que le groupe G considéré au chapitre 10 (groupe qui laisse invariantes les équations) peut être déterminé directement à partir du système $(\mathcal{F})$ d'équations à résoudre, contrairement au groupe de Galois d'un polynôme, dont le calcul nécessite une compréhension des relations entre les racines de ce polynôme, ce qui est mesuré par exemple par des factorisations de résolvantes.

$\star$

Les méthodes développées aussi bien dans la seconde partie (théorie de Galois effective) que dans la troisième (résolutions de systèmes algébriques) ont en commun d'effectuer une fois pour toutes un pré-calcul coûteux qui ne dépend que d'un groupe, ou plutôt d'une action de groupe (calcul des invariants fondamentaux, et des syzygies entre les invariants secondaires), et d'être ensuite très rapides une fois ce pré-calcul fait. Les annexes A et B en font la démonstration pour ce qui concerne la théorie de Galois : elles donnent en effet des formules explicites de résolution complète des degrés 5 et 6 transitifs, formules qui ont été obtenues par un pré-calcul plus coûteux. L'Annexe C en apporte l'illustration pour les systèmes symétriques : un pré-calcul coûteux des invariants fondamentaux et de leurs syzygies permet ensuite de résoudre très vite des systèmes symétriques — et qui plus est de présenter leurs solutions sous une forme réduite (résolution par radicaux par exemple).

Annexe A

Résolution du degré 5 (descente directe)

Nous illustrons dans cette annexe la méthode du chapitre 8 sur l'exemple du degré 5, dans la variante suivante : au lieu d'utiliser un élément primitif comme au chapitre 8, avec les techniques du chapitre 3, on utilise ici les techniques du chapitre 4, comme indiqué au § 6.4.3.

Le plus coûteux en degré 5 est de différencier les groupes $\mathfrak{D}_5$ et $\mathfrak{C}_5$: tous les autres groupes peuvent être identifiés facilement en factorisant des résolvantes absolues de degré inférieur à 6, et en se contentant de regarder les degrés de leurs facteurs irréductibles (un algorithme est donné dans [69]).

Par contre, l'algorithme de [69] utilise des factorisations de polynômes de degré 20 pour distinguer $\mathfrak{C}_5$ de $\mathfrak{D}_5$. Nous nous proposons ici de montrer qu'on peut en fait distinguer $\mathfrak{C}_5$ de $\mathfrak{D}_5$ par des factorisations de degré au plus 6.

Tous les sous-groupes de $\mathfrak{S}_5$ isomorphes à $\mathfrak{C}_5$ (resp. à $\mathfrak{D}_5$) sont conjugués, donc il revient au même ici de déterminer la représentation du groupe de Galois à conjugaison près ou à isomorphisme près.

$\star$

Soit $f \in k[T]$, où k est supposé de caractéristique nulle. On peut éliminer le coefficient sous-dominant s de f en remplaçant f par $f(T - s/5)$, ce qui ne change pas son groupe de Galois. Supposons donc f de la forme

$$f = T^5 + aT^3 - bT^2 + cT - d.$$

Soit Γ la représentation de $\mathrm{Gal}_k(f)$ dans $\mathfrak{S}_5$ définie par une numérotation (arbitraire) des racines de f, et $[\Gamma]$ sa classe de conjugaison.

Les polynômes symétriques élémentaires $E_1, \ldots, E_5$ se spécialisent alors comme suit :

$$\widetilde{E_1} = 0, \qquad a = \widetilde{E_2}, \qquad b = \widetilde{E_3}, \qquad c = \widetilde{E_4}, \qquad d = \widetilde{E_5}.$$

Soit V l'invariant primitif suivant du groupe alterné $\mathfrak{A}_5$:

$$V = \prod_{1 \le i < j \le 5} (X_j - X_i).$$

Calculons la résolvante associée, grâce au domaine `Polynomessymetriques` du chapitre 2. On obtient :

$$\begin{aligned}\mathcal{L}_{V,f} \;=\; & T^2 - (3125d^4 - 3750abd^3 + (2000ac^2 + (2250b^2 - 900a^3)c + 825a^2b^2 + 108a^5)d^2 \\ & + (-1600bc^3 + 560a^2bc^2 + (-630ab^3 - 72a^4b)c + 108b^5 + 16a^3b^3)d + 256c^5 \\ & - 128a^2c^4 + (144ab^2 + 16a^4)c^3 + (-27b^4 - 4a^3b^2)c^2)\end{aligned}$$

Si $\Gamma \subset \mathfrak{A}_5$, cette résolvante se factorise sur k ce qui permet de calculer la valeur spécialisée $v = \widetilde{V}$. En fait, on a le choix entre deux racines : v et $-v$, mais peu importe laquelle on choisit puisqu'on calcule Γ à conjugaison près.

Calculons maintenant une famille d'invariants fondamentaux de $\mathfrak{D}_5$ à l'aide du paquetage INVAR [39]. On obtient :

$$k[\mathbf{X}]^{\mathfrak{D}_5} = \bigoplus_{i=1}^{6} k[\mathbf{\Pi}]\Sigma_i \qquad \text{avec}$$

$$\begin{aligned}
\Pi_1 &= E_1 \\
\Pi_2 &= X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 \\
\Pi_3 &= X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 \\
\Pi_4 &= X_1^3 + X_2^3 + X_3^3 + X_4^3 + X_5^3 \\
\Pi_5 &= X_1^5 + X_2^5 + X_3^5 + X_4^5 + X_5^5 \\
\Sigma_1 &= 1 \\
\Sigma_2 &= X_1X_3(X_1 + X_3) + X_3X_5(X_3 + X_5) + X_5X_2(X_5 + X_2) + X_2X_4(X_2 + X_4) + X_4X_1(X_4 + X_1) \\
\Sigma_3 &= X_1^4 + X_2^4 + X_3^4 + X_4^4 + X_5^4 \\
\Sigma_4 &= X_1X_3(X_1^2 + X_3^2) + X_3X_5(X_3^2 + X_5^2) + X_5X_2(X_5^2 + X_2^2) + X_2X_4(X_2^2 + X_4^2) + X_4X_1(X_4^2 + X_1^2) \\
\Sigma_5 &= X_1^2X_3^2(X_1 + X_3) + X_3^2X_5^2(X_3 + X_5) + X_5^2X_2^2(X_5 + X_2) + X_2^2X_4^2(X_2 + X_4) + X_4^2X_1^2(X_4 + X_1) \\
\Sigma_6 &= \Sigma_3^2
\end{aligned}$$

Parmi ces polynômes, nous savons spécialiser ceux qui sont symétriques : on calcule

$$\begin{aligned}
\widetilde{\Pi_1} &= 0 \\
\widetilde{\Pi_2} &= -2a \\
\widetilde{\Pi_4} &= 3b \\
\widetilde{\Pi_5} &= 5d - 5ab \\
\widetilde{\Sigma_3} &= 2a^2 - 4c
\end{aligned}$$

Enfin, pour spécialiser les autres, il suffit de calculer une résolvantes relative à $\mathfrak{A}_5$ de chacun de ces invariants. On utilise à nouveau le domaine `Polynomessymetriques` et l'algorithme de la Proposition 4.11 et on obtient :

$$\begin{aligned}
\mathcal{L}^{\mathfrak{A}_5}_{\Pi_3,\mathbf{x}} &= T^6 - 3\,a\,T^5 + (3\,a^2 - 5\,c)\,T^4 + (-a^3 + 10\,c\,a)\,T^3 + \left(-8\,c\,a^2 + b^2\,a - 25\,d\,b + 15\,c^2\right)T^2 \\
&\quad + \left(-v + 3\,c\,a^3 - b^2\,a^2 + \left(25\,d\,b - 15\,c^2\right)a\right)T + \tfrac{1}{2}\,a\,v + \left(-\tfrac{15}{2}\,d\,b + c^2\right)a^2 + \left(\tfrac{7}{2}\,c\,b^2 + \tfrac{125}{2}\,d^2\right)a - b^4 - 25\,d\,c\,b + 5\,c^3
\end{aligned}$$

$$\begin{aligned}
\mathcal{L}^{\mathfrak{A}_5}_{\Sigma_2,\mathbf{x}} &= T^6 + 9\,b\,T^5 + \left(2\,c\,a + 33\,b^2\right)T^4 + \left(12\,c\,b\,a + 63\,b^3\right)T^3 + \left(\left(d\,b + c^2\right)a^2 + \left(26\,c\,b^2 - 25\,d^2\right)a + 66\,b^4 + 15\,d\,c\,b - 4\,c^3\right)T^2 \\
&\quad + \left(-d\,v + \left(3\,d\,b^2 + 3\,c^2\,b\right)a^2 + \left(24\,c\,b^3 - 75\,d^2\,b\right)a + 36\,b^5 + 45\,d\,c\,b^2 - 12\,c^3\,b\right)T - \tfrac{3}{2}\,d\,b\,v - d^2\,a^4 + d\,c\,b\,a^3 \\
&\quad + \left(2\,d\,b^3 + 2\,c^2\,b^2 + 10\,d^2\,c\right)a^2 + \left(8\,c\,b^4 - \tfrac{115}{2}\,d^2\,b^2 - 3\,d\,c^2\,b\right)a + 8\,b^6 + \tfrac{69}{2}\,d\,c\,b^3 - 9\,c^3\,b^2 + \tfrac{125}{2}\,d^3\,b - 25\,d^2\,c^2
\end{aligned}$$

$$\begin{aligned}
\mathcal{L}^{\mathfrak{A}_5}_{\Sigma_4,\mathbf{x}} &= T^6 + (6a^2 - 12c)T^5 + (12a^4 - 54ca^2 - 10b^2a + 10db + 52c^2)T^4 + (-av + 8a^6 - 72ca^4 - 40b^2a^3 + (40db + 160c^2)a^2 + 80cb^2a - 80dcb - 96c^3)T^3 \\
&\quad + ((-3a^3 + 6ca)v - 36ca^6 - 36b^2a^5 + (-97db + 169c^2)a^4 + (217cb^2 + 187d^2)a^3 + (27b^4 - 102dcb - 184c^3)a^2 + (-56db^3 - 196c^2b^2 - 60d^2c)a + 2cb^4 + 35d^2b^2 + 184dc^2b + 64c^4)T^2 \\
&\quad + ((-6a^5 + 11ca^3 + 3b^2a^2 + (-4db - 8c^2)a + cb^2 + d^2)v - 24ca^8 + 8b^2a^7 + (-274db + 162c^2)a^6 + (98cb^2 + 374d^2)a^5 + (54b^4 + 664dcb - 276c^3)a^4 + (-112db^3 - 300c^2b^2 - 868d^2c)a^3 \\
&\quad + (-104cb^4 + 70d^2b^2 - 184dc^2b + 96c^4)a^2 + (224dcb^3 + 144c^3b^2 + 240d^2c^2)a - 8c^2b^4 - 140d^2cb^2 - 96dc^3b)T \\
&\quad + (-4a^7 + 11ca^5 + 3b^2a^4 + (-4db - 6c^2)a^3 + (-5cb^2 + d^2)a^2 + 8dcba - 2c^2b^2 - 2d^2c)v - 108db^2a^8 + (84cb^2 + 207d^2)a^7 + (-24b^4 + 271dcb + 20c^3)a^6 + (229db^3 - 208c^2b^2 - 580d^2c)a^5 \\
&\quad + (-109cb^4 - 575d^2b^2 - 96dc^2b - 60c^4)a^4 + (-14b^6 + 77dcb^3 + 64c^2b^2 + 451d^2b + 504d^2c^2)a^3 + (54db^5 + 62c^2b^4 + 487d^2cb^2 - 152dc^3b + 64c^5 - 100d^4)a^2 \\
&\quad + (-3cb^6 - 41d^2b^4 - 282dc^2b^3 + 32c^4b^2 - 530d^3cb - 32d^2c^3)a - b^8 - 14dcb^5 + 13c^3b^4 + 10d^3b^3 + 126d^2c^2b^2 - 64dc^4b + 125d^4c
\end{aligned}$$

Nous avons fait l'économie du calcul de $\mathcal{L}^{\mathfrak{A}_5}_{\Sigma_5,\mathbf{x}}$ car, comme on pourra le constater, Σ_5 n'intervient pas dans la suite.

Remarque A.1 *Si l'on avait choisi $-v$ au lieu de v comme valeur de $\widetilde{V}$ (voir plus haut), on aurait obtenu des résultats différents pour les résolvantes relatives ci-dessus, qui dépendent de v. En fait, chacune de ces résolvantes divise la résolvante absolue correspondante (par exemple $\mathcal{L}^{\mathfrak{A}_5}_{\Pi_3,\mathbf{x}}$ divise $\mathcal{L}_{\Pi_3,\mathbf{x}}$), et le polynôme que l'on aurait obtenu à la place de $\mathcal{L}^{\mathfrak{A}_5}_{\Pi_3,\mathbf{x}}$ en utilisant $-v$ au lieu de v est simplement le quotient de $\mathcal{L}_{\Pi_3,\mathbf{x}}$ par $\mathcal{L}^{\mathfrak{A}_5}_{\Pi_3,\mathbf{x}}$. Cela ne changerait rien à la suite (à condition d'utiliser aussi $-v$ dans le calcul des autres résolvantes) puisqu'on cherche Γ à conjugaison près.*

On calcule $\varpi^{\mathfrak{A}_5}(\mathfrak{D}_5,\mathfrak{D}_5) = \varpi^{\mathfrak{A}_5}(\mathfrak{D}_5,\mathfrak{C}_5) = (5,1)$ (avec le programme d'A. Valibouze en GAP). Supposons les résolvantes ci-dessus séparables. Alors quand Γ est isomorphe à $\mathfrak{D}_5$ ou à $\mathfrak{C}_5$ (et seulement dans ce cas d'ailleurs, comme on peut le constater sur la table des ϖ donnée dans [69]) les résolvantes ont un facteur irréductible de degré 5 et un facteur linéaire sur k. Ces facteurs linéaires nous donnent donc les valeurs spécialisées π_3, σ_2 et σ_4 de conjugués respectifs de Π_3, Σ_2 et Σ_4. Normalement (voir Théorème 4.14), nous devrions tester que les valeurs qu'on obtient satisfont bien des syzygies, mais ici ce n'est pas la peine car on n'a pas le choix : chaque résolvante n'a qu'une racine. On est donc bien certain qu'il existe un même élément $\tau \in \mathfrak{S}_5$ tel que $\sigma_2 = \tau.\widetilde{\Sigma_2}$, $\sigma_4 = \tau.\widetilde{\Sigma_4}$ et $\pi_3 = \tau.\widetilde{\Pi_3}$.

Passons maintenant à l'étape finale : on sait que $[\Gamma]$ est soit la classe de conjugaison d'un groupe diédral soit d'un groupe cyclique. Pour identifier $[\Gamma]$, calculons donc une résolvante d'un invariant primitif Ψ de $\mathfrak{C}_5$ relatif à $\mathfrak{D}_5$. En voici un :

$$\Psi = X_1^2X_2 + X_2^2X_3 + X_3^2X_4 + X_4^2X_5 + X_5^2X_1.$$

Il admet un unique conjugué sous l'action de $\mathfrak{D}_5$:

$$\Psi' = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_5^2 + X_5X_1^2.$$

Nous calculons maintenant $\Psi+\Psi'$ et $\Psi.\Psi'$, qui appartiennent à $k[\mathbf{X}]^{\mathfrak{D}_5}$, et nous les exprimons en fonction des invariants fondamentaux Σ_i et Π_i à l'aide du paquetage INVAR. On en déduit la valeur de $\mathcal{L}_\Psi^{\mathfrak{D}_5} = (T-\Psi)(T-\Psi')$, puis

$$\mathcal{L}_{\Psi,\mathbf{x}}^{\mathfrak{D}_5} \;=\; T^2 + (\sigma_2+3b)T - \tfrac{1}{2}\,\pi_3^3 + \tfrac{5}{2}\,a\,\pi_3^2 + \left(-\tfrac{3}{2}\,\sigma_4 + \tfrac{11}{2}\,c - 5\,a^2\right)\,\pi_3 + 2\,b\,\sigma_2 + 2\,a\,\sigma_4 - 9\,a\,c + 7\,b^2 + 4\,a^3$$

Quand cette résolvante est séparable (rappelons que l'on peut toujours se ramener à des résolvantes séparables : voir la Prop. 8.5), il suffit donc de tester si elle se factorise sur k, c'est-à-dire si son discriminant est un carré. Si oui, Γ est un groupe cyclique, sinon c'est un groupe diédral.

Nous avons donc donné ici un algorithme entièrement formel pour identifier le groupe de Galois d'un polynôme de degré 5 par des factorisations de polynômes de degré inférieur ou égal à 6. Les algorithmes existants jusqu'ici en degré 5 factorisaient des résolvantes absolues de degré 20, ou bien calculaient les résolvantes relatives de façon numérique.

Annexe B

Résolution du degré 6 (descente diagonale)

Nous présentons dans cette annexe un algorithme de résolution du problème direct en degré 6 transitif sur un corps k de caractéristique nulle, en ne factorisant que des polynômes de degré au plus 10.

La méthode utilisée est la «descente diagonale» du chapitre 9.

On peut aussi, par la méthode de descente directe, résoudre le degré 6 en ne factorisant que des polynômes de degré au plus 10, mais on est alors obligé d'utiliser le Corollaire 6.11, c'est-à-dire de calculer le groupe de Galois des facteurs de bas degré des résolvantes.

Nous montrons ici que la méthode de descente diagonale permet d'éviter de calculer le groupe de Galois des facteurs de résolvantes.

Nous nous limiterons à distinguer les classes de conjugaison de $[T_6]$ et $[T_{11}]$: en effet, les autres classes sont faciles à distinguer par la méthode de descente directe ou par des résolvantes absolues.

Soit donc $f = T^6 + a\,T^4 - b\,T^3 + c\,T^2 - d\,T + e \in k[T]$ un polynôme irréductible. Calculons des invariants fondamentaux de T_{11} à l'aide du paquetage INVAR : on a

$$k[\mathbf{X}]^{T_{11}} = \bigoplus_{i=1}^{6} k[\Pi_1^{T_{11}}, \ldots, \Pi_6^{T_{11}}]\ \Sigma_i^{T_{11}}$$

avec

$$\Pi_1^{T_{11}} = P_1,\ \Pi_2^{T_{11}} = X_1X_2 + X_3X_4 + X_5X_6,\ \Pi_3^{T_{11}} = P_2,\ \Pi_4^{T_{11}} = P_3,\ \Pi_5^{T_{11}} = P_4,\ \Pi_6^{T_{11}} = P_6$$

et

$$\Sigma_1^{T_{11}} = 1,\ \Sigma_2^{T_{11}} = P_1P_2 - P_3 - X_1X_2(X_1 + X_2) - X_3X_4(X_3 + X_4) - X_5X_6(X_5 + X_6),$$
$$\Sigma_3^{T_{11}} = P_1P_3 - P_4 - X_1X_2(X_1^2 + X_2^2) - X_3X_4(X_3^2 + X_4^2) - X_5X_6(X_5^2 + X_6^2),$$
$$\Sigma_4^{T_{11}} = P_5,\ \Sigma_5^{T_{11}} = (\Sigma_2^{T_{11}})^2,\ \Sigma_6^{T_{11}} = P_5\,\Sigma_3^{T_{11}}$$

en posant $P_i = \sum_{j=1}^{6} X_j^i$ (polynômes de Newton).

On a $T_6 \subset T_{11}$. Pour séparer $[T_6]$ de $[T_{11}]$, nous allons calculer une résolvante d'un invariant Θ^{T_6} de T_6 relative à T_{11}. Un tel invariant est :

$$\Theta^{T_6} = (X_1X_2 - X_3X_4)(X_3X_4 - X_5X_6)(X_5X_6 - X_1X_2).$$

On a

$$\mathcal{L}_{\Theta^{T_6}}^{T_{11}} = T^2 - (\Theta^{T_6})^2$$

avec (calcul donné par le paquetage INVAR) :

$$(\Theta^{T_6})^2 \equiv -27(\Sigma_2^{T_{11}})^2 - 36\Pi_4^{T_{11}}\Sigma_2^{T_{11}} - 12(\Pi_4^{T_{11}})^2 + (1/2)(\Pi_3^{T_{11}})^3 + 3\Pi_2^{T_{11}}(\Pi_3^{T_{11}})^2 + 6(\Pi_2^{T_{11}})^2\Pi_3^{T_{11}} + 4(\Pi_2^{T_{11}})^3 \pmod{\Pi_1^{T_{11}}}$$

Il ne nous reste donc plus qu'à spécialiser les invariants $\Pi_2^{T_{11}}$ et $\Sigma_2^{T_{11}}$ (les autres invariants fondamentaux sont symétriques). Nous allons le faire grâce au calcul de résolvantes du groupe T_{13}, qui est d'indice 10 : c'est la méthode de «descente diagonale».

Soit Γ la représentation de $\mathrm{Gal}_k(f)$ dans $\mathfrak{S}_6$ pour une numérotation fixée arbitraire des racines de f.

Si $\Gamma \in [T_6]$ ou $[T_{11}]$ alors les degrés des facteurs irréductibles des résolvantes $\mathcal{L}_{\Theta^{T_{13}},f}$ sont 6 et 4 (voir les tables de partitions dans [69]).

On a les invariants primitifs suivants de T_{13} :

$$\Theta_1^{T_{13}} = X_1X_2X_3 + X_4X_5X_6$$
$$\Theta_2^{T_{13}} = X_1X_2 + X_2X_3 + X_3X_1 + X_4X_5 + X_5X_6 + X_6X_4.$$

On remarque que le polynôme suivant :

$$\Phi_1^{T_{11}} = (2354).\Theta_1^{T_{13}} + (143256).\Theta_1^{T_{13}} + (1365).\Theta_1^{T_{13}} + (163452).\Theta_1^{T_{13}} \in k[\mathbf{X}]^{T_{11}} \tag{B.1}$$

est un invariant de T_{11}. On peut, grâce au paquetage INVAR, le décomposer en fonction des invariants fondamentaux ; on obtient :

$$\Phi_1^{T_{11}} = -2/3\Pi_4^{T_{11}} + 1/2\Pi_1^{T_{11}}\Pi_3^{T_{11}} - \Pi_1^{T_{11}}\Pi_2^{T_{11}} + 1/6(\Pi_1^{T_{11}})^3 - \Sigma_2^{T_{11}}. \tag{B.2}$$

De même pour

$$\Phi_2^{T_{11}} = (2354).\Theta_2^{T_{13}} + (143256).\Theta_2^{T_{13}} + (1365).\Theta_2^{T_{13}} + (163452).\Theta_2^{T_{13}} \in k[\mathbf{X}]^{T_{11}} \tag{B.3}$$

qui s'écrit :

$$\Phi_2^{T_{11}} = -\Pi_3^{T_{11}} - 2\Pi_2^{T_{11}} + (\Pi_1^{T_{11}})^2. \tag{B.4}$$

Il suffit alors de calculer les spécialisés de $\Phi_1^{T_{11}}$ et $\Phi_2^{T_{11}}$: d'après (B.1) et (B.3), ce sont respectivement le coefficient sous-dominant du facteur de degré 4 des résolvantes $\mathcal{L}_{\Theta_1^{T_{13}},f}$ et $\mathcal{L}_{\Theta_2^{T_{13}},f}$.

On déduit alors des équations (B.2) et (B.4) les valeurs spécialisées de $\Pi_2^{T_{11}}$ et $\Sigma_2^{T_{11}}$. Le problème est alors résolu puisqu'on peut maintenant spécialiser $\mathcal{L}^{T_{11}}_{\Theta_{T_6}}$: on distingue alors $[T_6]$ de $[T_{11}]$ en testant si son discriminant est un carré dans k (quand elle est séparable, c'est-à-dire quand ce discriminant est non nul).

Annexe C

Autres exemples de systèmes symétriques

Dans cette annexe, nous présentons de bonnes illustrations du Théorème 10.10, que les exemples du Chapitre 10 n'exploitaient pas complètement.

C.1 Système aux racines cycliques cinquièmes

C'est le système suivant, déjà étudié aux paragraphes 10.7.4, 10.7.5 et 10.7.6 :

$$(S_5)\ \begin{cases} P_1 = X_1 + X_2 + X_3 + X_4 + X_5 & = & 0 \\ P_2 = X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 & = & 0 \\ P_3 = X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_1 + X_5X_1X_2 & = & 0 \\ P_4 = X_1X_2X_3X_4 + X_2X_3X_4X_5 + X_3X_4X_5X_1 + X_4X_5X_1X_2 + X_5X_1X_2X_3 & = & 0 \\ P_5 = X_1X_2X_3X_4X_5 - 1 & = & 0 \end{cases}$$

Nous nous proposons ici de le résoudre par une méthode qui utilise l'invariance des équations de ce système par le groupe diédral $\mathfrak{D}_5$, et qui ne fasse pas intervenir de fractions. On s'appuie sur le Théorème 10.10.

On a la décomposition d'Hironaka suivante (donnée par MAGMA [1]) de l'algèbre des invariants de $\mathfrak{D}_5$:

$$k[\mathbf{X}]^{\mathfrak{D}_5} = \bigoplus_{i=1}^{12} k[\mathbf{\Pi}]\Sigma_i$$

où $\Pi_i = E_i$ (polynômes symétriques élémentaires) pour $1 \leq i \leq 5$ et

$$\begin{aligned}
\Sigma_1 &= 1 \\
\Sigma_2 &= X_1X_2 + X_1X_5 + X_2X_3 + X_3X_4 + X_4X_5 \\
\Sigma_3 &= X_1X_2(X_1 + X_2) + X_2X_3(X_2 + X_3) + X_3X_4(X_3 + X_4) + X_4X_5(X_4 + X_5) + X_5X_1(X_5 + X_1) \\
\Sigma_4 &= \Sigma_2^2 \\
\Sigma_5 &= X_1X_2(X_1^2 + X_2^2) + X_2X_3(X_2^2 + X_3^2) + X_3X_4(X_3^2 + X_4^2) + X_4X_5(X_4^2 + X_5^2) + X_5X_1(X_5^2 + X_1^2) \\
\Sigma_6 &= \Sigma_2\Sigma_3 \\
\Sigma_7 &= X_1X_2(X_1^3 + X_2^3) + X_2X_3(X_2^3 + X_3^3) + X_3X_4(X_3^3 + X_4^3) + X_4X_5(X_4^3 + X_5^3) + X_5X_1(X_5^3 + X_1^3) \\
\Sigma_8 &= \Sigma_2\Sigma_5
\end{aligned}$$

$$\begin{aligned}
\Sigma_9 &= \Sigma_2^3 \\
\Sigma_{10} &= \Sigma_2\Sigma_7 \\
\Sigma_{11} &= \Sigma_3\Sigma_7 \\
\Sigma_{12} &= \Sigma_2\Sigma_3\Sigma_7.
\end{aligned}$$

On calcule en outre les relations entre les invariants secondaires de la forme $\Sigma_i\Sigma_j = A_1^{i,j}\Sigma_1 + \ldots + A_{12}^{i,j}\Sigma_{12}$, avec $A_k^{i,j} \in k[\mathbf{\Pi}]$: on sait (Lemme 4.13) qu'elles engendrent l'idéal des syzygies entre ces invariants secondaires. En fait, vu les relations du type $\Sigma_4 = \Sigma_2^2$, $\Sigma_6 = \Sigma_2\Sigma_3$, ... il suffit de décomposer les polynômes suivants : $\Sigma_3^2, \Sigma_3\Sigma_5, \Sigma_5^2, \Sigma_5\Sigma_7, \Sigma_7^2, \Sigma_2^2\Sigma_3, \Sigma_2^2\Sigma_5, \Sigma_2^2\Sigma_7, \Sigma_2^4$ dans la base $(\Sigma_1, \ldots, \Sigma_{12})$; à elles seules, ces relations engendrent en effet toutes les autres. Ce calcul est effectué en MAGMA [1].

Jusqu'ici, tous les calculs faits ne dépendent que de l'action du groupe $\mathfrak{D}_5$, pas du système particulier à résoudre. On peut donc effectuer ces pré-calculs une seule fois pour tous les systèmes invariants par cette action de groupe.

Revenons au système (S_5). On exprime ses équations en fonction des invariants fondamentaux Π_i et Σ_i, ce qui donne :

$$\left\{\begin{array}{lcl}
P_1 &=& \Pi_1 \\
P_2 &=& \Sigma_2 \\
P_3 &=& \Pi_1\Sigma_2 - \Pi_3 - \Sigma_3 \\
P_4 &=& \Pi_4 \\
P_5 &=& \Pi_5 - 1
\end{array}\right. .$$

Calculons maintenant une base standard de l'idéal engendré par $P_1, \ldots, P_5$ et par les syzygies précalculées plus haut. Nous prenons par exemple l'ordre lexicographique, avec $\Sigma_{12} > \ldots > \Sigma_1 > \Pi_5 > \ldots > \Pi_1$, de manière à éliminer les invariants secondaires (mais on pourrait utiliser l'ordre de Bayer et Stillman, cela suffirait pour éliminer les Σ_i à moindre coût). On obtient, par Maple [2] :

$$\begin{aligned}
\mathcal{S} = (&\Sigma_{12},\ 25\Sigma_{11} - 6\Pi_2^4,\ \Sigma_{10},\ \Sigma_9,\ \Sigma_8,\ 125\Sigma_7^2 + 625\Sigma_7 + 41\Pi_2^5 - 3125,\ \Pi_2\Sigma_7 - 30\Pi_2,\ \Sigma_6, \\
&5\Sigma_5 + 2\Pi_2^2,\ \Sigma_4,\ 125\Sigma_3 - \Pi_2^4,\ \Sigma_2,\ \Pi_5 - 1,\ \Pi_4,\ 125\Pi_3 + \Pi_2^4,\ \Pi_2^6 + 3125\Pi_2,\ \Pi_1).
\end{aligned}$$

Considérons le système formé par les 5 derniers éléments de cette base standard : il s'écrit

$$(S_5')\left\{\begin{array}{lcl}
\Pi_1 &=& 0 \\
\Pi_2^6 + 3125\Pi_2 &=& 0 \\
125\Pi_3 + \Pi_2^4 &=& 0 \\
\Pi_4 &=& 0 \\
\Pi_5 - 1 &=& 0
\end{array}\right. .$$

Sa résolution est immédiate, et conduit aux deux familles de solutions suivantes :

$(\pi_1 = 0, \pi_2 = 0, \pi_3 = 0, \pi_4 = 0, \pi_5 = 1)$ et $(\pi_1 = 0, \pi_2 = -5\omega^2, \pi_3 = -5\omega^3, \pi_4 = 0, \pi_5 = 1)$, où ω désigne l'une des 5 racines cinquièmes de l'unité.

Comme $\Pi_1, \ldots, \Pi_5$ sont les polynômes symétriques élémentaires, les X_i sont les 5 racines du polynôme $T^5 - \Pi_1 T^4 + \Pi_2 T^3 - \Pi_3 T^2 + \Pi_4 T - \Pi_5$. Donc les solutions $(x_1, \ldots, x_5)$ de (S_5) sont telles que les x_i sont les 5 racines d'un polynôme $T^5 - \pi_1 T^4 + \pi_2 T^3 - \pi_3 T^2 + \pi_4 T - \pi_5$ où $(\pi_1, \ldots, \pi_5)$ est solution de (S_5'). La réciproque est vraie d'après le Théorème 10.10 à condition d'ajouter à (S_5') les autres éléments de la base standard $(\mathcal{S})$, et, en appelant alors $(\sigma_2, \ldots, \sigma_{12})$ les solutions pour $\Sigma_2, \ldots, \Sigma_{12}$, de vérifier que $(x_1, \ldots, x_5)$ satisfait bien les équations $\Sigma_i = \sigma_i$. En fait, il suffit de rajouter l'équation $\Sigma_2 = 0$, c'est-à-dire

$X_1X_2 + X_1X_5 + X_2X_3 + X_3X_4 + X_4X_5 = 0$, car elle implique toutes les autres. On est donc ramené au même stade qu'à la fin du paragraphe 10.7.4, et l'on obtient les mêmes solutions. Ici, contrairement au §10.7.4, on n'a pas eu le problème des dénominateurs qui induisaient des solutions parasites : on a au contraire pu déterminer directement l'ensemble exact des solutions de (S_5), comme nous le garantit le Théorème 10.10.

Comparaison avec un calcul de base standard : Calculons la base standard lexicographique, ici donnée par GB [23], de l'idéal engendré par les polynômes du système (S_5) :

```
sugar(cyclic(5,DMP([X1,X2,X3,X4,X5],INT)))
```

```
[X1 + X2 + X3 + X4 + X5,275*X2**2 + 825*X2*X5 + 550*X4**6*X5 +
1650*X4**5*X5**2 + 275*X4**4*X5**3 -550*X4**3*X5**4 + 275*X4**2
-566*X4*X5**11 -69003*X4*X5**6 + 69019*X4*X5 -1467*X5**12 -178981*X5**7
+ 179073*X5**2,275*X2*X3 -275*X2*X5 + 275*X3**2 + 550*X3*X5
-330*X4**6*X5 -1045*X4**5*X5**2 -275*X4**4*X5**3 + 275*X4**3*X5**4
-550*X4**2 + 334*X4*X5**11 + 40722*X4*X5**6 -40726*X4*X5 + 867*X5**12 +
105776*X5**7 -105873*X5**2,275*X2*X4 -275*X2*X5 -110*X4**6*X5
-440*X4**5*X5**2 -275*X4**4*X5**3 + 275*X4**3*X5**4 + 124*X4*X5**11 +
15092*X4*X5**6 -15106*X4*X5 + 346*X5**12 + 42218*X5**7
-42124*X5**2,55*X2*X5**5 -55*X2 + X5**11 + 143*X5**6 -144*X5,275*X3**3 +
550*X3**2*X5 -550*X3*X5**2 + 275*X4**6*X5**2 + 550*X4**5*X5**3
-550*X4**4*X5**4 + 550*X4**2*X5 -232*X4*X5**12 -28336*X4*X5**7 +
28018*X4*X5**2 -568*X5**13 -69289*X5**8 + 69307*X5**3,275*X3*X4
-275*X3*X5 + 440*X4**6*X5 + 1210*X4**5*X5**2 -275*X4**3*X5**4 +
275*X4**2 -442*X4*X5**11 -53911*X4*X5**6 + 53913*X4*X5 -1121*X5**12
-136763*X5**7 + 136674*X5**2,55*X3*X5**5 -55*X3 + X5**11 + 143*X5**6
-144*X5,55*X4**7 + 165*X4**6*X5 + 55*X4**5*X5**2 -55*X4**2
-398*X4*X5**11 -48554*X4*X5**6 + 48787*X4*X5 -1042*X5**12 -127116*X5**7
+ 128103*X5**2,55*X4**2*X5**5 -55*X4**2 -2*X4*X5**11 -231*X4*X5**6 +
233*X4*X5 -8*X5**12 -979*X5**7 + 987*X5**2,X5**15 + 122*X5**10
-122*X5**5 -1]
```

et l'ensemble triangulaire correspondant, aussi donné par GB :

```
triangSets(lextri(sugar(cyclic(5,DMP([X1,X2,X3,X4,X5],INT)))))
```

```
[[55*X1 + 55*X4 -2*X5**6 -233*X5,55*X2 + X5**6 + 144*X5,55*X3 + X5**6 +
144*X5,55*X4**2 -2*X4*X5**6 -233*X4*X5 -8*X5**7 -987*X5**2,X5**10 +
123*X5**5 + 1],[5*X1 -6*X4**5*X5 -20*X4**4*X5**2 -15*X4**3*X5**3
-15*X4**2*X5**4 -15*X4 -9*X5,5*X2 -2*X4**5*X5 -10*X4**4*X5**2
-15*X4**3*X5**3 -10*X4**2*X5**4 -10*X4 -8*X5,5*X3 + 8*X4**5*X5 +
30*X4**4*X5**2 + 30*X4**3*X5**3 + 25*X4**2*X5**4 + 30*X4 + 22*X5,X4**6 +
4*X4**5*X5 + 5*X4**4*X5**2 + 5*X4**3*X5**3 + 5*X4**2*X5**4 + 4*X4 +
X5,X5**5 -1],[X1  - X5,X2 + X3 + 3*X5,X3**2 + 3*X3*X5 + X5**2,X4  -
X5,X5**5 -1],[X1 + X2 + 3*X5,X2**2 + 3*X2*X5 + X5**2,X3  - X5,X4  -
X5,X5**5 -1]]
```

La différence avec la méthode développée au Chapitre 10 et illustrée dans cette annexe n'est pas tant dans le temps de calcul que dans la forme du résultat obtenu, du moins sur cet exemple : nous y obtenons en effet directement une résolution par radicaux du système (voir les solutions décrites au § 10.7.4), ce que ne donnent ni la base standard lexicographique ni même l'ensemble triangulaire.

C.2 Système aux racines cycliques sixièmes

C'est le système suivant, déjà étudié au paragraphe 10.7.6 :

$$(S_6)\quad \begin{cases} X_1+X_2+X_3+X_4+X_5+X_6 = 0\\ X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_6+X_6X_1 = 0\\ X_1X_2X_3+X_2X_3X_4+X_3X_4X_5+X_4X_5X_6+X_5X_6X_1+X_6X_1X_2 = 0\\ X_1X_2X_3X_4+X_2X_3X_4X_5+X_3X_4X_5X_6+X_4X_5X_6X_1+X_5X_6X_1X_2+X_6X_1X_2X_3 = 0\\ X_1X_2X_3X_4X_5+X_2X_3X_4X_5X_6+X_3X_4X_5X_6X_1+X_4X_5X_6X_1X_2+X_5X_6X_1X_2X_3+X_6X_1X_2X_3X_4 = 0\\ X_1X_2X_3X_4X_5X_6-1 = 0 \end{cases}$$

Nous nous proposons ici de le résoudre en utilisant l'invariance des équations de ce système par le groupe diédral $\mathfrak{D}_6$, en nous appuyant sur le Théorème 10.9.

On a la décomposition d'Hironaka suivante (donnée par MAGMA [1]) de l'algèbre des invariants de $\mathfrak{D}_6$:

$$k[\mathbf{X}]^{\mathfrak{D}_6} = \bigoplus_{i=1}^{12} k[\mathbf{\Pi}]\Sigma_i$$

$$\begin{aligned}
\Pi_1 &= X_1+X_2+X_3+X_4+X_5+X_6\\
\Pi_2 &= X_1^2+X_2^2+X_3^2+X_4^2+X_5^2+X_6^2\\
\Pi_3 &= X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_6+X_6X_1\\
\Pi_4 &= X_1X_3+X_2X_4+X_3X_5+X_4X_6+X_5X_1+X_6X_2\\
\Pi_5 &= X_1^3+X_2^3+X_3^3+X_4^3+X_5^3+X_6^3\\
\Pi_6 &= X_1^6+X_2^6+X_3^6+X_4^6+X_5^6+X_6^6\\
\Sigma_1 &= 1\\
\Sigma_2 &= X_1^2(X_2+X_6)+X_2^2(X_3+X_1)+X_3^2(X_4+X_2)+X_4^2(X_5+X_3)+X_5^2(X_6+X_4)+X_6^2(X_1+X_5)\\
\Sigma_3 &= X_1^2(X_3+X_5)+X_2^2(X_4+X_6)+X_3^2(X_5+X_1)+X_4^2(X_6+X_2)+X_5^2(X_1+X_3)+X_6^2(X_2+X_4)\\
\Sigma_4 &= X_1^4+X_2^4+X_3^4+X_4^4+X_5^4+X_6^4\\
\Sigma_5 &= X_1^3(X_2+X_6)+X_2^3(X_3+X_1)+X_3^3(X_4+X_2)+X_4^3(X_5+X_3)+X_5^3(X_6+X_4)+X_6^3(X_1+X_5)\\
\Sigma_6 &= X_1^2X_2^2+X_2^2X_3^2+X_3^2X_4^2+X_4^2X_5^2+X_5^2X_6^2+X_6^2X_1^2\\
\Sigma_7 &= X_1^5+X_2^5+X_3^5+X_4^5+X_5^5+X_6^5\\
\Sigma_8 &= \Sigma_2^2\\
\Sigma_9 &= \Sigma_2\Sigma_4\\
\Sigma_{10} &= \Sigma_2\Sigma_5\\
\Sigma_{11} &= \Sigma_2\Sigma_7\\
\Sigma_{12} &= \Sigma_4\Sigma_7.
\end{aligned}$$

On calcule en outre les relations entre les invariants secondaires de la forme $\Sigma_i\Sigma_j = A_1^{i,j}\Sigma_1 + \ldots + A_{12}^{i,j}\Sigma_{12}$, avec $A_k^{i,j} \in k[\mathbf{\Pi}]$, en MAGMA [1].

Jusqu'ici, tous les calculs faits ne dépendent que de l'action du groupe $\mathfrak{D}_6$, pas du système particulier à résoudre. On peut donc effectuer ces pré-calculs une seule fois pour tous les systèmes invariants par cette action de groupe.

Revenons au système (S_6). On exprime (calcul fait en MAGMA) ses équations en fonction des invariants fondamentaux Π_i et Σ_i, ce qui donne :

$$\left\{\begin{array}{lcl} P_1 & = & \Pi_1 \\ P_2 & = & \Pi_3 \\ P_3 & = & -(1/4)\Pi_1^3 + (3/4)\Pi_1\Pi_2 + \Pi_1\Pi_3 + (1/2)\Pi_1\Pi_4 - (1/2)\Pi_5 - (1/2)\Sigma_3 - \Sigma_2 \\ P_4 & = & -(1/12)\Pi_1^4 + (1/2)\Pi_1^2\Pi_2 + (1/2)\Pi_1^2\Pi_3 - (2/3)\Pi_1\Pi_5 - \Pi_1\Sigma_2 - (1/4)\Pi_2^2 - (1/2)\Pi_2\Pi_3 \\ & & +\Sigma_6 + \Sigma_5 + (1/2)\Sigma_4 \\ P_5 & = & (1/120)\Pi_1^5 - (1/12)\Pi_1^3\Pi_2 + (1/6)\Pi_1^2\Pi_5 + (1/8)\Pi_1\Pi_2^2 - (1/4)\Pi_1\Sigma_4 - (1/6)\Pi_2\Pi_5 \\ & & +(1/5)\Sigma_7 \\ P_6 & = & (1/720)\Pi_1^6 - (1/48)\Pi_1^4\Pi_2 + (1/18)\Pi_1^3\Pi_5 + (1/16)\Pi_1^2\Pi_2^2 - (1/8)\Pi_1^2\Sigma_4 - (1/6)\Pi_1\Pi_2\Pi_5 \\ & & +(1/5)\Pi_1\Sigma_7 - (1/48)\Pi_2^3 + (1/8)\Pi_2\Sigma_4 + (1/18)\Pi_5^2 - (1/6)\Pi_6 - 1 \end{array}\right. .$$

Calculons maintenant une base standard de l'idéal engendré par $P_1, \ldots, P_6$ et par les syzygies précalculées plus haut. Nous prenons un ordre qui élimine les sommes de Newton, c'est-à-dire Π_1, Π_2, Π_5, Σ_4, Σ_7 et Π_6 (par exemple un ordre lexicographique). On obtient par GB une base standard puis l' ensemble triangulaire suivant (où `ti` désigne Π_i, et `si` désigne Σ_i) :

```
[[s12, s11, s10, s9, s8, 624*s6 + t2**5 + 2016*t2**2, 936*s5 - t2**5 - 2016*t2**2,
s3, s2, 624*t4 + t2**4 + 2328*t2, 1248*t6  - t2**6 - 2328*t2**3 + 7488, s7,
936*s4 - t2**5 -2484*t2**2, t5, t2**7 + 2160*t2**4 -1728*t2, t3, t1],
 [s12 -2970*t5, s11 + 480*t2, 36*s10  - t5*t2**2, 72*s9 + 11*t5*t2**2,
s8 -144, 18*s6  - t2**2, 9*s5 + t2**2, 2*s3 + t5, 4*s2 + t5, 3*t4 + t2,
t6 -2706, 6*s7 -5*t5*t2, 18*s4 -11*t2**2, t5**2 -2304, t2**3 -5832, t3, t1]].
```

On obtient ainsi différentes valeurs possibles pour les sommes de Newton Π_1, Π_2, Π_5, Σ_4, Σ_7 et Π_6, d'où par les formules de Newton différentes valeurs pour les polynômes symétriques élémentaires. L'application du Théorème 10.9 nous donne alors immédiatement les 156 solutions du système (S_6), qui ont déjà été indiquées au paragraphe 10.7.6.

La résolution du système (S_6) avec cette méthode a pris 29 secondes, en utilisant GB pour calculer la base standard du système intermédiaire, sur la machine Jules (PC bi-Pentium Pro 200 Mhz) du GDR MEDICIS. À titre de comparaison, GB appliqué directement sur le système initial (S_6) (sans utiliser les symétries) met 5 h 20 min sur Jules de MEDICIS. Mais le précalcul des invariants fondamentaux de $\mathfrak{D}_6$ et de leurs syzygies, dont on a besoin pour la première méthode mais qui est fait une seule fois pour toutes, aura pris auparavant 3 h 50 min en MAGMA sur la machine Anne de MEDICIS (Dec Alpha EV5 400 MHz).

Pour ce qui concerne le système aux racines cycliques septièmes, MAGMA sur Anne de MEDICIS n'est pas encore parvenu à calculer les syzygies de plus haut degré entre les 48 invariants secondaires de $\mathfrak{D}_7$, et nous ne pouvons donc pas encore commencer la résolution rapide de ce système.

Annexe D

Notations

Groupe	Ordre	Nom	Description	Famille génératrice dans $\mathfrak{S}_n$
$\mathfrak{S}_n$	$n!$	groupe symétrique sur n éléments	groupe des permutations de l'ensemble $\mathbb{N}_n^* = \{1, \ldots, n\}$	$\{(1,2), (1,2,\ldots,n)\}$
$\mathfrak{A}_n$ $(n \geq 2)$	$n!/2$	groupe alterné sur n éléments	sous-groupe de $\mathfrak{S}_n$ composé des permutations paires	$\{(1,2,i)/i \in \{3,\ldots,n\}\}$
$\mathfrak{D}_n$	$2n$	groupe diédral sur n éléments	sous-groupe de $\mathfrak{S}_n$ constitué des permutations des n sommets d'un polygône régulier qui peuvent se prolonger en une isométrie du plan	$\{(1,2,\ldots,n), \prod_{i=1}^{[n/2]}(i, n+1-i)\}$
$\mathfrak{C}_n$	n	groupe cyclique sur n éléments	sous-groupe de $\mathfrak{S}_n$ constitué des permutations des n sommets d'un polygône régulier qui peuvent se prolonger en une rotation du plan	$\{(1,2,\ldots,n)\}$
$\mathfrak{M}_n$ n premier impair	$n(n-1)$	groupe métacyclique principal sur n éléments	Groupe des similitudes $[x \mapsto ax+b]$, $(a,b) \in \mathbb{F}_n^* \times \mathbb{F}_n$ du corps $\mathbb{F}_n$. Il est produit semi-direct du sous-groupe des rotations par celui des translations. Plus généralement, un *groupe métacyclique* est un groupe fini G admettant un sous-groupe distingué C tel que C et G/C soient cycliques (voir [7]).	$\{(1,2,\ldots,n), (\alpha_1,\ldots,\alpha_{n-1})\}$ où $\alpha_i - 1$ est le reste modulo n de 2^i

Les permutations seront notées par leur décomposition en cycles à supports deux à deux disjoints. On désigne un sous-groupe de $\mathfrak{S}_n$ par ses générateurs entre crochets. Ainsi, $G =< (1\ 4)(2\ 3), (1\ 2) >$ désigne le sous-groupe de $\mathfrak{S}_4$ engendré par les permutations $(1\ 4)(2\ 3)$ et $(1\ 2)$ (on a $G \simeq \mathfrak{D}_4$).

Notation	Définition	Référ.
$E_1, \ldots, E_n$	polynômes symétriques élémentaires en $X_1, \ldots, X_n$	
$\mathbf{GL}_n(k)$	groupe général linéaire sur le corps k	
$[K : k]$	degré de l'extension de corps $K : k$	
$\mathrm{Gal}(K : k)$	groupe de Galois de l'extension de corps $K : k$	§ 1.1
$\mathrm{Gal}_k(f)$	groupe de Galois du polynôme f sur le corps k	§ 6.1
$\mathcal{S}tab_G(x)$	stabilisateur de x dans le groupe G	§ 1.1
$\mathcal{O}rb_G(x) = G.x$	orbite de x sous l'action de G	§ 1.1
$\mathcal{R}\mathrm{es}(P, Q)$	résultant des polynômes P et Q à une indéterminée	
$\mathcal{R}\mathrm{es}_X(P, Q)$	résultant des polynômes P et Q par rapport à l'indéterminée X (quand P et Q sont des polynômes à plusieurs indéterminées). Cela veut dire que l'on considère que les autres indéterminées appartiennent à l'anneau des coefficients de P et Q. Autrement dit, c'est X qui est éliminée.	
$\mathcal{L}_\Psi$	résolvante absolue générique de Ψ	Déf. 6.1
$\mathcal{L}_\Psi^L$	résolvante générique de Ψ relative à L	Déf. 6.1
$\mathcal{L}_{\Psi,f}$	résolvante absolue de Ψ spécialisée en f	Re. 6.4
$\mathcal{L}_{\Psi,\mathbf{x}}^L$	résolvante de Ψ relative à L spécialisée en la famille $\mathbf{x}$ des racines d'un polynôme	Déf. 6.3
$(L/H)_g$	ensemble des classes à gauche dans le groupe L de son sous-groupe H	
$(L//H)_g$	transversale gauche, ou famille de représentants des classes à gauche de H dans L ; *i.e.* ensemble de cardinal $[L : H]$ qui contient un et un seul élément de chaque classe à gauche	
$[L : H]$	indice dans le groupe L de son sous-groupe H	
$\lvert H\rvert = \mathrm{Card}(H)$	cardinal de l'ensemble H, ou ordre du groupe fini H	
$[H]_L$	classe de conjugaison dans le groupe L de son sous-groupe H	§ 6.1
$\mathbb{N}$	ensemble des entiers naturels	
$\mathbb{N}^*$	ensemble des entiers naturels non-nuls	
$\mathbb{N}_n$	ensemble $\{0, 1, \ldots, n\}$	
$\mathbb{N}_n^*$	ensemble $\{1, 2, \ldots, n\}$	
$\mathbb{Z}$	ensemble des entiers	
$\mathbb{Q}$	ensemble des rationnels	
$\mathbb{R}$	ensemble des réels	
$\mathbb{C}$	ensemble des complexes	
$\mathbb{F}_{p^\alpha}$	corps fini à p^α éléments, p nombre premier	
$\widetilde{P}$	valeur spécialisée $P(x_1, \ldots, x_n)$ du polynôme $P \in k[X_1, \ldots, X_n]$ en les scalaires $x_1, \ldots, x_n$ (absents dans la notation, ils doivent être évidents dans le contexte)	

Bibliographie

[1] *MAGMA V.2.1*, Université de Sydney, school of mathematics and statistics éd.

[2] *Maple V, Language reference manual*, London, Springer Verlag éd., 1991.

[3] H. Anai, M. Noro, et K. Yokoyama, « *Computation of the splitting fields and the Galois groups of polynomials* », dans *Algorithms in Algebraic Geometry and Applications*, 1996, p. 29–50.

[4] J.-M. Arnaudiès, « *Sur la résolution explicite des équations de degré 5, quand elles sont résolubles par radicaux* », dans *Bull. Sc. Math. 2^e série*, vol. 100, 1976, p. 241–254.

[5] J.-M. Arnaudiès, *Algèbres trigonales, fonctions de Moebius et polynômes symétriques.* prépublication LITP 92.86, Univ. Paris 6.

[6] J.-M. Arnaudiès, *Groupes, Algèbres et Géométrie*, Ellipses, 1993.

[7] J.-M. Arnaudiès et A. Valibouze, « *Résolvantes de Lagrange* », dans *Journal of Pure and Applied Algebra*, vol. 117-118, 1996, p. 23–40.

[8] J. Backelin et R. Fröberg, « *How we proved that there are exactly 924 cyclic 7-roots* », dans *Proceedings of ISSAC'91*, New-York, ACM, 1991, p. 103–111.

[9] C. Batut, D. Bernardi, H. Cohen, et M. Olivier, *GP/PARI CALCULATOR*, Université de Bordeaux 1, 1989-1995.

[10] E. Berwick, « *The condition that a quintic equation should be soluble by radicals* », dans *Proc. London Math. Soc.*, vol. 2 n° 14, 1915, p. 301–307.

[11] E. Berwick, « *On soluble sextic equations* », dans *Proc. London Math. Soc.*, vol. 2 n° 29, 1929, p. 1–28.

[12] G. Björck et R. Fröberg, « *A Faster Way to Count the Solutions of Inhomogeneous Systems of Algebraic Equations, with Applications to Cyclic n-roots* », dans *Journal of Symbolic Computation*, vol. 12, 1991, p. 329–336.

[13] N. Bourbaki, *Éléments de Mathématiques*, Paris, Masson, 1991.

[14] G. Butler et J. McKay, « *The transitive groups of degree up to eleven* », dans *Comm. Algebra*, vol. 11, 1983, p. 863–911.

[15] D. Casperson, D. Ford, et J. McKay, « *Ideal decompositions and subfields* », dans *J. Symbolic Computation*, 1996.

[16] C. Chevalley, « *Invariants of finite groups generated by reflections* », dans *American Journal of Mathematics*, vol. 77, 1955, p. 778–782.

[17] A. Colin, « *Formal Computation of Galois Groups with Relative Resolvents* », dans G. Cohen, M. Giusti, et T. Mora (éds.), *proc. AAECC'95, Lecture Notes in Computer Science*, vol. 948, Springer Verlag, 1995, p. 169–182, aussi Note Informelle de Calcul Formel 95-07, 1995, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/95nouvelles.html`.

[18] A. Colin, « *Relative resolvents and partition tables in Galois group computations* », dans O. Gloor (éd.), *Proc. ISSAC'97*, ACM, 1997. aussi Note Informelle de Calcul Formel 97-02, 1997, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/97nouvelles.html`.

[19] A. Colin, « *Solving a System of Algebraic Equations with Symmetries* », dans *Journal of Pure and Applied Algebra*, vol. 117-118, 1997, p. 195–215. aussi Note Informelle de Calcul Formel 96-04, 1996, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/96nouvelles.html`.

[20] D. Cox, J. Little, et D. O'Shea, *Ideals, Varieties, and Algorithms*, New-York, Springer, 1992.

[21] Y. Eichenlaub, *Problèmes effectifs de théorie de Galois en degrés 8 à 11*, Thèse, Université de Bordeaux 1, 1996.

[22] Y. Eichenlaub et M. Olivier, *Computation of Galois groups for polynomials with degree up to eleven*, prépublication, Université de Bordeaux 1, 1995.

[23] J.-C. Faugère, *GB Version 3.0*, LIP6, Université de Paris 6, 1994.

[24] K. Gatermann, « *Symbolic solution of polynomial equation systems with symmetry* », dans M. N. S. Watanabe (éd.), *proc. ISSAC'90*, New-York, ACM, 1990.

[25] K. Gatermann, « *Semi-Invariants, equivariants and algorithms* », dans *AAECC*, vol. 7, 1996, p. 105–124.

[26] I. Gelfand, M. Kapranov, et A. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Berlin, Birkhäuser, 1994.

[27] H. Geyer, *Programme zur Berechnung der Galoisgruppen von Polynomen 8. und 9. Grades Dokumentation*. Prépublication 93.10, Université de Heidelberg.

[28] I. Gil-Delessalle et A. Valibouze, *Galois inverse problem for some subgroups of degree 12*. Prépublication LITP, Université de Paris 6.

[29] K. Girstmair, « *On Invariant Polynomials and their Application in Field Theory* », dans *Maths of Comp.*, vol. 48 n° 178, 1987, p. 781–797.

[30] M. Giusti et J. Heintz, « *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial* », dans *Proc. Intern. Meeting on Commutative Algebra, Cortona*, Cambridge University Press, 1991.

[31] M. Giusti, J. Heintz, K. Hägele, J. Morais, L. Pardo, et J. Montaña, « *Lower bounds for diophantine approximations* », dans *Journal of Pure and Applied Algebra*, vol. 117 et 118, 1997, p. 277–317. Aussi Note Informelle de Calcul Formel 96-08, 1996, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/96nouvelles.html`.

[32] M. Giusti, J. Heintz, J. Morais, et L. M. Pardo, « *When polynomial equations can be "solved" fast ?* », dans G. Cohen, M. Giusti, et T. Mora (éds.), *proc. AAECC'95, Lecture Notes in Computer Science*, vol. 948, Springer, 1995, p. 169–182, aussi Note Informelle de Calcul Formel 95-10, 1995, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/95nouvelles.html`.

[33] M. Giusti, J. Heintz, J. E. Morais, et L. M. Pardo, « *Le rôle des structures de données dans les problèmes d'élimination* », dans *Note au Compte-Rendu de l'Académie des Sciences*, 1997. Aussi Note Informelle de Calcul Formel 97-01, 1997, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/97nouvelles.html`.

[34] M. Giusti, D. Lazard, et A. Valibouze, « *Algebraic transformations of polynomial equations, symmetric polynomials and elimination* », dans P. Gianni (éd.), *Proc. ISSAC'88*, vol. 358 de *LNCS*, 1988, p. 309–314.

[35] M. Göbel, « *Computing bases for rings of permutation-invariant polynomials* », dans *J. Symbolic Computation*, vol. 19, 1995, p. 285–291.

[36] A. Hulpke, « *Block Systems of a Galois Group* », dans *Experimental Mathematics*, vol. 4 n° 1, 1995.

[37] R. D. Jenks et R. S. Sutor, *AXIOM 2.1, The Scientific Computation System*, NAG, New-York, 1992.

[38] G. Kemper, *Das Noethersche Problem und generische Polynome*, Thèse, Universität Heidelberg, 1994.

[39] G. Kemper, *The Invar package for calculating rings of invariants.* IWR Prépublication **93-34**, Heidelberg.

[40] G. Kemper, « *Calculating Invariant Rings of Finite Groups over Arbitray Fields* », dans *J. Symbolic Computation*, vol. 21, 1996, p. 351–366.

[41] G. Kemper, *Calculating Optimal Homogeneous Systems of Parameters.* IWR Prépublication **97-08**, Heidelberg.

[42] J. Klüners, « *On polynomial decompositions* », dans *J. Symbolic Computation*, 1997.

[43] J. Lagarias et A. Odlyzko, « *Effective versions of the Tchebotarev density theorem* », dans A. Frölich (éd.), *Algebraic Number Fields (L-functions and Galois properties)*, Academic Press, 1977, p. 409–464.

[44] J.-L. de Lagrange, *Réflexions sur la résolution algébrique des équations*, Prussian Academy, 1770.

[45] J.-L. de Lagrange, *Réflexions sur la résolution algébrique des équations*, Mémoires de l'Académie de Berlin, 1770, vol. IV, ch. Œuvres de Lagrange, p. 205–421.

[46] J.-L. de Lagrange, *Traité de la résolution des équations numériques*, Oeuvres de Lagrange, 1770, vol. VIII, ch. Notes sur la théorie des équations algébriques, p. 133–367.

[47] A. Lascoux et M. Schützenberger, *Formulaire raisonné des fonctions symétriques.* prépublication LITP UER Math, L.A. 248, Paris 7, 1985.

[48] D. Lazard, Private communication, december 1995.

[49] F. Lehobey, « *Resolvent Computations by Resultants Without Extraneous Powers* », dans *Proceedings of ISSAC'97*, (ACM), 1997.

[50] A. Mattuck, « *The Field of multisymmetric functions* », dans *Proceedings of the American Mathematical Society*, vol. 19, 1968, p. 764–765.

[51] B. H. Matzat, *Konstruktive Galoistheorie*, Springer-Verlag, 1987.

[52] J. McKay et L. Soicher, « *Computing Galois groups over the rationals* », dans *Journal of Number Theory*, vol. 20, 1985, p. 273–281.

[53] T. Miyata, « *Invariants of Certain Groups I* », dans *Nagoya Math. J.*, vol. 41, 69-73.

[54] T. Molien, « *Über die Invarianten der linearen Substitutionsgruppe* », dans *Sitzungsber. Königl. Preuss. Akad. Wiss.*, 1897, p. 1152–1156.

[55] V. Noonburg, « *A Neural Network Modeled by an Adaptive Lotka-Volterra System* », dans *SIAM J. Appl. Math.*, vol. 49 n° 6, 1989, p. 1779–1792.

[56] F. Ollivier, *Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*, Thèse, École polytechnique, France, juin 1990.

[57] N. Rennert et A. Valibouze, *Modules de Cauchy, polynômes caractéristiques et résolvantes.* Soumis à Exp. Math, extrait du rapport LITP 95-62, 1995.

[58] M. Schönert, *Groups, Algorithms and Programming (GAP)*, RWTH, Aachen, Lehrstuhl D für Mathematik éd., 1992.

[59] L. Soicher, *The Computation of Galois Groups*, Thèse, Concordia University, Montreal, April 1981.

[60] R. Stanley, « *Invariants of finite groups and their applications to combinatorics* », dans *Bull. Amer. Society*, vol. 3, 1979, p. 475–511.

[61] R.-P. Stauduhar, « *The Computation of Galois Groups* », dans *Math. Comp.*, vol. 27, 1973, p. 981–996.

[62] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, 1993.

[63] N. Tchebotareff, « *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören* », dans *Math. Annalen*, vol. 95, 1925, p. 191–228.

[64] A. Valibouze, *Cours de théorie de Galois.* Cours effectué à l'université de Pise, 1997.

[65] A. Valibouze, *Galois groups of all polynomials with applications up to degree 7.* prépublication, 1997.

[66] A. Valibouze, *Manipulation des fonctions symétriques*, Thèse, Université de Paris 6, 1986.

[67] A. Valibouze, « ***SYM**, Symbolic computation with symmetric polynomials, an extension to Macsyma* », dans *proc. Computers and Mathematics*, (MIT), Cambridge, Mass., Springer, 1989, p. 308–320.

[68] A. Valibouze, *Résolvantes et groupe de Galois d'un polynôme.* Prépublication, Paris.

[69] A. Valibouze, Théorie de Galois constructive, Université de Paris 6, December 1994. Mémoire d'habilitation.

[70] A. Valibouze, « *Computation of the Galois Groups of the Resolvent Factors for the Direct and Inverse Galois Problems* », dans G. Cohen, M. Giusti, et T. Mora (éds.), *proc. AAECC'95, Lecture Notes in Computer Science*, vol. 948, Springer Verlag, 1995, p. 456–468, aussi Note Informelle de Calcul Formel 95-09, 1995, disponible à l'adresse électronique `http://medicis.polytechnique.fr/gage/notes/95nouvelles.html`.

[71] J. Verschelde et K. Gatermann, « *Symmetric Newton Polytopes for Solving Sparse Polynomial Systems* », dans *Advances in Applied Mathematics*, vol. 16, 1995, p. 95–127.

[72] P. A. Worfolk, « *Zeros of equivariant vector fields: Algorithms for an invariant approach* », dans *Journal of Symbolic Computation*, vol. 17, 1994, p. 487–511.

[73] K. Yokoyama, « *A modular method for computing the Galois groups of polynomials* », dans *Journal of Pure and Applied Algebra*, vol. 117-118, 1997.