Solving zero-dimensional structured polynomial systems

Jules Svartz

UNIVERSITÉ PIERRE ET MARIE CURIE - PARIS 6

ÉCOLE DOCTORALE EDITE

T H È S E

pour obtenir le titre de

Docteur en Sciences

de l'Université Pierre et Marie Curie - Paris 6
Mention : Informatique

Présentée par

Jules Svartz

Résolution de Systèmes Polynomiaux Structurés de Dimension Zéro

Algorithmes et Complexité

Thèse dirigée par Jean-Charles Faugère
préparée au Laboratoire d'Informatique de Paris 6 (UPMC)

Soutenue le 30 octobre 2014 après avis des rapporteurs :

Marc Giusti	-	Directeur de Recherche CNRS, LIX
Bernard Mourrain	-	Directeur de Recherche INRIA, INRIA Sophia Antipolis

devant le jury composé de :

Jean-Charles Faugère	-	Directeur de Recherche INRIA, CRI Paris-Rocquencourt
Marc Giusti	-	Directeur de Recherche CNRS, LIX
Bernard Mourrain	-	Directeur de Recherche INRIA, INRIA Sophia Antipolis
Mohab Safey El Din	-	Professeur, Université Pierre et Marie Curie
Bruno Salvy	-	Directeur de Recherche INRIA, ENS Lyon
Pierre-Jean Spaenlehauer	-	Chargé de Recherche INRIA, LORIA

Résumé

Les systèmes polynomiaux à plusieurs variables apparaissent naturellement dans de nombreux domaines scientifiques. Ces systèmes issus d'applications possèdent une structure algébrique spécifique. Une méthode classique pour résoudre des systèmes polynomiaux repose sur le calcul d'une base de Gröbner de l'idéal associé au système. Cette thèse présente de nouveaux outils pour la résolution de tels systèmes structurés, lorsque la structure est induite par l'action d'un groupe ou une structure monomiale particulière, qui englobent les systèmes multi-homogènes ou quasi-homogènes.
D'une part, cette thèse propose de nouveaux algorithmes qui exploitent ces structures algébriques pour améliorer l'efficacité de la résolution de systèmes (systèmes invariant sous l'action d'un groupe ou à support dans un ensemble de monômes particuliers). Ces techniques permettent notamment de résoudre un problème issu de la physique pour des instances hors de portée jusqu'à présent.
D'autre part, ces outils permettent d'améliorer les bornes de complexité de résolution de plusieurs familles de systèmes polynomiaux structurés (systèmes globalement invariant sous l'action d'un groupe abélien, individuellement invariant sous l'action d'un groupe quelconque, ou ayant leur support dans un même polytope). Ceci permet en particulier d'étendre des résultats connus sur les systèmes bilinéaires aux systèmes mutli-homogènes généraux.

Abstract

Multivariate polynomial systems arise naturally in many scientific fields. These systems coming from applications often carry a specific algebraic structure. A classical method for solving polynomial systems is based on the computation of a Gröbner basis of the ideal associated to the system. This thesis presents new tools for solving such structured systems, where the structure is induced by the action of a particular group or a monomial structure, which include multihomogeneous or quasihomogeneous systems.
On the one hand, this thesis proposes new algorithms using these algebraic structures to improve the efficiency of solving such systems (invariant under the action of a group or having a support in a particular set of monomials). These techniques allow to solve a problem arising in physics for instances out of reach until now.
On the other hand, these tools improve the complexity bounds for solving several families of structured polynomial systems (systems globally invariant under the action of an abelian group or with their support in the same polytope). This allows in particular to extend known results on bilinear systems to general mutlihomogeneous systems.

Contents

Introduction

Problématique.

La résolution effective de systèmes algébriques est un problème central en calcul formel, notamment vis à vis de son vaste champ d'applications. De tels systèmes apparaissent par exemple dans des domaines aussi variés que les sciences physiques et biologiques, la théorie des jeux, la théorie du contrôle ou la géométrie.

Si les propriétés théoriques des systèmes algébriques ont été étudiées depuis les dix-huitième et dix-neuvième siècles avec les travaux de Bézout, Hilbert, Noether ou Sylvester, c'est Macaulay qui le premier donne une méthode pour déterminer *effectivement* si un système algébrique homogène possède une solution non triviale, à l'aide du résultant multivarié. Il faut attendre les années 1960 pour qu'Hironaka et Buchberger définissent indépendamment le concept de base de Gröbner. C'est d'ailleurs dans sa thèse [14] que Buchberger donne le premier algorithme pour calculer une telle base.

Depuis, la théorie des bases de Gröbner a été intensément étudiée, du fait de l'augmentation croissante de la puissance de calcul des ordinateurs. En particulier, Lazard montre en 1983 [71] les connexions entre le calcul de bases de Gröbner et l'élimination Gaussienne. Faugère [34] propose en 1999 une version de l'algorithme de Buchberger où les choix de paires critiques et de polynômes réducteurs sont remplacés par de l'algèbre linéaire. En 2002, il propose le premier algorithme [35] basé sur la notion de *signature*. Ces deux algorithmes sont de nos jours parmi les plus utilisés pour résoudre de manière *certifiée* un système algébrique.

Du point de vue de la complexité, le problème de la résolution d'un système polynomial sur un corps fini est NP-difficile : la borne de Bézout établit qu'un système *générique* de n polynômes de degrés $d_1, \ldots, d_n$ en n variables possède $\prod_{i=1}^{n} d_i$ solutions dans un corps algébriquement clos. Si aucun des polynômes n'est linéaire, le nombre de solutions est donc exponentiel en le nombre de variables.

Les systèmes provenant d'applications pratiques sont algébriquement *structurés*, la structure étant liée à la formulation du problème originel. On peut alors essayer d'exploiter cette structure de différentes manières.

- Du point de vue du nombre de solutions, il se peut que celui d'un système structuré soit plus faible que pour un système générique.
- Du point de vue du *degré maximal* atteint lors du calcul d'une base de Gröbner pour un *ordre gradué*, celui-ci peut-être plus petit que celui-d'un système générique : la complexité de résoudre un tel système s'en trouve réduite.
- La structure peut permettre d'exprimer le système de façon plus compacte que la représentation dense en somme de monômes. La manipulation algorithmique des objets est donc facilitée, ce qui induit un gain en complexité.

Le sujet de cette thèse porte principalement sur l'étude et l'utilisation des structures induites par l'action d'un groupe fini (systèmes avec symétries), ou possédant une structure

monomiale particulière (principalement lorsque le support des polynômes du système est inclus dans un même polytope). Ces deux structures ne sont pas indépendantes : on verra qu'on peut se ramener de polynômes stables sous l'action d'un groupe abélien à des polynômes ayant peu de monômes. Le but de cette thèse est d'exploiter cette structure pour accélérer le processus de résolution.

Le problème POSSO.

Il est important de préciser ce que l'on entend par « résoudre un système polynomial ayant un nombre fini de solutions ».

Résolution d'équations polynomiales en une variable. Le but de cette thèse est de résoudre des systèmes polynomiaux de manière certifiée. Or, même pour des polynômes en une seule variable sur le corps $K = \mathbb{Q}$, il n'est pas possible d'exprimer les solutions de l'équation $P(x) = 0$ dans $\mathbb{C}$ par radicaux (ce n'est pas non plus souhaitable !), si le degré de P excède 4. Par conséquent, si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, le recours à l'approximation de racines est inévitable. Les techniques d'isolation de racines réelles et complexes forment un domaine de recherche à part entière, pour lesquelles on dispose d'algorithmes efficaces et certifiés. On pourra se référer par exemple à [82, 83, 84]. Dans le cas d'un polynôme en une variable sur un corps $\mathbb{K}$ fini, il est possible de décomposer le polynôme en facteurs irréductibles sur $\mathbb{K}$ à l'aide d'algorithmes spécifiques (voir par exemple l'algorithme de Cantor-Zassenhaus qu'on pourra trouver dans [107]), ce qui permet de donner une description des solutions dans $\mathbb{K}$ ou $\bar{\mathbb{K}}$.

Que ce soit sur un corps fini, sur $\mathbb{R}$ ou sur $\mathbb{C}$, le coût de ces algorithmes est en général négligeable devant le coût du calcul d'une base de Gröbner. Dans la suite on va se ramener systématiquement au cas de polynômes en une variable.

Base de Gröbner pour l'ordre lexicographique. Soit $\mathcal{I}$ un idéal de dimension zéro (ayant un nombre fini de solutions) dans une algèbre polynomiale $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. Alors la base de Gröbner réduite de $\mathcal{I}$ pour l'ordre lexicographique tel que $x_1 \succ \cdots \succ x_n$ a la forme suivante :

$$\mathcal{G}_{lex} = \left\{ \begin{array}{l} P_{1,1}(x_1, \ldots, x_n) \succ \cdots \succ P_{1,\ell_1}(x_1, \ldots, x_n) \succ \\ P_{2,1}(x_2, \ldots, x_n) \succ \cdots \succ P_{2,\ell_2}(x_1, \ldots, x_n) \succ \\ \vdots \\ P_{n-1,1}(x_{n-1}, x_n) \succ \cdots \succ P_{n-1,\ell_{n-1}}(x_1, \ldots, x_n) \succ \\ P_n(x_n) \end{array} \right\}$$

où les polynômes $P_{i,1}$ sont des polynômes unitaires (vus comme polynômes de $\mathbb{K}[x_{i+1}, \ldots, x_n][x_i]$), et le polynôme P_n appartient à $\mathbb{K}[x_n]$. En particulier, on s'aperçoit que la résolution d'un système peut-être obtenue en calculant une base de Gröbner lexicographique de l'idéal engendré par les polynômes du système, et utiliser ensuite les techniques décrites pour les polynômes d'une seule variable : on calcule d'abord les solutions du polynôme en la seule variable P_n, puis on reporte les racines dans les autres polynomes. On procède de même pour x_{n-1}, et ainsi de suite, de proche en proche.

Cette méthode a l'inconvénient de présenter une ambiguïté, car à chaque étape (excepté pour P_n), il faut calculer les racines communes à plusieurs polynômes en une seule variable. Cette ambiguïté peut-être levée en calculant au préalable une *décomposition en ensembles*

triangulaires de la base de Gröbner lexicographique. Pour ce faire, on peut utiliser l'algorithme de décomposition de Lazard [73].

Ainsi, le problème de résolution d'un système polynomial de dimension zéro est essentiellement résolu, dés lors qu'une base de Gröbner lexicographique de l'idéal engendré par les polynômes du système a été calculée.

Stratégie usuelle de résolution d'un système polynomial par calcul de bases de Gröbner. En général, le calcul direct d'une base de Gröbner lexicographique d'un idéal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ est difficile alors que le calcul d'une base de Gröbner pour un ordre *gradué* (et en particulier l'ordre DRL, ou grevlex, pour « *graded reversed lexicographical ordering* ») est beaucoup plus aisé. Puisque c'est une base de Gröbner lexicographique qui permet de se ramener à des polynômes en une seule variable, un algorithme de changement d'ordre est intéressant. Plusieurs algorithmes permettent de passer d'une base de Gröbner a une autre par changement d'ordre, dont l'algorithme Gröbner walk [24] qui peut-être appliqué quel que soit la dimension de l'idéal considéré. Lorsque l'idéal est de dimension zéro, il est certainement plus rapide d'utiliser l'algorithme FGLM [39], qui est essentiellement cubique en le nombre de solutions. La stratégie usuelle de résolution d'un système polynomial ayant un nombre fini de solutions à l'aide de techniques de bases de Gröbner est résumée en figure 0.1.

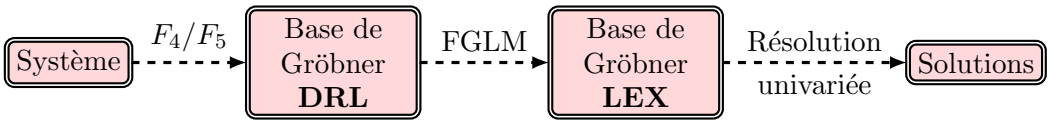


FIGURE 0.1 – Résolution de systèmes polynomiaux par bases de Gröbner.

Changements linéaires de variables « génériques ». Un idéal $\mathcal{I}$ de $\mathbb{K}[x_1, \ldots, x_n]$ de dimension zéro est dit en *shape position*, si sa base de Gröbner pour l'ordre lexicographique a la structure suivante :

$$\mathcal{G}_{lex} = \left\{ \begin{array}{c} x_1 - Q_1(x_n) \\ x_2 - Q_2(x_n) \\ \vdots \\ x_{n-1} - Q_{n-1}(x_n) \\ P_n(x_n) \end{array} \right\}$$

où les Q_i sont des polynômes de la seule variable x_n. L'ensemble des changements linéaires sur $\overline{\mathbb{K}}$ (correspondant aux matrices de $\mathcal{GL}_n(\overline{\mathbb{K}})$) qui mettent l'idéal en shape position forme un ouvert de Zariski non vide (on parle de propriété générique). Avant d'appliquer la stratégie de la figure 0.1, il est ainsi courant de procéder à un changement de variables aléatoire, ayant pour but de mettre l'idéal en shape position. Sous cette hypothèse, le changement d'ordre peut se faire en complexité sous-cubique, voir [38]. Beaucoup d'autres algorithmes de résolution de systèmes polynomiaux comprennent un ou plusieurs changement de variables aléatoires, voir plus bas.

Dans cette thèse, on s'intéresse aux systèmes structurés, possédant soit une structure monomiale particulière, soit une invariance sous l'action d'un groupe. Un changement linéaire de variables aléatoire a tendance à casser les structures monomiales et rendre moins visibles les symétries, c'est pourquoi on ne procèdera jamais à de tels changements. Pour traiter un

idéal invariant sous l'action d'un groupe abélien, on verra qu'au contraire, il est judicieux de procéder à un changement de variables particulier. De plus, si l'on utilise toute la structure du problème, on se retrouve heuristiquement en « shape position ».

D'autres approches pour résoudre un système polynomial. Dans cette thèse, on développe essentiellement des stratégies pour résoudre un système polynomial avec des bases de Gröbner. Ce n'est bien sûr pas la seule méthode possible pour résoudre un système. On présente ici les approches les plus classiques. Chacune possède ses spécificités propres, détaillées ci-dessous.

Algorithme de résolution géométrique. Soit $\mathsf{F} = (f_1, \ldots, f_n)$ une suite régulière dans un anneau de polynômes $\mathbb{K}[x_1, \ldots, x_n]$ avec $\mathbb{K}$ de caractéristique 0. Alors il est possible de calculer une *représentation rationnelle* des solutions du système en

$$O\left(n(nL + n^4)(\mathsf{M}(d\delta))^2\right)$$

opérations dans $\mathbb{K}$, où L est la taille maximale d'un programme en ligne directe [1] permettant d'évaluer les f_i, d est une borne sur le degré des f_i et δ est le maximum des degrés des idéaux intermédiaires $\langle f_1\rangle, \langle f_1, f_2\rangle, \ldots, \langle f_1, \ldots, f_{n-1}\rangle$, et $\mathsf{M}(\ell) = \ell \log(\ell)^2 \log\log(\ell)$. Cet algorithme probabiliste (il utilise des changements de variables génériques) a été présenté dans [53] et implémenté dans le package Magma Kronecker [2]. On peut étendre l'algorithme en rajoutant la condition $g(x_1, \ldots, x_n) \neq 0$ pour un certain polynôme g.

Résultant multivarié. Historiquement, les premières techniques *d'élimination* de variables utilisaient intensivement le résultant. Pour deux polynômes unitaires d'une variable z à coefficient dans un anneau intègre $\mathbb{A}$, on définit le résultant comme le déterminant de la *matrice de Sylvester* associée aux deux polynômes. Celui-ci s'annule si et seulement si les polynômes ont une racine commune dans $\overline{\mathrm{Frac}(\mathbb{A})}$. Le résultant multivarié est plus dur à définir et ne s'obtient pas aussi simplement qu'un déterminant. On réfère à [75, 19, 18, 15] pour plus de détails. Une variante du résultant pour l'étude de systèmes creux a également été proposée, voir [17, 31].

Méthodes homotopiques. Ces méthodes font partie de la grande famille des algorithmes *symboliques-numériques*. Pour calculer les solutions isolées d'un système polynomial sur $\mathbb{C}$, l'idée est de partir d'un système ayant même nombre de solutions et de le déformer progressivement pour revenir au système de départ. On calcule des solutions approchées des systèmes intermédiaires, et à la fin du processus on obtient une approximation des solutions cherchées. L'algorithme a été implémenté, voir PHCpack [105] [3] ou plus récemment Bertini[7] [4]. De nombreuses variantes existent, y compris pour traiter les systèmes creux, voir par exemple [106].

Solutions numériques. Des méthodes générales, comme la méthode de Newton-Raphston, peuvent s'appliquer en particulier à la résolution de systèmes polynomiaux sur $\mathbb{R}$ ou $\mathbb{C}$. La convergence vers une solution est quadratique, mais n'est que locale, et certaines solutions peuvent être oubliées...

1. l'auteur s'excuse de ne pas savoir traduire correctement « straight line program »...
2. disponible à l'adresse : `http://lecerf.perso.math.cnrs.fr/software/kronecker/distribution.html`
3. disponible à l'adresse : `http://homepages.math.uic.edu/~jan/`
4. disponible à l'adresse : `https://bertini.nd.edu/`

Systèmes présentant des symétries.

On commence ici par expliquer pourquoi il est intéressant d'avoir des algorithmes de résolution de systèmes tenant compte des symétries, et ce que l'on entend exactement par symétries.

Exemple 0.2.

Commençons par un exemple simple, en petite dimension. On souhaite déterminer les solutions réelles du système de deux équations en deux variables x et y suivant :

$$\left\{ \begin{array}{rcl} f(x,y) & = & x^2+y^2-2 \\ g(x,y) & = & x^3-6x^2y-3xy^2+2y^3+1 \end{array} \right. \begin{array}{l} = 0 \\ = 0 \end{array}$$

Ces deux polynômes sont tous deux invariants sous l'action d'une rotation planaire d'angle $2\pi/3$. En effet, en considérant

$$A = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$$

on observe que $f(x',y') = f(x,y)$ et $g(x',y') = g(x,y)$. Cette symétrie apparaît également sur les variétés réelles $\mathbb{V}_{\mathbb{R}}(f)$ et $\mathbb{V}_{\mathbb{R}}(g)$ représentées en figure 0.3.

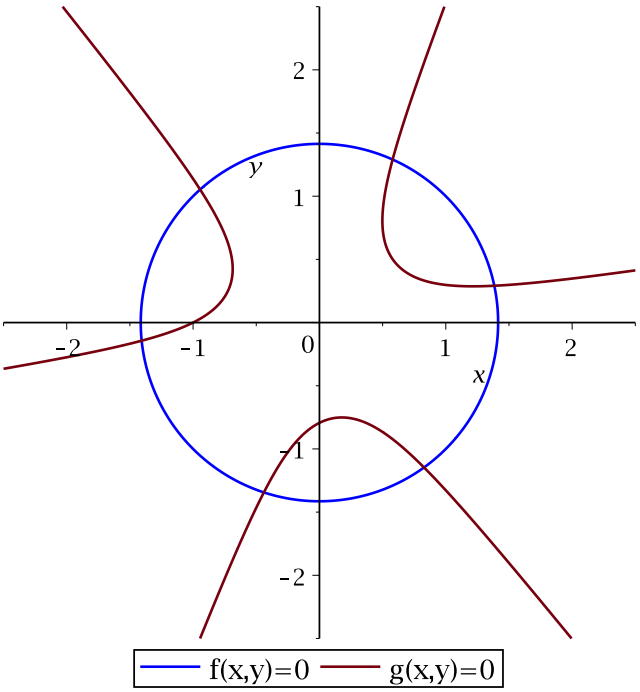


FIGURE 0.3 – Les variétés réelles associées à f et g.

Notons que la petitesse des degrés de f et g impose une symétrie supplémentaire (les variétés présentent trois axes de symétries), que nous ignorerons ici. L'ensemble des zéros communs à f est g est de cardinal 6, ce qui coïncide d'ailleurs avec la borne de Bézout. Pour calculer précisément les solutions, on peut éliminer l'une des variables, disons x. Pour ce faire,

on peut calculer un résultant par rapport à x ou une base de Gröbner lexicographique pour l'ordre $x > y$. L'idéal $\langle f, g\rangle \cap \mathbb{R}[y]$ contient un unique polynome unitaire, à savoir :

$$h(y) = y^6 - 3y^4 + \frac{1}{5}y^3 + \frac{9}{4}y^2 - \frac{3}{10}y - \frac{7}{80}$$

On a tracé en figure 0.4 le graphe de la fonction polynomiale associée à h. Si les deux po-

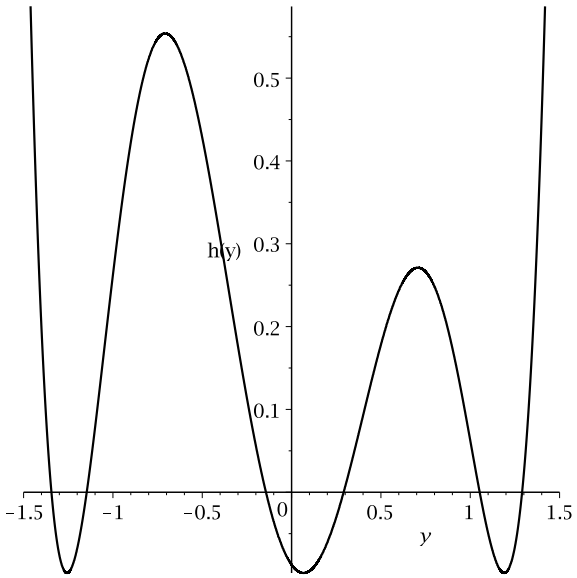


FIGURE 0.4 – Le graphe de la fonction polynomiale associée à h.

lynômes f et g présentaient une symétrie par rotations, ce n'est plus le cas du polynôme h. L'idée principale développée dans cette thèse est de conserver les symétries pour diminuer la complexité des calculs. On explique maintenant précisément ce que l'on entend par symétrie.

Que signifie « présenter des symétries » ? Un sous-groupe de $\mathcal{GL}_n(\mathbb{K})$ agit naturellement sur les espaces $\mathbb{K}^n$ et $\overline{\mathbb{K}}^n$. Il agit également sur $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ par l'action

$$\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) & \longrightarrow & \mathfrak{S}_{\mathbb{K}[X]} \\ A & \longmapsto & \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ f & \mapsto & f^A \end{array} \right. \end{array}$$

où f^A est déduit de f par substitution de AX à $X = {}^t(x_1, \ldots, x_n)$. Notons $\mathcal{I} = \{f_1, \ldots, f_s\}$ un idéal d'un anneau de polynômes $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$, et $\mathbb{V}_{\mathbb{K}}(\mathcal{I})$ la variété associée, sur $\mathbb{K}$. On note également $\overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$. Enfin, soit $\mathbf{G}$ un sous-groupe fini de $\mathcal{GL}_n(\mathbb{K})$. Les différents cas de symétries qui peuvent se présenter sont les suivants :

- **Variété stable.** Le groupe $\mathbf{G}$ agit naturellement sur l'espace affine associé à $\mathbb{K}^n$. La variété $\mathbb{V}_{\mathbb{K}}(\mathcal{I})$ est dite *globalement stable sous l'action de* $\mathbf{G}$ si

  $$\forall x \in \mathbb{V}_{\mathbb{K}}(\mathcal{I}) \quad \forall A \in \mathbf{G} \qquad A.x \in \mathbb{V}_{\mathbb{K}}(\mathcal{I})$$

  Puisqu'il n'y a aucune hypothèse algébrique sur l'action de $\mathbf{G}$ ici, tenir compte des symétries pour calculer $\mathbb{V}_{\mathbb{K}}(\mathcal{I})$ est très difficile. Par contre, si $\mathbb{K}$ et algébriquement

clos (ou si $\mathbb{V}_{\overline{\mathbb{K}}}(\mathcal{I})$ est globalement stable sous l'action de $\mathbf{G}$), le théorème des zéros de Hilbert (Nullstellensatz) prouve que pour tout polynôme f de $\mathcal{I}$ et tout élément A de $\mathbf{G}$, f^A appartient à $\sqrt{\mathcal{I}}$, dont la variété associée coïncide avec celle de $\mathcal{I}$. Par conséquent, le cas d'une variété stable peut se ramener au cas suivant.

- **Idéal stable.** L'idéal $\mathcal{I}$ est dit *globalement stable sous l'action de* $\mathbf{G}$ si

$$\forall f \in \mathcal{I} \quad \forall A \in \mathbf{G} \qquad f^A \in \mathcal{I}$$

Du point de vue des applications, ce cas est le plus important car celui qui apparaît le plus en pratique. Notons que, puisque $\mathbf{G}$ est fini, l'ensemble $\{f_i^A \mid 1 \leq i \leq s \text{ et } A \in \mathbf{G}\}$ est un ensemble fini de générateurs de $\mathcal{I}$ globalement stable sous l'action de $\mathbf{G}$. Ainsi, quite à augmenter artificiellement l'ensemble des générateurs de l'idéal, on pourra supposer avoir un ensemble stable de générateurs.

- **Équations semi-stables.** L'idéal $\mathcal{I}$ est dit engendré par des équations *individuellement* semi-invariantes si

$$\forall i \in \{1, \ldots, s\} \quad \forall A \in \mathbf{G} \qquad f_i^A = \xi_i f_i$$

où ξ_i est un scalaire pour tout i. La finitude du groupe $\mathbf{G}$ impose que ξ_i soit une racine de l'unité. Ce cadre est un cas particulier du précédent.

- **Équations stables.** L'idéal $\mathcal{I}$ est dit engendré par des équations *individuellement* invariantes si

$$\forall i \in \{1, \ldots, s\} \quad \forall A \in \mathbf{G} \qquad f_i^A = f_i$$

Ce cadre est un cas particulier du précédent. Puisque les polynômes sont individuellement stables sous l'action de $\mathbf{G}$, ils appartiennent à l'algèbre des invariants $\mathbb{K}[X]^{\mathbf{G}}$.

Dans l'exemple présenté plus haut, les deux polynômes f et g sont individuellement stables sous l'action du groupe $\mathbf{G}$ d'ordre 3 engendré par A.

On précise maintenant la distinction entre les symétries dans les cas modulaire et non-modulaire. L'action de $\mathbf{G}$ sur $\mathbb{K}[X]$ est dite modulaire si $\mathrm{char}(\mathbb{K})$, la caractéristique de $\mathbb{K}$, divise le cardinal de $\mathbf{G}$, et non-modulaire dans le cas contraire. De nombreux résultats valables dans le cas non-modulaires ne subsistent pas dans le cas modulaire. En particulier, la structure de l'algèbre des invariants $\mathbb{K}[X]^{\mathbf{G}}$ est beaucoup moins bien comprise dans le cas modulaire. Dans la suite, on fera explicitement mention des résultats qui subsistent dans le cas modulaires.

Lorsque les équations du systèmes sont individuellement invariantes sous l'action d'un groupe, il est naturel de travailler dans l'algèbre des invariants du groupe. On pourra par exemple se reporter à [100, 27] pour une étude de la structure de cette algèbre pour des groupes finis ou non. Le cas particulier de la reformulation de systèmes invariants à l'aide de *polynômes de Laurent* est traité dans [62, 59, 60]. Hubert et Labahn étendent également leur approche aux groupes abéliens finis [61].

Dans cette thèse, on s'intéresse aux systèmes invariants sous l'action d'un groupe fini. Dans [23], Colin montre comment on peut reformuler un tel système à l'aide de seulement n invariants polynomiaux (un ensemble d'invariants *primaires*) et un seul autre invariant secondaire, en payant le prix de se placer dans le cadre des *fractions rationnelles invariantes* plutôt que dans l'algèbre des polynômes invariants. Une autre approche pour résoudre un système formé de polynômes individuellement invariants sous l'action d'un sous-groupe du groupe symétrique a été développée par Faugère et Rahmany dans [41]. L'approche consiste à remplacer la notion de base de Gröbner d'un idéal par celle de base SAGBI dans l'algèbre des invariants. L'un des axes de cette thèse est d'étendre leurs résultats.

Concernant les idéaux globalement invariants sous l'action d'un groupe, Gatermann montre dans [51], comment la présence de *réflexions* dans le groupe permet de séparer le système en deux sous-systèmes. Elle montre également comment le fait de diagonaliser un groupe abélien fini permet d'accélérer le calcul d'une base de Gröbner d'un idéal invariant sous l'action du groupe. Cette approche a été reprise par Steidel [96]. Nous en déduirons des algorithmes dédiés et une estimation de complexité.

Exemple 0.5 (Suite de l'exemple 0.2)**.** *Pour l'exemple présenté ci-dessus, la matrice A se diagonalise de la façon suivante :*

$$A = PD_AP^{-1} \qquad avec \qquad D_A = \begin{pmatrix} \jmath & 0 \\ 0 & \jmath^2 \end{pmatrix} \quad et \quad P = \begin{pmatrix} 1 & 1 \\ \imath & -\imath \end{pmatrix} \quad où \quad \imath^2 = \jmath^3 = 1.$$

Appliquer le changement de variables P aux polynômes f et g donne les deux polynômes $f^P = 4xy - 2$ et $g^P = (-8\imath + 4)x^3 + (8\imath + 4)y^3 + 1$. Ces deux polynômes sont invariants sous l'action de la matrice diagonale D_A, par conséquent ils ne sont composés que de monômes m vérifiant $m^{D_A} = m$. Les polynômes intervenant lors du calcul de la base de Gröbner de f^P et g^P sont uniquement des polynômes semi-invariants *sous l'action du groupe $\mathbf{G}' = P^{-1}\mathbf{G}P$, ils sont donc très creux. En particulier, les bases de Gröbner pour les ordre DRL et lexicographique (avec $x \succ y$) de l'idéal $\langle f^P, g^P \rangle$ sont :*

$$\mathcal{G}_1 = \begin{cases} y^4 - \frac{1}{10}(3 + 4\imath)x^2 + \frac{1}{20}(1 - 2\imath)y \\ x^3 + \frac{1}{5}(-3 + 4\imath)y^3 + \frac{1}{20}(1 + 2\imath) \\ xy - \frac{1}{2} \end{cases} \quad et \quad \mathcal{G}_2 = \begin{cases} x + \frac{1}{5}(-12 + 16\imath)y^5 + \frac{1}{5}(1 + 2\imath)y^2 \\ y^6 + \frac{1}{20}(1 - 2\imath)y^3 - \frac{3}{40} + \frac{-\imath}{10} \end{cases}$$

Pour certains systèmes formant un idéal invariant sous l'action d'un groupe formé de matrices diagonales, le degré maximal atteint lors d'un calcul de base de Gröbner pour l'ordre DRL peut être plus faible que pour un système quelconque (ce n'est pas le cas dans l'exemple ci-dessus) : par exemple, un système d'équations quadratiques individuellement invariantes sous l'action du groupe cyclique est résoluble en temps polynomial en le nombre de variables. En essayant de déterminer précisément quels étaient ces systèmes, on s'est rendu compte que cette faiblesse du degré maximal atteint n'était pas dûe à l'action du groupe, mais au fait que les polynômes de tels systèmes n'ont pas une structure monomiale dense. On a donc été amené à travailler sur les systèmes ayant leurs monômes dans une sous-algèbre *monomiale* de $\mathbb{K}[X]$.

Systèmes polynomiaux creux.

On s'intéresse ici aux systèmes ayant leur support dans une sous-algèbre monomiale $\mathcal{A}$, strictement incluse dans $\mathbb{K}[X]$, qu'on appelera des « systèmes creux ». Cette dénomination regroupe de nombreuses structures ayant déja été étudiées, qu'on présente ici de manière non-exhaustive.

— Un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ est dit quasi-homogène pour un système de poids $(w_1, \ldots, w_n) \in \mathbb{N}^n$ si $f(x_1^{w_1}, \ldots, x_n^{w_n})$ est homogène. Dans [37], Faugère, Safey el Din et Verron développent une approche pour estimer la complexité de résolution d'un système composés de polynômes quasi-homogènes (pour un même système de poids), et donnent une algorithmique dédiée. Il existe un lien entre l'approche qu'ils proposent et l'étude de systèmes invariants sous-un groupe abélien, qu'on explicitera ultérieurement.

— Soit $X_1, \ldots, X_\ell$ une partition des variables $x_1, \ldots, x_n$, de taille $n_1, \ldots, n_\ell$. Un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ est dit multi-homogène de multidegré $(d_1, \ldots, d_\ell)$ par rapport à la partition $X_1, \ldots, X_\ell$, s'il vérifie

$$f(\lambda_1 X_1, \ldots, \lambda_\ell X_\ell) = \lambda_1^{d_1} \cdots \lambda_\ell^{d_\ell} f(X_1, \ldots, X_\ell) \qquad \text{pour tous } \lambda_1, \ldots, \lambda_\ell \in \mathbb{K}$$

Les systèmes bilinéaires (multi-homogènes de bidegré $(1,1)$ par rapport à une partition des variables en deux sous-ensembles) ont été étudiées par Faugère, Safey el Din et Spaenlehauer dans [36]. Dans cette article, ils montrent qu'un idéal $\mathcal{I}$ engendré par une suite *birégulière* $f_1, \ldots, f_s$ (voir [36, Définition 8]) de polynômes bilinéaires admet une bisérie de Hilbert de la forme suivante

$$\mathsf{HS}_{\mathcal{I}}(z_1, z_2) := \sum_{(\alpha,\beta)\in\mathbb{N}^2} \dim(\mathbb{K}[X]_{\alpha,\beta}/\mathcal{I}_{\alpha,\beta}) {z_1}^\alpha {z_2}^\beta = \frac{N_s(z_1, z_2)}{(1-z_1)^{n_x+1}(1-z_2)^{n_y+1}}$$

où n_x et n_y sont les tailles des deux blocs de variables, et N_s est un numérateur qu'ils donnent explicitement. La composante $\mathbb{K}[X]_{\alpha,\beta}$ (respectivement $\mathcal{I}_{\alpha,\beta}$) est celle des polynômes bihomogènes de bidegré (α, β) (respectivement des polynômes de $\mathcal{I}$ de bidegré (α, β)). Dans [45], les mêmes auteurs étendent leurs résultats aux systèmes bihomogènes de bidegrés $(D, 1)$, et appliquent leurs résultats à l'étude de systèmes déterminantiels.

Dans cette thèse, on s'intéressera aux systèmes d'équations polynomiales appartenant à une sous-algèbre de $\mathbb{K}[X]$, avec la contrainte de ne calculer que des polynômes de cette sous-algèbre.

Exemple 0.6 (Suite de l'exemple 0.5)**.** *Les polynômes f^P et g^P calculés précédemment appartiennent à la sous-algèbre $\mathbb{Q}[\imath][xy, x^3, y^3]$ de $\mathbb{Q}[\imath][x, y]$. En se restreignant à des calculs dans cette sous-algèbre, on obtient notamment les deux polynômes :*

$$\begin{cases} y^6 + \frac{1}{20}(1-2\imath)y^3 - \frac{3}{40} - \frac{\imath}{10} \\ xy - \frac{1}{2} \end{cases}$$

On obtient les solutions du système $f^P = g^P = 0$ en résolvant les deux équations précédentes (en les inconnues xy et y^3), puis en inversant l'application monomiale $(x, y) \mapsto (xy, y^3)$.

Travailler dans la sous-algèbre uniquement permet de donner un cadre unique pour ces systèmes creux, ainsi que d'autres. Si les polynômes sont à support dans un même *polytope*, on donne des bornes de complexité dépendant des propriétés combinatoires du polytope, qui permettent d'améliorer les complexités connues pour la résolution de systèmes bihomogènes, et se généralisent notamment à des systèmes multihomogènes.

Contributions.

On présente ici les principaux résultats de cette thèse. On commencera par décrire les nouveaux algorithmes, puis les résultats de complexité obtenus, et enfin les résultats obtenus en pratique. Les différents systèmes étudiés dans cette thèse sont résumés dans la figure 0.7.

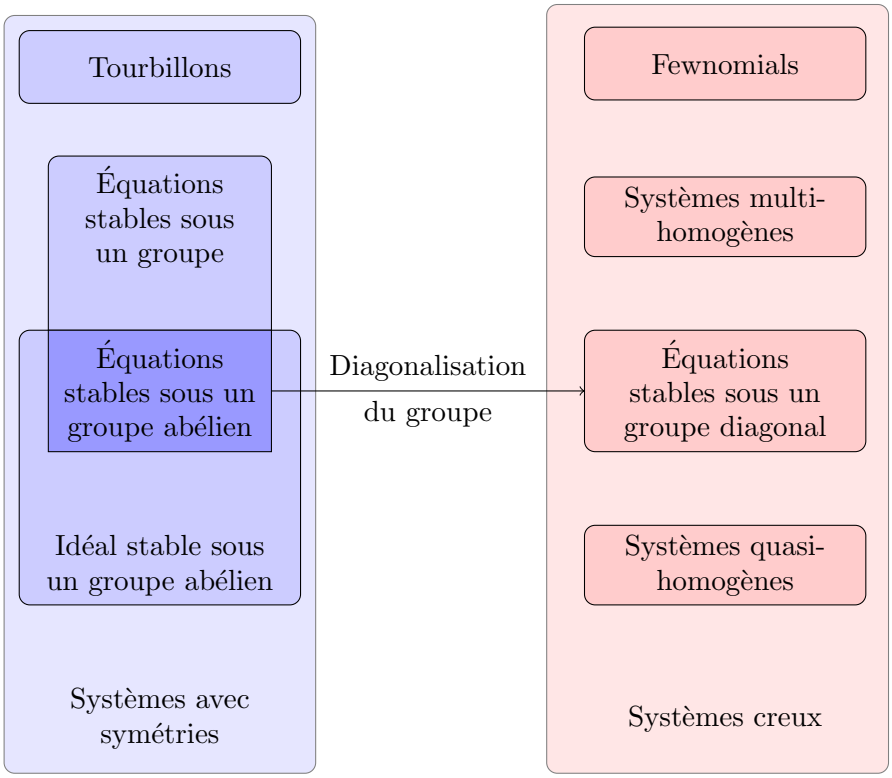


FIGURE 0.7 – Résumé des systèmes étudiés

Nouveaux algorithmes.

Un algorithme SAGBI-F_5 général. Dans cette thèse, on étend les algorithmes usuels de calcul d'une base de Gröbner dans un anneau de polynômes $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ à une sous algèbre graduée $\mathcal{A} = \oplus_{d=0}^{\infty} \mathcal{A}_d$ de $\mathbb{K}[X]$. Pour ce faire, la base canonique de $\mathbb{K}[X]_d$ formée des monômes de degré total d est remplacée par une base échelonnée $(b_i^d)_i$ de $\mathcal{A}_d$ (deux polynômes de la base n'ont pas même monôme de tête). Réécrire un polynôme f de $\mathcal{A}$ dans la base $\cup_{d=0}^{\infty}(b_i^d)$ de $\mathcal{A}$ permet d'avoir une représentation plus creuse, et effectuer des calculs uniquement dans $\mathcal{A}$ permet de garder cette représentation creuse.

Exemple 0.8. *Considérons l'exemple du système suivant, connu sous le nom de problème Cyclic-n.*

$$\begin{cases} f_1 &= x_1 + \cdots + x_n \\ f_2 &= x_1x_2 + x_2x_3 + \cdots + x_nx_1 \\ &\vdots \\ f_{n-1} &= x_1x_2\cdots x_{n-1} + \cdots + x_nx_1\cdots x_{n-2} \\ f_n &= x_1x_2\cdots x_n - 1 \end{cases}$$

invariant sous le groupe $\mathbf{G}$ *engendré par les matrices de permutation associées au cycle* $(1\ 2\ \cdots\ n)$ *et au produit de transposition* $(1\ n)(2\ (n-1))\cdots$. *Dans le cas non-modulaire, une base de* $\mathbb{K}[X]_d^{\mathbf{G}}$ *est donnée par* $\{\Re(m) \mid m \text{ monôme de degré } d\}$ *où* $\Re$ *est l'opérateur de moyenne sous l'action du groupe, défini par* $\Re(f) = \frac{1}{|\mathbf{G}|}\sum_{A\in\mathbf{G}} f^A$. *Ainsi, le système se*

reformule comme

$$\{f_i = \Re(x_1 \cdots x_i) \text{ pour } 1 \leq i \leq n-1 \text{ et } f_n = \Re(x_1 \cdots x_n) - \Re(1)\}$$

Revenons au cas général d'une sous algèbre $\mathcal{A}$. La notion de réduction (par rapport à un ordre $\preceq$ donné) du terme de tête est alors définie comme suit : f est réductible par $p \neq 0$ si il existe un élément b_i^d tel que le terme de tête de f s'écrive $\lambda b_i^d \mathsf{LT}_{\preceq}(p)$, où $\mathsf{LT}_{\preceq}(p)$ est le terme de tête de p. La réduction de f par p est alors le polynôme $f - \lambda b_i^d p$. Avec cette définition de réductibilité, la notion de base de Gröbner d'un idéal dans $\mathcal{A}$ est remplacée par celle de *base SAGBI*. On propose une variante de l'algorithme Matrix-F_5 permettant de calculer une base SAGBI d'un idéal $\langle f_1, \ldots, f_s \rangle_{\mathcal{A}}$ tronquée en un certain degré passé en paramètre. Une séquence de polynômes $(f_1, \ldots, f_s)$ est dite régulière dans $\mathcal{A}$ si f_i ne divise pas 0 dans l'anneau $\mathcal{A}/\langle f_1, \ldots, f_{i-1} \rangle$. L'algorithme SAGBI-$F_5$ ne produit aucune *réduction à zéro* si la suite $(f_1, \ldots, f_s)$ est régulière, car le *critère* F_5 s'étend facilement : les matrices construites sont de rang maximal.

Cet algorithme général peut-être utilisé dans plusieurs contextes, dépendant de l'algèbre $\mathcal{A}$ ambiante. Une spécialisation à $\mathcal{A} = \mathbb{K}[X]$ permet par exemple de retrouver l'algorithme Matrix-F_5 usuel. Deux autres cas sont étudiés dans cette thèse : $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$ est l'algèbre des invariants sous l'action d'un groupe fini $\mathbf{G}$, et $\mathcal{A} = \mathbb{K}[S]$ où S est un semi-groupe de $\mathbb{Z}^n$.

Processus de résolution d'un système d'équations individuellement invariantes sous l'action d'un groupe. Soit $\{f_1, \ldots, f_s\}$ un ensemble de polynômes appartenant à $\mathbb{K}[X]^{\mathbf{G}} = \mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$, où $\mathbf{G}$ est un sous-groupe fini de $\mathcal{GL}_n(\mathbb{K})$. On souhaite résoudre le système $\{f_1 = \cdots = f_s = 0\}$ en préservant la symétrie induite par le groupe $\mathbf{G}$. Le calcul d'une base de Gröbner de l'idéal engendré par les f_i dans $\mathbb{K}[X]$ détruirait cette symétrie, c'est pourquoi on calcule une base SAGBI de l'idéal $\mathcal{I}^{\mathbf{G}} = \langle f_1, \ldots, f_s \rangle_{\mathbb{K}[X]^{\mathbf{G}}}$ engendré par les f_i dans l'algèbre des invariants. Contrairement à une base de Gröbner, une base SAGBI n'est pas nécessairement finie, on ne peut donc obtenir qu'une base tronquée en un certain degré D. Cette base SAGBI permet de tester l'appartenance de polynômes de $\mathbb{K}[X]^{\mathbf{G}}$ à $\langle f_1, \ldots, f_s \rangle_{\mathbb{K}[X]^{\mathbf{G}}}$ de degré au plus D. On choisit donc un nombre fini d'invariants : par exemple si $\mathbf{G}$ est un sous-groupe du groupe symétrique (c'est le cas pour le système Cyclic-n présenté ci-dessus) on peut prendre comme invariants les fonctions symétriques élémentaires des x_i.

Notons $(h_1, \ldots, h_r)$ ces invariants. On cherche alors des combinaisons linéaires entre les produits $\prod_{i=1}^{r} h_i^{\alpha_i}$, modulo l'idéal $\mathcal{I}^{\mathbf{G}}$, ce qui mène à l'algorithme SAGBI-FGLM, qui est une variante de l'algorithme FGLM. Si le système a un nombre fini de solutions, on obtient pourvu que D soit assez grand, un idéal de dimension zéro dans l'algèbre $\mathbb{K}[H_1, \ldots, H_r]$, chaque H_i symbolisant l'invariant h_i. Le degré minimal D qui convient étant inconnu, on applique successivement deux étapes des algorithmes SAGBI-F_5 et SAGBI-FGLM jusqu'à obtenir un idéal de dimension zéro. Avec des invariants bien choisis, il est possible de remonter facilement de la variété associée à cet idéal aux solutions du système originel. Cette approche mène à la stratégie de résolution reproduite en figure 0.9.

Exemple 0.10 (Suite de l'exemple 0.8)**.** *On souhaite calculer les solutions du problème Cyclic-5 présenté plus haut, sur un corps $\mathbb{K}$ de caractéristique différente de 5. On prend comme invariants particuliers les fonctions symétriques élémentaires $(\sigma_i)_{1 \leq i \leq 5}$. Pour obtenir un idéal de dimension zéro dans $\mathbb{K}[\sigma_1, \ldots, \sigma_5]$, il est nécessaire d'avoir calculé une base SAGBI de $\mathcal{I}^{\mathbf{G}} = \langle f_1, \ldots, f_5 \rangle$ au moins jusqu'en degré 8 (ce degré est déterminé automatiquement lors du processus de résolution 0.9, il était inconnu initialement). L'idéal obtenu dans $\mathbb{K}[\sigma_1, \ldots, \sigma_5]$ est engendré par les polynômes suivants, de bas degrés :*

$$\left\{{\sigma_2}^3 + 5\,{\sigma_3}^2, {\sigma_2}^2\sigma_3 - 25\,\sigma_2, \sigma_2\,{\sigma_3}^2 - 25\,\sigma_3, \sigma_1, \sigma_4, \sigma_5 - 1\right\}$$

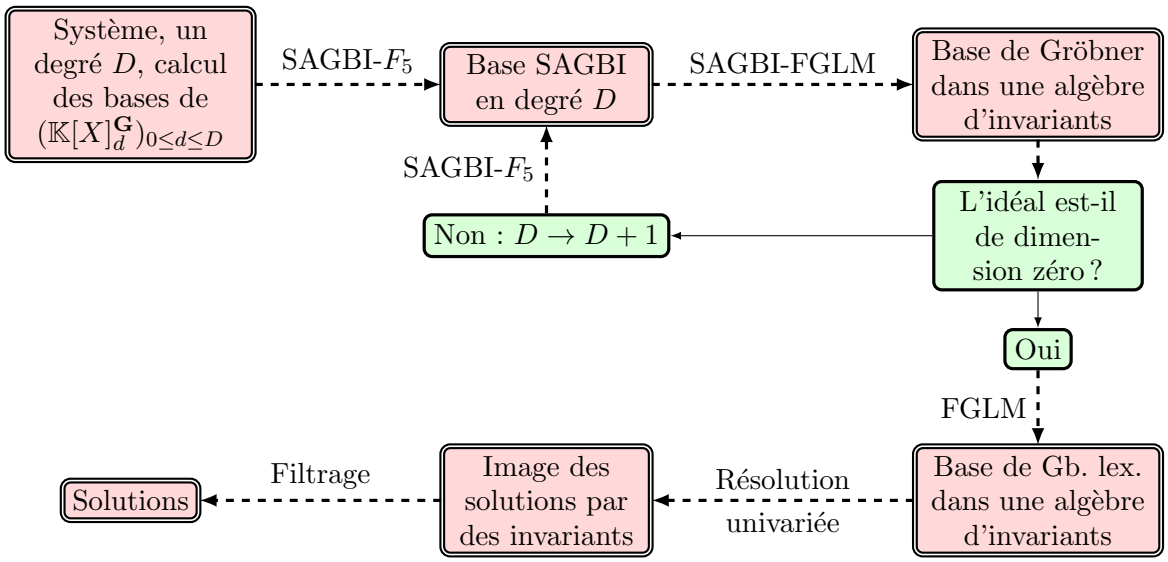


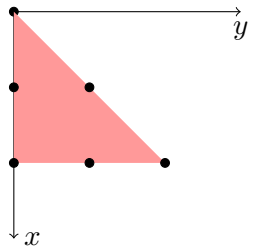
FIGURE 0.9 – Stratégie de résolution d'un système d'invariants sous l'action d'un groupe fini.

L'application de l'algorithme FGLM classique produit la base de Gröbner pour l'ordre lexicographique :

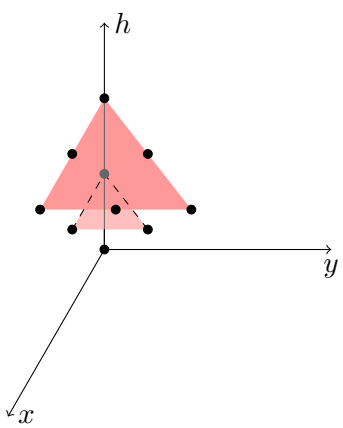
$$\left\{\sigma_5 - 1, \sigma_4, \sigma_3^6 + 5^5\,\sigma_3, 5^3\sigma_2 + \sigma_3^4, \sigma_1\right\}$$

La variété associée à l'idéal précédent ne contient que 6 points. Connaissant les fonctions symétriques des solutions, il est facile de remonter aux solutions elles-mêmes. Parmi les solutions possibles, seules 70 d'entre elles sont effectivement solutions du problème Cyclic-5.

Processus de résolution d'un système polynomial à support dans des multiples d'un même ensemble de monômes. Fixons un ensemble de monômes $\mathcal{M}$ de $\mathbb{K}[x_1, \ldots, x_n]$, qui s'identifie à un sous-ensemble de $\mathbb{N}^n$. À $\mathcal{M}$ on associe deux semi-groupes : l'un, S, est le semi-groupe engendré par $\mathcal{M}$ dans $\mathbb{N}^n$. L'autre, $S^{(h)}$ est généré par $\{(\alpha, 1) \in \mathbb{N}^{n+1} \mid \alpha \in M\}$ dans $\mathbb{N}^{n+1}$. On a représenté ci-dessous les deux semi-groupes pour $n = 2$, avec $\mathcal{M} = \{x, xy\}$.



Le semi-groupe S



Le semi-groupe $S^{(h)}$

À un semi-groupe S est associé une sous-algèbre de $\mathbb{K}[x_1, \ldots, x_n]$, appelée l'algèbre

du semi-groupe et notée $\mathbb{K}[S]$. Elle est définie comme l'espace vectoriel des sommes finies $\sum_{p\in S} a_p X^p$. L'algèbre $\mathbb{K}[S^h]$ est naturellement graduée par sa dernière composante. Dans l'exemple 0.6, on avait $\mathbb{Q}[\imath][S]$ générée par $\{xy, x^3, y^3\}$ et $\mathbb{Q}[\imath][S^{(h)}]$ généré par $\{h, xyh, x^3h, y^3h\}$.

On note $d\cdot\mathcal{M}$ l'ensemble $\{\prod_{i=1}^d m_i \mid m_i \in \mathcal{M}\}$, et on considère des polynômes $f_1,\dots,f_s$ tel que le support de f_i est inclus dans $d_i\cdot\mathcal{M}$. On dit que f_i est de degré d_i, et on lui associe un polynôme de $\mathbb{K}[S^h]$ noté $\tilde{f}_i$. L'algorithme SAGBI-F_5 présenté précedemment permet de calculer une base SAGBI jusqu'à un degré fixé de l'idéal engendré dans $\mathbb{K}[S^h]$ par $\tilde{f}_1,\dots,\tilde{f}_s$.

Exemple 0.11. *[Suite de l'exemple 0.6] La base de Gröbner creuse de $\widetilde{f^P}, \widetilde{g^P}$ dans $\mathbb{Q}[\imath][S^{(h)}]$ obtenue à l'aide de l'algorithme SAGBI-F_5 est :*

$$\widetilde{\mathcal{G}} = \begin{cases} h^3(x^6 + \frac{1}{100}(11-2\imath)y^3 + \frac{1}{400}(-27+36\imath)) \\ h^3(y^6 + \frac{1}{20}(1-2\imath)y^3 - \frac{3}{40} - \frac{\imath}{10}) \\ h^2(x^4y + \frac{1}{10}(-3-4\imath)y^3 + \frac{1}{40} + \frac{\imath}{20}) \\ h^2(xy^4 - \frac{1}{2}y^3) \\ h^2(x^3 + \frac{1}{5}(-3+4\imath)y^3 + \frac{1}{20} + \frac{\imath}{10}) \\ h(xy - \frac{1}{2}) \end{cases}$$

Une grande différence vis à vis des bases SAGBI dans les algèbres d'invariants est que les bases SAGBI dans $\mathbb{K}[S^h]$ sont finies, et on préfère les appeler bases de Gröbner creuses. De même, la mise en oeuvre de l'algorithme SAGBI-F_5 en pratique est également beaucoup plus aisée : les produits $b_i^d \times b_{i'}^{d'}$ sont beaucoup plus simples à calculer (ce sont des produits de monômes !), l'implémentation effective s'en trouve simplifiée. On lui donne donc le nom de Sparse-F_5.

La déshomogénéisation (oubli de la dernière composante des monômes de $\mathbb{K}[S^h]$) d'une base de Gröbner creuse donne une base de Gröbner creuse dans $\mathbb{K}[S]$, dans un sens défini dans le chapitre 5. Cette base de Gröbner permet en particulier de tester l'appartenance d'un polynôme à l'idéal $\langle f_1,\dots,f_s\rangle_{\mathbb{K}[S]}$.

La finitude de la base de Gröbner creuse permet de réaliser une variante de l'algorithme FGLM. Rappelons que pour la résolution d'un système d'invariants par base SAGBI, on fixe un ensemble d'invariants $h_1,\dots,h_r$ et on cherche les éléments de $\mathbb{K}[h_1,\dots,h_r]$ appartenant à l'idéal. On suit la même idée ici en considérant $h_1,\dots,h_r$ des éléments de $\mathcal{M}$: pour un système multi-homogène, on peut prendre les variables $x_1,\dots,x_n$. Dans l'exemple ci-dessus, on peut prendre $h_1 = xy$ et $h_2 = y^3$. L'objet calculé est une base de Gröbner pour l'ordre lexicographique dans l'algèbre $\mathbb{K}[H] = \mathbb{K}[H_1,\dots,H_r]$; la variété correspondante étant l'image de $\mathbb{V}(\mathcal{I})$ par une application monomiale

$$\begin{array}{rccc} \phi : & \overline{\mathbb{K}}^n & \longrightarrow & \overline{\mathbb{K}}^r \\ & \mathbf{a} = (a_1,\dots,a_n) & \longmapsto & (h_i(\mathbf{a}))_{i=1,\dots,r} \end{array}$$

L'algorithme Sparse-FGLM correspondant présente des similitudes avec l'algorithme SAGBI-FGLM évoqué précédemment par la nature de l'objet calculé, cependant la mise en oeuvre est beaucoup plus proche de l'algorithme FGLM standard. La variété $\mathbb{V}(\mathcal{I})$ étant

l'image réciproque par l'application ϕ de la variété dans $\mathbb{K}[H]$, le processus se termine par le calcul de cette variété et inversion de l'application monomiale. Le processus complet est représenté en figure 0.12.

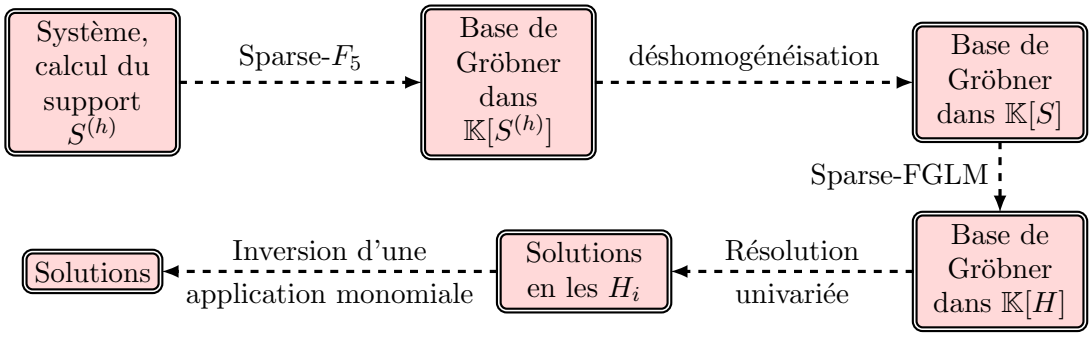


FIGURE 0.12 – Résolution de systèmes polynomiaux creux.

Enfin, le processus se généralise aux sous-algèbres de l'algèbre des polynômes de Laurent $\mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, sous réserve que le semi-groupe S ne contienne pas deux éléments distincts dont le produit vaut 1.

Versions abéliennes des algorithmes F_5 et FGLM. On s'intéresse ici au calcul de la variété d'un ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ invariant sous l'action d'un groupe fini $\mathbf{G} \subseteq \mathcal{GL}_n(\mathbb{K})$ supposé *abélien*. On suppose de plus que l'action est *non-modulaire* : la caractéristique de $\mathbb{K}$ ne divise pas le cardinal de $\mathbf{G}$.

Il a déja été remarqué par Gatermann et Steidel [51, 96] que diagonaliser le groupe et répercuter le changement de variables correspondant sur les polynômes f_i constituait une stratégie efficace, préalablement à un calcul de base de Gröbner. Cependant, ni un algorithme *dédié* ni une étude du gain en complexité n'avaient été proposés. Supposons maintenant $\mathbf{G}$ constitué de matrices *diagonales*. Alors, l'action d'un tel groupe sur $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ induit une gradation plus précise que le seul degré :

$$\mathbb{K}[X] = \bigoplus_{d=0}^{+\infty} \mathbb{K}[X]_d = \bigoplus_{d=0}^{+\infty} \bigoplus_{g \in \mathbf{X}(\mathbf{G})} \mathbb{K}[X]_{d,g} = \bigoplus_{g \in \mathbf{X}(\mathbf{G})} \mathbb{K}[X]_g$$

où $\mathbf{X}(\mathbf{G})$ est un groupe isomorphe à $\mathbf{G}$, et les composantes $\mathbb{K}[X]_g$ sont engendrés par des monômes. Un élément de $\mathbb{K}[X]_g$ est dit *de $\mathbf{G}$-degré g*.

Exemple 0.13. *Reprenons l'exemple 0.5. Après diagonalisation, on obtient des polynômes invariants sous l'action du groupe engendré par la matrice matrice $D_A = \mathrm{Diag}(\jmath, \jmath^2)$. Pour tout monôme m de $\mathbb{K}[X]$, il existe un unique entier tel que $m^{D_A} = \jmath^k m$, cet entier est unique modulo 3, et donc $\mathbf{X}(\mathbf{G}) = \mathbb{Z}/3\mathbb{Z}$. La base de Gröbner pour l'ordre DRL de $\langle f^P, g^P \rangle$ est :*

$$\mathcal{G}_1 = \begin{cases} f_1 = y^4 - \frac{1}{10}(3 + 4\imath)x^2 + \frac{1}{20}(1 - 2\imath)y \\ f_2 = x^3 + \frac{1}{5}(-3 + 4\imath)y^3 + \frac{1}{20}(1 + 2\imath) \\ f_3 = xy - \frac{1}{2} \end{cases}$$

Alors f_2 et f_3 sont de $\mathbf{G}$-degré 0, et f_1 de $\mathbf{G}$-degré 2. De même, les polynômes de la base de Gröbner lexicographique présentée dans l'exemple 0.5 sont de $\mathbf{G}$-degré 1 et 0.

On montre tout d'abord le théorème suivant :

Théorème. *Si $f \in \mathcal{I}$, alors pour tout g dans $\mathbf{X}(\mathbf{G})$, la composante de f dans $\mathbb{K}[X]_g$ appartient également à $\mathcal{I}$.*

Le théorème précédent permet de se ramener du cas d'un ensemble de générateurs stable, à celui d'un système de générateurs *semi-stables* : un polynôme f appartenant à une composante $\mathbb{K}[X]_g$ vérifie $f^A = \xi_{A,g} f$ pour tout $A \in \mathbf{G}$, où $\xi_{A,g}$ est une racine de l'unité indépendante de f. Les polynômes de $\mathbb{K}[X]_g$ sont dits $\mathbf{G}$-homogène de $\mathbf{G}$-degré g. On prouve que les composantes $\mathbb{K}[X]_g$ sont engendrées par des monômes, et que si m et m' sont de $\mathbf{G}$-degrés respectivement g et g', alors mm' est de $\mathbf{G}$-degré $g + g'$. Par conséquent, tous les polynômes intervenant dans un calcul de base de Gröbner d'un système constitué de polynômes $\mathbf{G}$-homogènes sont eux-mêmes $\mathbf{G}$-homogènes.

Les algorithmes F_5 et FGLM reposent sur de l'algèbre linéaire : la structure induite par $\mathbf{G}$ permet donc de découper les matrices intervenant dans ces deux algorithmes en $|\mathbf{G}|$ matrices plus petites (chacune indexée par l'un des $\mathbf{G}$-degrés). De plus, chaque étape de l'algorithme F_5 (passage d'une base de Gröbner en degré D à une base de Gröbner en degré $D+1$) peut être parallélisée car les matrices sont construites et réduites de manière indépendante.

Le processus de résolution est décrit en figure 0.14. Dans cette description, le groupe abélien $\mathbf{G}$, constitué de matrices non nécessairement diagonales, agit sur $\mathcal{I}$. On répercute la diagonalisation de $\mathbf{G}$ en $\mathbf{G}'$ sur $\mathcal{I}$ pour obtenir $\mathcal{I}'$. Le calcul de $\mathbb{V}(\mathcal{I}')$ est mené de façon classique, mais en utilisant les variantes abéliennes de nos algorithmes. On retrouve $\mathbb{V}(\mathcal{I})$ en appliquant la matrice de passage P^{-1} aux éléments de $\mathbb{V}(\mathcal{I}')$.

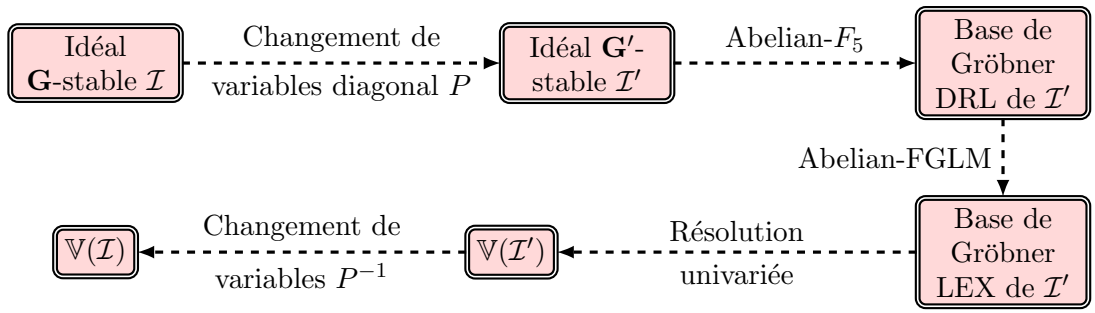


FIGURE 0.14 – Résolution de systèmes polynomiaux invariants sous un groupe abélien.

Système d'équations globalement invariant sous l'action du groupe symétrique. On a considéré au paragraphe précédent le cas d'un idéal globalement stable sous l'action d'un groupe abélien. On considère maintenant une situation similaire, mais le groupe qui agit est le groupe symétrique $\mathfrak{S}_N$. Celui-ci agit sur une algèbre polynomiale à $n = (\ell+1)N$ variables à travers la représentation *diagonale par blocs* :

$$\begin{array}{ccc} \mathfrak{S}_N & \longrightarrow & \mathcal{GL}_n(\mathbb{Z}) \\ \sigma & \longmapsto & \begin{pmatrix} M_\sigma & & & 0 \\ & M_\sigma & & \\ & & \ddots & \\ 0 & & & M_\sigma \end{pmatrix} \end{array}$$

où M_σ est la matrice de taille $N \times N$ canoniquement associée à σ. Nommons les variables $\mathcal{Z} = \{z_1, \ldots, z_N\}$ et $\mathcal{V} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_\ell$, avec $\mathcal{V}_i = \{x_{i,1}, \ldots, x_{i,N}\}$. Le groupe $\mathfrak{S}_N$ agit donc sur l'ensemble de variables $\mathcal{Z} \cup \mathcal{V}$ par $z_i^\sigma = z_{\sigma(i)}$ et $x_{i,j}^\sigma = x_{i,\sigma(j)}$.

On considère un système de N équations polynomiales $(U_i)_{1 \leq i \leq N}$ à coefficients dans $\mathbb{K}[\mathcal{Z} \cup \mathcal{V}]$ tel que $U_i = D_i P_i + R_i$ avec $D_i = \prod_{k \neq i}(z_i - z_k)$, $P_i \in \mathbb{K}[\mathcal{Z} \cup \mathcal{V}]$ et $R_i \in \mathbb{K}[\mathcal{Z}]$, tels que $P_i^\sigma = P_{\sigma(i)}$ et $R_i^\sigma = R_{\sigma(i)}$ pour tout σ dans $\mathfrak{S}_N$. Les polynômes U_i vérifient alors $U_i^\sigma = U_{\sigma(i)}$ pour tout σ dans $\mathfrak{S}_N$. On s'intéresse à un ouvert de la variété associée aux U_i constituée des points dont les composantes associées aux z_i sont toutes distinctes. On a alors le résultat suivant :

Théorème. *Soit d le degré (commun) des polynômes U_i. Il existe N polynômes $V_1, \ldots, V_N$ de degrés $\deg(V_i) = d - i + 1$ individuellement invariants sous l'action de $\mathfrak{S}_N$, dont la variété associée coïncide avec $\mathbb{V}(\langle U_1, \ldots, U_N \rangle)$ sur les points n'ayant pas deux composantes associées aux z_i égales.*

Le théorème précédent est *effectif*, puisqu'il est associé à un algorithme calculant effectivement les polynômes V_i. Les *différences divisées* sont l'ingrédient principal de l'algorithme. L'intérêt est double : le degré des équations a diminué et elles sont maintenant individuellement invariantes sous l'action de $\mathfrak{S}_N$.

Dans le cas $\ell = 0$ (il n'y a alors que les variables z_i), on peut maintenant reformuler les équations V_i à l'aide des fonctions symétriques élémentaires e_i des z_i. Le système qui en résulte est bien plus facile à résoudre, puisqu'on a tenu compte de la symétrie des équations pour ne calculer que les fonctions symétriques des solutions et non les solutions elles-même.

Supposons maintenant $\ell = 1$, et notons $\mathcal{V} = \{Z_1, \ldots, Z_N\}$. On explique maintenant comment éliminer complètement les variables $\mathcal{V}$ et obtenir des équations symétriques en les seules variables z_i (qu'on pourra reformuler à l'aide des e_i), sous la condition qu'il y ait d'autres équations d'un type particulier dans le système.

Soit z une nouvelle variable, et M et N deux polynômes de $\mathbb{K}[z_1, \ldots, z_N, z]$. On suppose que M et N, vus comme polynômes en la seule variable z, ont leur coefficients invariants sous l'action du groupe $\mathfrak{S}_N$. Par conséquent, ces coefficients peuvent être reformulés à l'aide des (e_i), les fonctions symétriques élémentaires des (z_i). M et N appartiennent donc à l'algèbre $\mathbb{K}[e_1, \ldots, e_N, z]$. Ajoutons au système $\{V_i\}$ les polynômes $W_i = M(z_i)Z_i - N(z_i)$. Alors, on peut éliminer algorithmiquement les variables Z_i de façon à construire des équations symétriques en les z_i, que l'on peut reformuler à l'aide des fonctions symétriques élémentaires.

Application à la résolution symbolique du problème des tourbillons. L'approche développée pour l'étude des systèmes globalement invariant sous une action du groupe symétrique agissant sur des blocs de variables s'applique en particulier à la détermination des configurations stables du problème des tourbillons : on s'intéresse aux configurations planaires de N tourbillons ayant même vorticité, dont la forme géométrique est maintenue au cours du temps. Les tourbillons se meuvent autour du centre de masse, mais la forme qu'ils déterminent reste la même. En d'autres termes, la configuration des N points reste invariante par similitudes directes au cours du temps.

En supposant le centre de masse des tourbillons à l'origine, déterminer les configurations stables revient à résoudre le système formé des N équations :

$$\bar{z_i} = \sum_{j \neq i} \frac{1}{z_i - z_j} \qquad \text{pour tout } i \text{ entre 1 et } N$$

où z_i est l'affixe complexe du tourbillon numéroté i, $\bar{z_i}$ son conjugué et $z_i \neq z_j$ pour i différent de j. Puisqu'il est impossible de séparer un complexe de son conjugué de façon algébrique, on introduit de nouvelles variables Z_i symbolisant les conjugués des z_i. La réduction au même dénominateur nous ramène aux équations :

$$U_i = Z_i \prod_{j \neq i} (z_i - z_j) - \sum_{j \neq i} \prod_{k \neq i,j} (z_i - z_k) \in \mathbb{Q}[z_1, \ldots, z_N, Z_1, \ldots, Z_N]$$

On montre également que le problème des tourbillons vérifie les équations : $M(z_i)Z_i = N(z_i)$ avec $M(z) = 2Q'(z)$, $N(z) = Q''(z)$ et Q est le polynôme $\prod_{i=1}^{N}(z - z_i)$. On remarque que les coefficients de Q sont les fonctions symétriques e_i des z_i. Par suite, on peut appliquer la méthodologie décrite ci-dessus pour résoudre le problème des tourbillons.

Les équations V_i obtenues par différences divisées des polynômes U_i admettent une reformulation très simple à partir d'invariants de l'action du groupe $\mathfrak{S}_N$ sur $\mathbb{Q}[z_1, \ldots, z_n, Z_1, \ldots, Z_n]$. On montre plus précisément le théorème suivant :

Théorème. *En notant, pour tout $k \geq 0$, $s_k = \sum_{i=1}^{N} z_i^k$ et $r_k = \sum_{i=1}^{N} Z_i z_i^k$ (avec $s_0 = N$), les solutions du problème des tourbillons vérifient les équations suivantes, pour tout $k \geq 1$:*

$$2\, r_k = \left(\sum_{i=0}^{k-1} s_i\, s_{k-1-i} \right) - k\, s_{k-1}$$

En suivant l'approche expliquée précédemment, consistant à reporter les équations $2Q'(z_i) = Q''(z_i)$ dans les équations du théorème, on obtient des équations en les fonctions symétriques (e_i) des (z_i). À l'aide du package FGb [63], il est possible de résoudre ces équations et d'obtenir toutes les solutions du problème des tourbillons jusqu'à $N = 7$. On présente en figure 0.15 l'ensemble des solutions pour $N = 7$. Avant cette approche, le problème n'était résoluble que jusqu'à $N = 5$.

Résultats de complexité.

Puisqu'ils présentent des similitudes, on a regroupé ici les principaux résultats de complexité présentés dans ce manuscrit. Les opérations dénombrées sont les opérations arithmétiques dans le corps $\mathbb{K}$, et on utilise la notation de Landau O. La lettre ω désigne l'exposant de l'algèbre linéaire, c'est à dire la borne inféfieure des réels γ tels que la multiplication de deux matrices de taille $N \times N$ peut se faire en $O(N^\gamma)$ opérations arithmétiques. La meilleure borne actuelle est $\omega < 2.3728639$, voir [50].

Résolution d'un système polynomial globalement invariant sous l'action d'un groupe abélien. Après diagonalisation du groupe (possible dans le cas non-modulaire), on montre que les matrices contruites dans les variantes abéliennes des algorithmes F_5 et FGLM ont leur nombre de lignes et de colonnes divisées par un facteur correspondant au cardinal du groupe, comparées à leurs analogues dans les algorithmes F_5 et FGLM. On en déduit les résultats de complexité suivants :

Théorème. *Soit $\mathbf{G}$ un sous-groupe de $\mathcal{GL}_n(\mathbb{K})$ constitué de matrices diagonales sans autre dilatation que l'identité. Soit $F = (f_1, \ldots, f_s) \in \mathbb{K}[X]^s$ une famille de polynômes homogènes formant un idéal de dimension zéro $\mathcal{I}$ globalement invariant sous l'action de $\mathbf{G}$. Alors la complexité du calcul d'une base de Gröbner pour l'ordre DRL de l'idéal $\mathcal{I}$ est bornée par*

$$O\Big(\frac{s}{|\mathbf{G}|^\omega} \binom{n + d_{reg}(F)}{d_{reg}(F)}^\omega \Big)$$

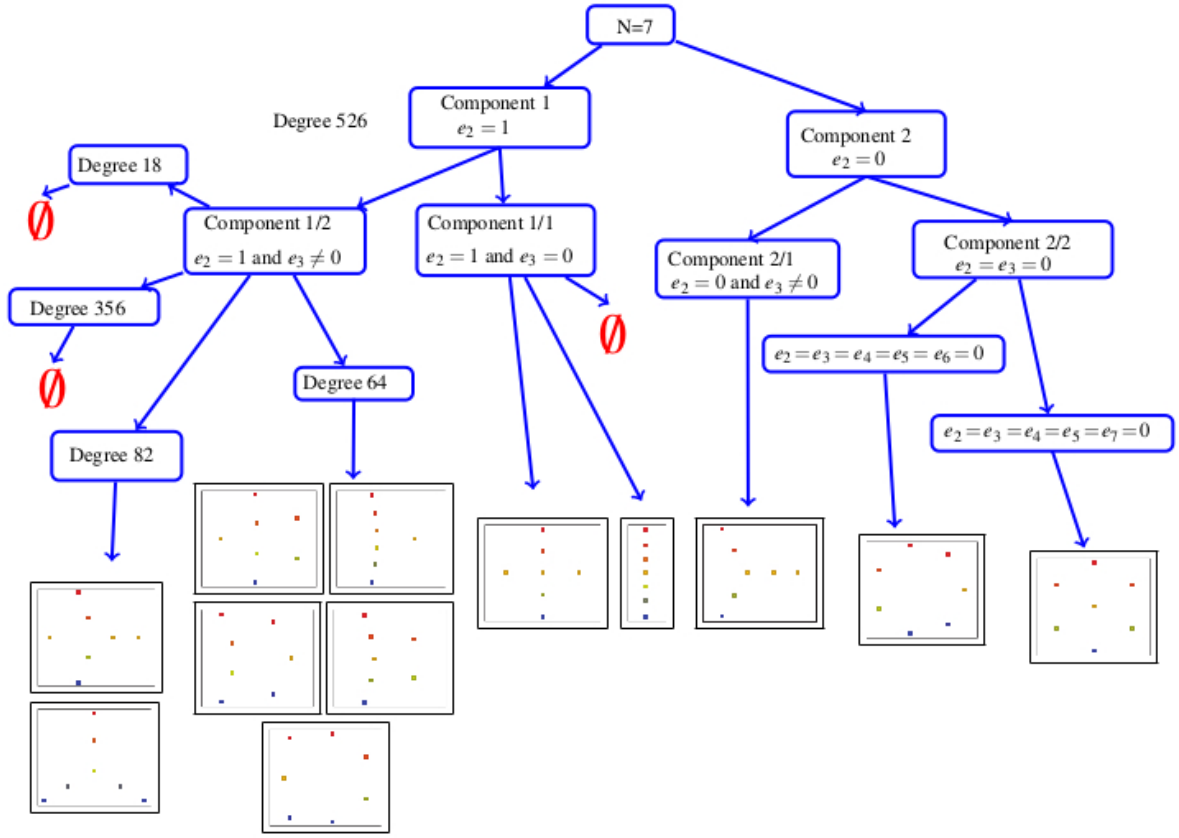


FIGURE 0.15 – L'ensemble des solutions pour le cas $N = 7$.

operations dans $\mathbb{K}$*, avec* $d_{reg}(F)$ *le degré de régularité de* F*.*

En supposant $\mathcal{I}$ de dimension 0, on montre en analysant l'analyse de l'algorithme Abelian-FGLM le résultat suivant :

Théorème. *Sous l'hypothèse (vérifiée en pratique) que les monomes de* $\mathbb{K}[X]/\mathcal{I}$ *sont bien répartis entre les différents* $\mathbf{G}$*-degrés, il est possible d'effectuer le changement d'ordre de l'idéal* $\mathcal{I}$ *en* $O\left(n \cdot \delta^3/|\mathbf{G}|^2\right)$ *opérations arithmétiques dans* $\mathbb{K}$*, avec* $\delta = \dim_{\mathbb{K}}(\mathbb{K}[X]/\mathcal{I})$*.*

Résolution d'un système d'équations invariantes sous l'action d'un groupe. Dans cette approche, on donne une complexité en fonction du degré maximal atteint durant le calcul de la base SAGBI. Ce degré dépend implicitement des invariants choisis pour réexprimer les solutions.

Théorème. *Soit* $\mathbf{G}$ *un sous-groupe de* $\mathcal{GL}_n(\mathbb{K})$ *sans autre dilatation que l'identité. Soit* $\mathbf{F} = (f_1, \ldots, f_s) \in (\mathbb{K}[X]^{\mathbf{G}})^s$ *une famille de polynômes invariants sous l'action de* $\mathbf{G}$*. Alors la complexité du calcul d'une base SAGBI en degré* D *pour l'ordre DRL de l'idéal* $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ *est bornée par*

$$O\left(\frac{s}{|\mathbf{G}|^\omega}\binom{D+n}{D}^\omega\right)$$

operations dans $\mathbb{K}$*, avec* ω *un exposant faisable pour l'algèbre linéaire.*

Résolution d'un système d'équations à support dans un même polytope. L'approche creuse expliquée précédemment permet notamment de traiter les cas où les polynômes sont à support dans un même polytope $\mathscr{P}$. Pour ces systèmes, on donne des bornes de complexité précises, dépendant des propriétés combinatoires du polytope. Le calcul d'une base de Gröbner creuse par l'algorithme SAGBI-F_5 est effectuée dans *l'algèbre polytopale* $\mathbb{K}[\mathscr{P}] = \mathbb{K}[S^{(h)}_{\mathscr{P}}]$ où $S^{(h)}_{\mathscr{P}}$ est le semi-groupe engendré par $\{(\alpha, 1) \mid \alpha \in \mathscr{P}\}$. Un outil essentiel est la série de Hilbert de cette algèbre polytopale définie par

$$\mathsf{HS}_{\mathscr{P}}(z) = \sum_{d=0}^{+\infty} \mathsf{HP}_{\mathscr{P}}(d) z^d \qquad \text{où} \qquad \mathsf{HP}_{\mathscr{P}}(d) = \#(d \cdot \mathscr{P})$$

Commençons par un cas particulier : celui des systèmes bilinéaires. Considérons une partition des variables en deux blocs de tailles n_x, n_y. Le polytope considéré est donc $\mathscr{P} = \Delta_{n_x} \times \Delta_{n_y}$, produit de deux simplexes de $\mathbb{N}^{n_x}$ et $\mathbb{N}^{n_y}$. On a alors $\mathsf{HP}_{\mathscr{P}}(d) = \binom{n_x+d}{n_x}\binom{n_y+d}{n_y}$. Dans [36], les auteurs montrent que pour un système de n polynômes biliénaires affines génériques, le degré maximal atteint lors du calcul d'une base de Gröbner pour un ordre gradué est $\mathrm{d_{wit}} \leq \min(n_x, n_y) + 2$. Ils en déduisent une complexité de

$$O\left(\binom{n_x + n_y + \min(n_x, n_y) + 2}{\min(n_x, n_y) + 2}^{\omega}\right)$$

Avec l'approche creuse, on retrouve la même borne sur le degré maximal atteint $\mathrm{d_{wit}}$, mais le fait d'effectuer les calcul dans $\mathbb{K}[\mathscr{P}]$ permet de borner la complexité du calcul d'une base de Gröbner creuse par

$$O(n\,\mathsf{HP}(\mathrm{d_{wit}})^{\omega}) = O\left(n\binom{n_x + \min(n_x, n_y) + 1}{\min(n_x, n_y) + 1}^{\omega}\binom{n_y + \min(n_x, n_y) + 1}{\min(n_x, n_y) + 1}^{\omega}\right)$$

Cette formule s'étend facilement au systèmes multilinéaires, ce qui n'était pas connu : si les variables sont réparties en blocs de tailles $n_1, \ldots, n_\ell$, $\mathrm{d_{wit}} \leq \sum_{i=1}^{\ell} n_i - \max(n_i) + 1$. On donne de même une borne générale pour les systèmes multi-homogènes. Pour une algèbre polytopale quelconque, la *régularité de Castelnuovo-Mumford* (voir définition 3.109) de l'algèbre $\mathbb{K}[\mathscr{P}]$ intervient dans le résultat suivant, qui suppose que $\mathbb{K}[\mathscr{P}]$ est *Cohen-Macaulay* (voir définition 2.9).

Théorème. *La complexité de calculer une base de Gröbner creuse de $\langle f_1, \ldots f_n\rangle \subset \mathbb{K}[\mathscr{P}]$ en degré $\mathrm{d_{wit}}$ est borné par $O\left(n\,\mathsf{HP}_{\mathscr{P}}(\mathrm{d_{wit}})^{\omega}\right)$ où $\mathrm{d_{wit}} \leq \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1)$.*

En supposant également le semi-groupe S engendré par $\mathscr{P}$ *simplicial* (voir définition 3.91), la complexité de l'algorithme Sparse-FGLM est la suivante. On appelle base de Hilbert un système de générateurs du semi-groupe S.

Théorème. *Soit $\delta = \dim_{\mathbb{K}}(\mathbb{K}[S]/\mathcal{I})$ et soit r le cardinal d'une base de Hilbert du semi-groupe S. Si S est un semi-groupe affine simplicial et $\mathbb{K}[S]$ une algèbre Cohen-Macaulay, l'algorithme Sparse-FGLM calcule la base de Gröbner dans $\mathbb{K}[H]$ en au plus $O(r \cdot \delta^3)$ operations dans $\mathbb{K}$.*

Enfin, contrairement à [36], l'approche s'applique également aux systèmes surdéterminés, ce qui nous permet de proposer une variante de la conjecture de Fröberg (conjecture 2.43), non détaillée ici, ainsi que d'autres résultats de complexité.

Implémentation.

Les variantes des algorithmes F_5 et FGLM présentées plus haut ont été implémentées en Magma. Ont également été implémentées dans un langage de bas niveau (C), par Jean-Charles Faugère :

- une version de l'algorithme F_5 pour calculer une base SAGBI d'un idéal invariant sous l'action du groupe cyclique.
- une version de l'algorithme F_4 (parallélisée) pour calculer une base de Gröbner d'un idéal globalement sous l'action d'un groupe abélien.
- une version matricielle (sp-Matrix F_5) de l'algorithme F_5 pour calculer une base de Gröbner creuse d'une algèbre monomiale. Cette version prend un degré maximal comme paramètre.

Pour terminer, on exhibe trois exemples montrant l'efficacité des nouvelles approches. La table 0.16 présente les différences de tailles des objets calculés entre l'approche classique et l'approche par base SAGBI pour résoudre les problèmes Cyclic-5 et Cyclic-6. Pour la base de Gröbner lexicographique de l'idéal dans $\mathbb{K}[x_1, \ldots, x_n]$ (approche classique) ou la base de Gröbner obtenue dans $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$ (approche SAGBI) où les σ_i sont les fonctions symétriques des variables, on présente le nombre d'éléments dans la base, la taille maximale des polynômes, et la taille de la variété associée dans une clôture algébrique. Pour tous ces critères, la base de Gröbner invariante est beaucoup plus petite que la base de Gröbner classique.

$\mathcal{G}$	$\lvert\mathcal{G}\rvert$	$\max\{\lvert\text{support}(g)\rvert \mid g \in \mathcal{G}\}$	$\mathbb{V}(\langle\mathcal{G}\rangle)$
Base de Gröbner de $\mathcal{I}^{D_6}$	17	27	156
Base de Gröbner $\mathfrak{S}_6$-invariante de $\mathcal{I}^{D_6}$	7	4	13
Base de Gröbner de $\mathcal{I}^{D_7}$	35	132	924
Base de Gröbner $\mathfrak{S}_6$-invariante de $\mathcal{I}^{D_7}$	7	9	57

TABLE 0.16 – Tailles des bases de Gröbner classiques et bases de Gröbner invariantes pour le problème Cyclic-n.

La figure 0.17 montre les différents temps de calcul d'une base de Gröbner DRL du problème cyclique avec l'algorithme F_4 pour différentes valeurs de n. Le problème cyclique est invariant sous l'action du groupe cyclique. L'idéal $\mathcal{I}$ est l'idéal engendré par les polynômes avant changement de variables et $\mathcal{I}'$ est l'idéal après changement de variables. F_4 est l'algorithme classique du package FGb et $F_4^{//}$ est le nouvel algorithme parallélisant construction et réduction des matrices. C'est la première fois qu'une base de Gröbner du problème Cyclic-11 est calculée avec l'algorithme F_4.

En table 0.18, on reporte quelques temps de calculs de systèmes bilinéaires surdéterminés, d'une part avec une implémentation basique de la nouvelle approche « creuse », et d'autre part avec l'algorithme F_5 du package FGb. On observe une amélioration significative des temps de calculs.

Pespectives.

On présente ici différentes directions pouvant étendre les résultats de cette thèse.

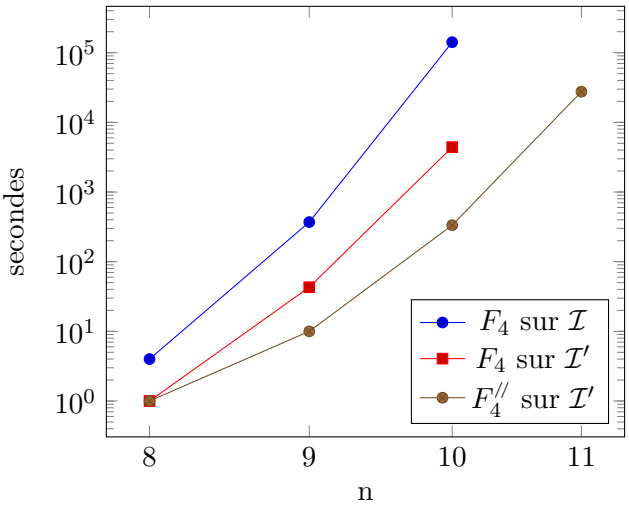


FIGURE 0.17 – Temps de calcul d'une base de Gröbner DRL pour le problème Cyclic-n

(n_x, n_y, m)	sp-Matrix F_5	FGb-F_5	Speed-up
(2,29,40)	0.12s	5.2s	43
(2,39,53)	0.49s	36.7s	74
(2,49,65)	1.53s	298.5s	195
(2,59,78)	4.63s	852.3s	184
(6,19,52)	1.10s	25.2s	22
(6,21,56)	2.13s	51.5s	24
(6,27,71)	7.07s	236.0s	33

TABLE 0.18 – Systèmes bilinéaires surdéterminés en (n_x, n_y) variables et m équations.

Idéaux stables sous l'action diagonale du groupe symétrique. Dans cette thèse, on étudie notamment un système d'équations de la forme

$$\left\{ Z_i = \frac{P(z_i)}{Q'(z_i)} \quad i = 1..N \right\} \qquad \text{où } Q(z) = \prod_{i=1}^{N} (z - z_i)$$

Ce système est globalement invariant sous l'action du groupe symétrique $\mathfrak{S}_N$ agissant sur les variables z_i et Z_i par $\sigma(z_i) = z_{\sigma(i)}$ et $\sigma(Z_i) = Z_{\sigma(i)}$. On explique comment reformuler un tel système en termes des fonctions symétriques élémentaires des (z_i). Ce type de système, avec action du groupe symétrique sur plusieurs blocs de variables , apparaît très fréquemment dans les applications. On donne ici un exemple de problème présentant une telle symétrie, que l'approche développée dans cette thèse ne permet pas de résoudre et qui constitue une intéressante perspective : la résolution des équations de Brent [10].

On s'intéresse au système d'équations à $3N^2T$ inconnues et N^6 équations suivant :

$$\forall (i,j,k,\ell,m,n) \in \{1,\dots,N\} \qquad \sum_{p=1}^{T} \alpha_{ijp}\beta_{klp}\gamma_{mnp} = \delta_{in}\delta_{jk}\delta_{\ell m}$$

où δ est le symbole de Kronecker. Parmi beaucoup d'autres symétries apparaît une action diagonale du groupe symétrique $\mathfrak{S}_T$ agissant sur α_{ijp} par $\sigma(\alpha_{ijp}) = \alpha_{ij\sigma(p)}$, et de même sur β_{klp} et γ_{mnp}. Ce système intervient dans la multiplication rapide de matrices carrées : Strassen [98] a exhibé une solution avec $T = 7$ et $N = 2$, ce qui a mené à la première complexité sous-cubique de la multiplication de deux matrices $N \times N$. L' approche menant à la meilleure complexité connue actuellement pour ce problème [108, 50] exploite également ces équations. Pour $N = 3$, on sait qu'il n'y a pas de solution pour $T \leq 20$ et qu'il en existe une pour $T = 23$ (voir [69]), mais les cas $T = 21$ et 22 restent ouverts.

En dimension positive ? Cette thèse se concentre sur la résolution de systèmes n'admettant qu'un nombre fini de solutions. Si les variantes de l'algorithme F_5 que l'on a proposées sont valables en toute dimension, ce n'est pas le cas des variantes de l'algorithme de changement d'ordre FGLM. Une perspective intéressante est donc l'élimination de variables en dimension positive.

Base de Gröbner creuses : le cas mixte. L'approche développée dans le dernier chapitre ne traite, du point de vue théorique comme du point de vue algorithmique, que du cas où les polynômes du système ont leur support inclus dans un même polytope. Dans l'approche par résultant, le cas mixte (les polynômes sont à support dans des polytopes différents) est bien compris. C'est pourquoi une perspective proche est de traiter ce cas mixte.

Complexité de la résolution de systèmes dont le support est constitué de monômes dispersés. Les algorithmes présentés dans le dernier chapitre s'appliquent dans le cas où les polynômes ont leur support constitué d'un même ensemble de monômes dispersés, et les tests effectués sont très prometteurs. Expliquer pourquoi est un travail en cours avec Jean-Charles Faugère et Pierre-Jean Spaenlehauer.

Idéaux stables sous l'action d'un groupe. L'extension du travail effectué pour les idéaux stables sous l'action d'un groupe abélien à des groupes non abéliens serait d'un grand intérêt. La théorie des représentations devrait y jouer un rôle prépondérant, c'est pourquoi elle a été développée dans ce manuscrit.

Organisation du Manuscrit

Ce manuscrit est divisé en deux parties. La première présente les rappels nécessaires à la compréhension de cette thèse et comporte trois chapitres. La seconde partie présente les contributions, elles-mêmes réparties en deux chapitres.

Chapitre 1 : Ce chapitre introduit la notion de base de Gröbner et présente les algorithmes classiques de calcul de bases de Gröbner que sont F_5 et FGLM. Y est également étudié leur complexité dépendant notamment de deux paramètres que sont le degré maximal atteint lors du calcul d'une base de Gröbner pour un ordre du degré, ainsi que le degré d'un idéal de dimension zéro. La fin du chapitre présente une généralisation de l'algorithme F_5 pour le calcul de bases SAGBI jusqu'à un degré fixé, dans le cadre d'algèbres graduées. Cette généralisation n'apparaît pas dans la littérature, cependant elle est essentielle car les variantes de l'algorithme F_5 présentées dans la suite en sont des spécialisations.

Chapitre 2 : Dans ce chapitre, on présente les outils algébriques classiques permettant d'estimer les deux paramètres dont il est question dans le chapitre précédent. On définit notamment la *série de Hilbert* d'un idéal, la propriété d'être *Cohen-Macaulay* et la notion de *suite régulière*.

Chapitre 3 : Ce dernier chapitre préliminaire présente les deux types de structures algébriques sur une algèbre de polynômes qui sont étudiées dans cette thèse. Il est tout d'abord question de l'action des groupes finis sur les algèbres de polynômes. Après avoir présenté *l'algèbre des invariants* sous l'action d'un groupe fini, on verra comment calculer effectivement ces invariants ainsi qu'une estimation de la série de Hilbert associée à cette algèbre. La notion d'invariant est ensuite généralisée à celle *d'invariant relatif* par la théorie des représentations linéaires des groupes finis. Il est ensuite question des sous-algèbres générées par un ensemble fini de monômes. L'outil algébrique sous-jacent est le semi-groupe, et l'on présente la notion essentielle de *semi-groupe normal*.

Chapitre 4 : Ce premier chapitre contributif est le plus volumineux de cette thèse. Il se subdivise en trois sections, qui sont en grande partie indépendantes.

- Dans la première section, il est question de systèmes d'équations polynômiales *globalement* invariants sous une action du groupe symétrique. L'étude de ce problème est motivée par la résolution symbolique d'un problème physique : celui de déterminer les configurations planaires stables d'un ensemble de tourbillons ayant même vorticité. On montrera comment se ramener à des équations individuellement invariantes à l'aide de différences divisées, et comment reformuler les équations à l'aide des fonctions symétriques des positions complexes des tourbillons. Les résultats présentés dans cette partie sont l'objet d'un travail commun avec Jean-Charles Faugère et ont fait l'objet d'une présentation à la conférence ISSAC 2012 [43].
- La deuxième section porte sur la résolution de systèmes d'équations polynômiales *individuellement* invariantes sous l'action d'un groupe fini. Il est question ici d'étendre l'approche par bases SAGBI dans le cadre de sous-groupes de permutations de l'article [41] de Jean-Charles Faugère et Sajjad Rahmany : cette approche se généralise à tous les groupes finis, et il est possible d'en estimer la complexité. Se pose également la question de l'élimination de solutions parasites engendrées par cette approche. Le résultats présentés ici sont l'objet d'un travail avec Jean-Charles Faugère et Guënael Renault, qui sera soumis ultérieurement.
- Dans la troisième et dernière section, il est question d'accélérer le calcul de bases de Gröbner d'idéaux globalement stables sous l'action d'un groupe abélien fini, dans le cas *non-modulaire*. On montre qu'il est possible de se ramener au cas d'un groupe constitué de matrices diagonales, et l'action du groupe se traduit par une structure additionnelle sur l'algèbre des polynômes. Cette structure permet de découper les matrices intervenant dans les algorithmes classiques de calculs de base de Gröbner par algèbre linéaire que sont F_5 et FGLM. Les résultats présentés ici ont fait l'objet d'une présentation à la conférence ISSAC 2013 [44]. Cependant, l'accent est mis ici sur le lien entre les représentations de groupes et la stucture additionnelle, qui n'était pas présent dans l'article originel.

Chapitre 5 : Ce dernier chapitre, petit par la taille, présente pourtant des résultats qui sont peut-être les plus significatifs de cette thèse. On étudie ici les systèmes d'équations dont le support est inclus dans un même sous-ensemble de monômes. Si ce sous-ensemble forme un polytope, l'utilisation des propriétés combinatoires du polytope permet de donner des

bornes de complexité précices : on retrouve facilement des résultats connus sur la complexité de résolution de systèmes bilinéaires et on étend ces résultats aux systèmes multihomogènes. L'approche présentée ici s'applique également dans le cas où le support est constitué de monômes dispersés. Ce cadre n'est pas encore couvert par l'approche théorique, mais les résultats pratiques semblent très prometteurs. Ce travail en collaboration avec Jean-Charles Faugère et Pierre-Jean Spaenlehauer a été accepté pour publication à la conférence ISSAC 2014 [42].

Part I

Preliminaries

Chapter 1

Gröbner Bases

The aim of this chapter is to present the classical algorithms used in order to compute a Gröbner basis of an ideal. In section 1.1, we recall classical notions and present Buchberger algorithm. Section 1.2 is devoted to the links between linear algebra and Gröbner bases. In particular, we present the F_5 and FGLM algorithms. Finally, we generalize in section 1.3 the Gröbner concepts to subalgebras. The aim of this section is to introduce the SAGBI-Matrix F_5 algorithm used in chapter 4 and 5.

1.1 Gröbner Basics [1]

The aim of this section is to recall basic material and to fix notations. One main reference is [25].

1.1.1 Ideals and Varieties

Let $\mathbb{K}$ be a field, n be a positive integer and $\mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ring with base-field $\mathbb{K}$ and indeterminates $x_1, \ldots, x_n$ that will be abbreviated $\mathbb{K}[X]$. In this subsection, we fix some notations and recall basic links between ideals and varieties.

Definition 1.1. *Throughout this thesis, we define:*
- *a monomial as a product of indeterminates* $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ *with* $\alpha_i \in \mathbb{N}$.
- *a term as a product of a monomial with an element of* $\mathbb{K}$.
- *a polynomial as a linear combination of terms.*

Ideals. The basic objects in commutative algebra are ideals and varieties. We now recall definitions and fundamental theorems.

Definition 1.2. *An ideal* $\mathcal{I}$ *of* $\mathbb{K}[X]$ *is a non-empty additive subgroup of* $\mathbb{K}[X]$ *such that:*

$$f \in \mathcal{I} \quad \text{and} \quad g \in \mathbb{K}[X] \qquad \Longrightarrow \qquad fg \in \mathcal{I}$$

Proposition – Definition 1.3. *Let* $f_1, \ldots, f_s$ *be polynomials in* $\mathbb{K}[X]$. *Then the subset*

$$\left\{ f \in \mathbb{K}[X] \;\middle|\; \exists s \in \mathbb{N}^* \quad \exists g_1, \ldots, g_s \in \mathbb{K}[X], \quad f = \sum_{i=1}^{s} f_i g_i \right\}$$

is an ideal of $\mathbb{K}[X]$, *denoted by* $\langle f_1, \ldots, f_s \rangle$.

1. I found this wordplay in Sturmfels' book [102].

The following theorem shows that we can always give such a writing for an ideal:

Theorem 1.4 (Hilbert basis theorem)**.** *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[X]$. Their exist polynomials $f_1, \ldots, f_s \in \mathbb{K}[X]$ such that $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$.*

Affine Varieties. We are now interested in studying the common roots of the polynomials in an ideal.

Definition 1.5. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[X]$, and $\mathbb{L}$ be a field such that $\mathbb{K} \subseteq \mathbb{L}$ or $\mathbb{L} \subseteq \mathbb{K}$. The Variety defined by $\mathcal{I}$ in $\mathbb{L}$ is the set*

$$\mathbb{V}_{\mathbb{L}}(I) = \{(\mathbf{x}_1, \ldots, \mathbf{x}_n) \in \mathbb{L}^n \mid f(\mathbf{x}_1, \ldots, \mathbf{x}_n) = 0 \quad \textit{for all } f \in \mathcal{I}\}$$

When $\mathbb{L} = \overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$, $\mathbb{V}_{\mathbb{L}}(\mathcal{I})$ will be simply denoted by $\mathbb{V}(\mathcal{I})$.

Conversely, from a set of points in $\mathbb{K}^n$, we can define an ideal:

Proposition – Definition 1.6. *Let $S \subseteq \mathbb{K}^n$ be a set of points. Then the set*

$$\{f \in \mathbb{K}[X] \mid f(\mathbf{x}) = 0 \textit{ for all } \mathbf{x} \textit{ in } S\}$$

is an ideal of $\mathbb{K}[X]$ denoted by $I(S)$.

In order to explain the strong links between ideal and varieties, we have to define the radical of an ideal.

Definition – Proposition 1.7. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[X]$. We define $\sqrt{\mathcal{I}}$, the* radical *of $\mathcal{I}$, by*

$$\sqrt{\mathcal{I}} = \{f \in \mathbb{K}[X] \mid \exists \ell \in \mathbb{N}, f^\ell \in I\}$$

which is also an ideal of $\mathbb{K}[X]$. An ideal $\mathcal{I}$ is said to be radical *if $\mathcal{I} = \sqrt{\mathcal{I}}$.*

We are now able to give one of the fundamental theorem in algebraic geometry.

Theorem 1.8 (Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraic closed field, and $\mathcal{I}$ an ideal of $\mathbb{K}[X]$. Then*

$$I(\mathbb{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$$

Given two ideals I and J of $\mathbb{K}[X]$, we can define many other ideals: $I + J, I \cap J, IJ, (I : J), (I : J^\infty), \ldots$ We refer to [25] for the operations on ideals and the geometric meaning of these operations.

Zariski topology. We continue this subsection with the *Zariski topology*, that we can define on $\mathbb{K}^n$.

Definition 1.9. *A subset of $\mathbb{K}^n$ is said to be a* Zariski closed subset *if it can be written $\mathbb{V}(\mathcal{I})$ for a suitable ideal $\mathcal{I} \subseteq \mathbb{K}[X]$.*

From the operations on ideals and the links with operations on varieties, it is straightforward to verify that these subsets are the closed sets of a topology, called the *Zariski topology*. If the field $\mathbb{K}$ is infinite, the open sets of this topology are "big", which allows us to set the following definition:

Definition 1.10. *If $\mathbb{K}$ is infinite, a property $\mathcal{P}$ on $\mathbb{K}^n$ is said to be* generic *if $\{\mathbf{x} \in \mathbb{K}^n \mid \mathcal{P}(\mathbf{x})\}$ contains a non-empty Zariski open subset.*

For now, we do not know how to answer, among others, the following questions:

— Given $(f, f_1, \ldots, f_s) \in \mathbb{K}[X]^{s+1}$, decide whether f lies in $\langle f_1, \ldots, f_s \rangle$.

— Given $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$, decide whether $\mathbb{V}(\mathcal{I})$ is empty.

Gröbner bases of ideals are a computational tool which allows to solve those questions, and will be introduced in the following subsection.

Zero-dimensional ideals. This thesis mainly focuses on systems generating an ideal said to be of *Krull dimension* zero. This notion of dimension will be defined in the next chapter. These ideals are interesting since the associated variety (in the algebraic closure) is finite.

Proposition – Definition 1.11. *[25] An ideal $\mathcal{I}$ of $\mathbb{K}[X]$ is of Krull dimension zero if and only if $\mathbb{K}[X]/I$ is of finite dimension as a $\mathbb{K}$-vector space. This dimension is called the* degree *of $\mathcal{I}$, and is a bound for the number of points in $\mathbb{V}_{\overline{\mathbb{K}}}(\mathcal{I})$.*

Bounding the number of points in $\mathbb{V}_{\overline{\mathbb{K}}}(\mathcal{I})$ by the degree of $\mathcal{I}$ is sharp: equality holds for radical ideals.

1.1.2 Monomial Orderings and Gröbner bases

Degrees and monomial orderings. In order to design algorithms solving symbolically polynomial systems, we have to put an ordering on polynomial rings: this is necessary to decide what the *greatest* monomial in a given polynomial is. Since several monomial orderings use implicitly the *total degree* of a monomial, we also have to define some degrees of monomials.

Definition 1.12. *A monomial ordering $\preceq$ on $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ is a total ordering defined on the set of monomials of $\mathbb{K}[X]$ (which is isomorphic, as a monoid, to $\mathbb{N}^n$), such that:*
- *For all $\alpha, \beta, \gamma \in \mathbb{N}^n$, $x^\alpha \preceq x^\beta \Rightarrow x^{\alpha+\gamma} \preceq x^{\beta+\gamma}$*
- *Every non-empty subset of monomials has a smallest element ($\preceq$ is a well-ordering).*

Note that any ordering implies an ordering on the indeterminates $x_1, \ldots, x_n$. We usually assume that $x_1 \succ \cdots \succ x_n$. We now give the definitions of the most common orderings used in practice, namely the lexicographical and the graded reverse lexicographical orderings.

Definition 1.13. *The lexicographic ordering, denoted by $\preceq_{Lex}$, is defined by: $x^\alpha \prec_{Lex} x^\beta$ if and only if the first non-zero left entry of $\alpha - \beta$ is negative.*

Since weighted orderings will also be used in this thesis, we recall the notion of weighted degree of a monomial.

Definition 1.14. *Let $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{N}^n$. The weigted degree associated to $\mathbf{w}$ of a monomial x^α is $\deg_{\mathbf{w}}(x^\alpha) = \sum_i w_i \alpha_i$. When $\mathbf{w} = (1, \ldots, 1)$, $\deg_{\mathbf{w}}$ will simply be denoted by* deg.

Definition 1.15. *The weighted graded lexicographical ordering (abbreviated w-glex) and denoted by $\preceq_{wglex}$ is defined by: $x^\alpha \prec_{glex} x^\beta$ if and only if $\deg_{\mathbf{w}}(x^\alpha) < \deg_{\mathbf{w}}(x^\beta)$ or $\deg_{\mathbf{w}}(x^\alpha) = \deg_{\mathbf{w}}(x^\beta)$ and $x^\alpha \prec_{Lex} x^\beta$. When $\mathbf{w} = (1, \ldots, 1)$, the ordering will be simply called the* glex ordering.

Definition 1.16. *The weighted graded reverse lexicographical ordering (abbreviated w-grevlex or w-DRL) and denoted by $\preceq_{wdrl}$, is defined by: $x^\alpha \prec_{wdrl} x^\beta$ if and only if $\deg_{\mathbf{w}}(x^\alpha) < \deg_{\mathbf{w}}(x^\beta)$ or $\deg_{\mathbf{w}}(x^\alpha) = \deg_{\mathbf{w}}(x^\beta)$ and the first non-zero right entry of $\alpha - \beta$ is* **positive**. *When $\mathbf{w} = (1, \ldots, 1)$, the ordering will simply be called graded lexicographical and abbreviated grevlex or DRL.*

Definition 1.17. *Let $\mathbf{w} = (w_1, \ldots, w_n) \in (\mathbb{N}^*)^n$. A polynomial $f \in \mathbb{K}[X]$ is said to be $\mathbf{w}$-homogeneous if all its monomials share the same $\mathbf{w}$-degree. If $\mathbf{w} = (1, \ldots, 1)$, we simply say that f is homogeneous.*

Leading Monomial and Reduction. Now that we have defined ordering on monomials, we are able to define reductions of a polynomial with respect to a list of polynomials.

Definition 1.18. *Let $\preceq$ be a monomial ordering on $\mathbb{K}[X]$. For a non-zero polynomial $f = \sum c_\alpha x^\alpha \in \mathbb{K}[X]$, we define its* leading monomial, leading coefficient *and* leading term *as follows:*

- $\mathsf{LM}_\preceq(f) = \max_\preceq\{x^\alpha \mid c_\alpha \neq 0\}$
- $\mathsf{LC}_\preceq(f) = c_\alpha$ *with* $x^\alpha = \mathsf{LM}_\preceq(f)$
- $\mathsf{LT}_\preceq(f) = \mathsf{LC}_\preceq(f)\mathsf{LM}_\preceq(f)$.

Note that sometimes, terms are called monomials and conversely.

Notations 1.19. *We recall here some notations that will be used throughout this thesis, although there are not standard: let $f \in \mathbb{K}[X]$ and $\preceq$ an ordering on $\mathbb{K}[X]$. We denote by $o_\preceq(f)$ (resp. $O_\preceq(f)$) the set of linear combinations of monomials smaller (resp. smaller or equal) than $\mathsf{LM}_\preceq(f)$. This notation extends for a set of polynomials F: $o_\preceq(F) = \cap_{f\in F} o_\preceq(f)$.*

Definition 1.20. *Let $f, g \in \mathbb{K}[X]\backslash\{0\}$ and $\preceq$ a monomial ordering on $\mathbb{K}[X]$. f is said to be top-reducible by g (for the ordering $\preceq$), if $\mathsf{LM}_\preceq(g)|\mathsf{LM}_\preceq(f)$. If F is a finite subset of $\mathbb{K}[X]$, f is said to be top-reducible by F, if $\mathsf{LM}_\preceq(g)|\mathsf{LM}_\preceq(f)$ for some $g \in F$.*

With notations of previous definition, we see that in the case of top-reducibility of f by g, the polynomial $f - \frac{\mathsf{LT}_\preceq(f)}{\mathsf{LT}_\preceq(g)}g$ lies in $o_\preceq(f)$. We now describe algorithms 1.21 and 1.22 that compute reduction and full reduction of a polynomial f with respect to a list of polynomials F.

Algorithm 1.21: Reduction algorithm

Input : $f \in \mathbb{K}[X]$, $\mathsf{F} = [f_1, \ldots, f_s]$ a list of polynomials in $\mathbb{K}[X]$, a monomial ordering $\preceq$.
Output: A polynomial r such that r is not top-reducible by F and $f - r \in \langle F\rangle$

```
h := f;
i := 0;
while h ≠ 0 and i < s + 1 do
    i := i + 1;
    if h is top-reducible by f_i then
        h := h − (LT_⪯(h) / LT_⪯(f_i)) f_i;
        i := 0
return h
```

Note that the result of algorithm 1.21 (and therefore algorithm 1.22) depends on the order of the sequence F. However, when F is a *Gröbner basis*, the result is unique.

Gröbner basis. In order to give the definition of a Gröbner basis, we recall first the definition of the initial ideal of an ideal.

Definition 1.23. *Let $\mathcal{I}$ be an ideal in $\mathbb{K}[X]$ and $\preceq$ be an ordering on $\mathbb{K}[X]$. The initial ideal $\mathsf{in}_\preceq(\mathcal{I})$ of $\mathcal{I}$ with respect to $\preceq$ is defined by*

$$\mathsf{in}_\preceq(\mathcal{I}) = \langle\{x^\alpha \mid \exists f \in \mathcal{I}, x^\alpha = \mathsf{LM}_\preceq(f)\}\rangle$$

The initial ideal of an ideal is a *monomial ideal*, that is, an ideal generated by monomials. We now define what a Gröbner basis is.

Algorithm 1.22: Full-Reduction algorithm

Input : $f \in \mathbb{K}[X]$, $\mathsf{F} = [f_1, \ldots, f_s]$ a list of polynomials in $\mathbb{K}[X]$, a monomial ordering $\preceq$.
Output: A polynomial r such that no monomial of r is top-reducible by F and $f - r \in \langle F \rangle$.

```
r := 0; h := f;
while h ≠ 0 do
    h := Reduction(h, F);
    r := r + LT_≼(h);
    h := h − LT_≼(h);
return r
```

Definition 1.24. *Let $\mathcal{I}$ be an ideal in $\mathbb{K}[X]$ and $\preceq$ be an ordering on $\mathbb{K}[X]$. A Gröbner basis $\mathcal{G}$ for the ideal $\mathcal{I}$ with respect to $\preceq$ is a subset of $\mathcal{I}$ such that*

$$in_{\preceq}(\mathcal{I}) = \langle \{ LM_{\preceq}(g) \mid g \in \mathcal{G} \} \rangle$$

One fundamental property of Gröbner bases, that ensures that the outputs of both algorithms 1.21 and 1.22 do not depend on the order of the sequence $\mathsf{F} = [f_1, \ldots, f_s]$ is the following:

Proposition 1.25. *Let $\mathcal{I} \subseteq \mathbb{K}[X]$ be an ideal and $\mathcal{G}$ be a Gröbner basis of $\mathcal{I}$ for a monomial ordering $\preceq$. Let $f \in \mathbb{K}[X]$. Then*

$$f \in \mathcal{I} \qquad \Longleftrightarrow \qquad Reduction(f, \mathcal{G}) = 0$$

A Gröbner basis for a given ordering $\preceq$ of an ideal $\mathcal{I}$ is not unique with definition 1.24. However, uniqueness holds:

Definition 1.26. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[X]$, and $\mathcal{G}$ be a Gröbner basis of $\mathcal{I}$ with respect to a given ordering $\preceq$. $\mathcal{G} = \{g_1, \ldots, g_s\}$ is said to be* reduced *if no monomial of g_i is (top-)reducible by $\mathcal{G} \backslash \{g_i\}$.*

Proposition 1.27. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[X]$, and $\preceq$ be a monomial ordering on $\mathbb{K}[X]$. Then $\mathcal{I}$ has a unique reduced Gröbner basis with respect to $\preceq$.*

The next subsection is devoted to the presentation of the first historical algorithm that computes Gröbner bases.

1.1.3 Buchberger Algorithm

Buchberger algorithm dates back to 1965 and is able to compute a Gröbner basis of an ideal $\mathcal{I}$ for any ordering.

Idea. The input of the algorithm is a set of polynomials $F = \{f_1, \ldots, f_s\}$ and an ordering $\preceq$. The aim is to compute a Gröbner basis of $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ with respect to $\preceq$. At the beginning of the algorithm, the monomial ideal $\langle \{ \mathsf{LM}_{\preceq}(f) \mid f \in F \} \rangle$ is only included in $\mathsf{in}_{\preceq}(\mathcal{I})$. The idea is to increase the family F unless equality holds, according to definition 1.24. The key object is to consider critical pairs and S-polynomials of elements in F.

S-polynomials. In order to define S-polynomial, we have to recall the definition of *lowest common multiple* and *greatest common divisor* of two monomials.

Definition 1.28. *Let $m = x^\alpha$ and $m' = x^\beta$ be two monomials of $\mathbb{K}[X]$. We define*
- *the lowest common multiple of m and m' by $\mathsf{LCM}(m, m') = \prod_{i=1}^n x_i^{\max(\alpha_i,\beta_i)}$. It will be denoted by $m \vee m'$.*
- *the greatest common divisor of m and m' by $\mathsf{GCD}(m, m') = \prod_{i=1}^n x_i^{\min(\alpha_i,\beta_i)}$. It will be denoted by $m \wedge m'$.*

Note that the definition 1.28 does not depend on a choice of a monomial ordering on $\mathbb{K}[X]$.

Definition 1.29. *Let f and g be two non-zero polynomials of $\mathbb{K}[X]$ and let $\preceq$ be a monomial ordering. The S-polynomial of f and g is defined by*

$$\mathsf{Spol}(f,g) = \frac{\mathsf{LM}_\preceq(f) \vee \mathsf{LM}_\preceq(g)}{\mathsf{LT}_\preceq(f)} f - \frac{\mathsf{LM}_\preceq(f) \vee \mathsf{LM}_\preceq(g)}{\mathsf{LT}_\preceq(g)} g$$

The S-polynomial can also be defined by GCD's since $\frac{\mathsf{LM}_\preceq(f)\vee\mathsf{LM}_\preceq(g)}{\mathsf{LM}_\preceq(f)} = \frac{\mathsf{LM}_\preceq(g)}{\mathsf{LM}_\preceq(f)\wedge\mathsf{LM}_\preceq(g)}$.

Buchberger algorithm. We can now describe Buchberger algorithm 1.30. The algorithm maintains a list of *critical pairs*, which are no more than pairs of polynomials, and computes S-polynomials and reduces it with respect to the current family of polynomials. If the remainder is non-zero, it is added to the family. The algorithm stops when all critical pairs have been examined.

Algorithm 1.30: Buchberger algorithm

Input : $F = \{f_1, \ldots, f_s\}$ a finite subset of $\mathbb{K}[X]$, and a monomial ordering $\preceq$.
Output: A Gröbner basis of $\langle f_1, \ldots, f_s\rangle$ with respect to $\preceq$.

```
G := F;
L := {(f_i, f_j) | 1 ≤ i < j ≤ s}; //list of critical pairs
while L ≠ ∅ do
    Choose a critical pair P = (f, g) of L and remove P from L;
    r := Reduction(Spol(f, g), G);
    if r ≠ 0 then
        G := G ∪ {r};
        L := L ∪ {(r, f) | f ∈ G}
return G
```

The proof of algorithm 1.30 relies heavily on the following theorem:

Theorem 1.31 (Buchberger)**.** *Let G be a subset of $\mathbb{K}[X]$, graded by a monomial ordering $\preceq$. Then G is a Gröbner basis of $\langle G\rangle$ with respect to $\preceq$ if and only if*

$$\mathit{Reduction}(\mathsf{Spol}(f,g), G) = 0 \quad \text{for all } f \neq g \text{ in } G.$$

Notations 1.32. *When G is a Gröbner basis, the result of Full-Reduction(f, G) does not depend on the choice of the reductions performed in algorithm 1.21. We call the result the Normal Form of f with respect to G, which will be denoted in the sequel by $\mathsf{NF}_\preceq(f, G)$.*

1.1.4 What is Solving ?

In this subsection, we recall what solving means, in the context of Gröbner basis computation. We first give the shape of a lexicographical Gröbner basis of an ideal.

Proposition 1.33. *Let $\mathcal{I}$ be a zero dimensional ideal of $\mathbb{K}[X]$, and $\mathcal{G}_{lex}$ be the reduced Gröbner basis of $\mathcal{I}$ for the lexicographic ordering with $x_1 \succ \cdots \succ x_n$. Then $\mathcal{G}_{lex}$ has the following shape:*

$$\mathcal{G}_{lex} = \begin{cases} g_{1,1}(x_1, \ldots, x_n) \succ \cdots \succ g_{1,\ell_1}(x_1, \ldots, x_n) \\ g_{2,1}(x_2, \ldots, x_n) \succ \cdots \succ g_{2,\ell_2}(x_2, \ldots, x_n) \\ \vdots \\ g_{n-1,1}(x_{n-1}, x_n) \succ \cdots \succ g_{n-1,\ell_{n-1}}(x_{n-1}, x_n) \\ g_n(x_n) \end{cases}$$

with $\ell_i \geq 1$ for $i \in \{1, \ldots, n-1\}$, and $\mathsf{LM}_{\preceq}(g_{i,1})$ is a power of x_i for all $i \in \{1, \ldots, n\}$.

Note that the last element of the Gröbner basis is a univariate polynomial.

Solving polynomial systems with computer algebra. A polynomial system is a finite set of equations $f_1 = \cdots = f_s = 0$ with $f_i \in \mathbb{K}[X]$. Solving the system means finding the common zeros of the polynomials f_i in field $\mathbb{L}$ containing $\mathbb{K}$. Assuming that the set of solutions is finite (this is the case if and only if $\langle f_1, \ldots, f_s \rangle$ is zero dimensional), it could be understood as "giving the list of the solutions". Observe first that once a lexicographical Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ has been computed, we see that with notations of proposition 1.33, g_n is univariate, and plugging roots of g_n in $g_{n-1,1}, \ldots, g_{n-1,\ell_{n-1}}$ leads to univariate polynomials in x_{n-1}, and so on. Depending on the field $\mathbb{K}$, and on the field $\mathbb{L}$ where we are looking for solutions, several techniques could apply.

Solving in finite fields. If $\mathbb{K} = \mathbb{F}_q$ is a finite field with $q = p^r$, we may look for solutions in $\mathbb{F}_p$, in $\mathbb{F}_q$ or in $\overline{\mathbb{F}_p}$, but in each case it is possible to output the list of exact solutions: even if $\overline{\mathbb{F}_p}$ is not finite, the solutions lie in a finite extension $\mathbb{F}_{p^k}$ since they are in finite number. Manipulating elements in exact fields (like finite fields) is easy, hence we can solve the systems by computing roots of univariate polynomials. We refer for example to [107] for efficient algorithms.

Solving on $\mathbb{R}$. If $\mathbb{K} = \mathbb{R}$, dedicated algorithms compute efficiently approximations of the roots of *univariate polynomials*, with certificated errors. We refer for example to [83, 84] for the complexity of isolating real solutions and computing approximations of them. From the lexicographical Gröbner basis, we cannot apply directly the method of computing successively approximations of roots of $g_n(x_n)$, $g_{n-1}(x_{n-1}, x_n), \ldots$, since errors would be dramatically increased. But it is possible to first compute a decomposition into *triangular sets*, with for example the Lazard Lex-Triangular algorithm (see [73]), and then isolate the real roots in this tower of extensions with certificated methods, see for example [99].

Consequently, throughout this thesis, solving a polynomial system means computing the lexicographical Gröbner basis of the ideal that the system generates. In practice, applying Buchberger's algorithm in order to compute a lexicographical Gröbner basis is not satisfactory: most of the critical pairs reduce to zero; therefore this is a waste of time to consider them. Moreover, it is much faster to compute a Gröbner basis for the DRL ordering than for

the lexicographical ordering. Nowadays, the common strategy used to solve zero-dimensional polynomial systems with Gröbner bases is to use an efficient algorithm able to compute a Gröbner basis for DRL ordering, and then perform a change of ordering to obtain a lexicographical Gröbner basis. This strategy and the associated algorithms are presented in the next section.

1.2 Gröbner bases and Linear Algebra

The aim of this section is to present an efficient strategy to solve zero-dimensional systems. The first step is to compute a Gröbner basis for a graded ordering, and the most common is the DRL ordering. In [71], Lazard showed the link between linear algebra and Gröbner bases computations. Faugère presented in [34] an efficient algorithm which includes Buchberger criterions into linear algebra computations of Gröbner basis. In [35], he presented the first signature-based algorithm: the advantage of this algorithm is that no useless pairs are considered if the input is a *regular sequence* (see chapter 2). The two last algorithms have been implemented in [63], and are the most efficient algorithms to compute Gröbner bases for a graded ordering. We focus on the zero-dimensional case: the FGLM algorithm [39] can be used to compute a Gröbner basis for any ordering of a zero-dimensional ideal, once a *Normal Form* is known. This Normal Form is usually available as soon as a first Gröbner basis of the ideal has been computed. Figure 1.34 summarizes the common strategy to solve a zero-dimensional system.

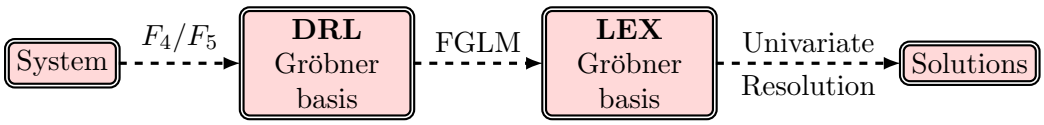


Figure 1.34 – Strategy to compute solutions of a zero-dimensional system.

In this section, we first present the link between linear algebra and Gröbner basis computation through the Lazard algorithm 1.40, and then exhibits a simplified version of Matrix-F_5 algorithm 1.44. The original one uses rewriting rules to get sparser matrices, and is itself a simplified version of the original F_5 algorithm which does not need a maximal degree to stop the computations. Since our aim is to propose some variants of this algorithm that handle algebraic structures, the simplified Matrix-F_5 is sufficient, and easier to describe. Then, we present the FGLM algorithm 1.52.

1.2.1 Lazard's algorithm and Macaulay's matrices

The aim of this subsection is to present the Lazard's algorithm, which computes a Gröbner basis for a graded ordering. In order to simplify notations, we present it only in the homogeneous case. Before giving the algorithm, we present the so-called Macaulay's matrix of a sequence of polynomials in a given degree, and then explain the authorized operations on it.

Macaulay's matrix.

Definition 1.35. *Let $\mathcal{I} \subseteq \mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ be an ideal generated by homogeneous polynomials $f_1, \ldots, f_s$, and let $\preceq$ be an ordering on $\mathbb{K}[X]$. We say that $\mathcal{G}$ is a* Gröbner basis up

to degree D *of* $\mathcal{I}$*, if*

$$\forall f \in \mathcal{I}, \quad \deg(f) \leq D \qquad \Longrightarrow \qquad \exists g \in \mathcal{G}, \quad \mathsf{LM}_{\preceq}(g) | \mathsf{LM}_{\preceq}(f)$$

An homogeneous ideal has a unique reduced Gröbner basis up to degree D. From the finitness of reduced Gröbner bases, it is clear that for D big enough, a D-Gröbner basis is a Gröbner basis. We now present the Macaulay's matrix of a finite set of polynomials, the reduction of which gives a D-Gröbner basis by Lazard's algorithm.

Definition 1.36. *Let* $\mathsf{F} = f_1, \ldots, f_s \in \mathbb{K}[X]$ *be homogeneous polynomials of degrees* $d_1, \ldots, d_s$ *and* $\preceq$ *be an ordering on* $\mathbb{K}[X]$*. Let* D *be an integer. The Macaulay's matrix* $\mathsf{Mac}_{\preceq,D}(\mathsf{F})$ *is a matrix:*

- *with* $\binom{n+D-1}{n-1}$ *columns, indexed by monomials of degree* D *of* $\mathbb{K}[X]$*, sorted by* decreasing *ordering, with respect to* $\preceq$*.*
- *with* $\sum_{i=1}^{s} \binom{n+D-d_i-1}{n-1}$ *rows, indexed by pairs* (i, m)*, where* $i \in \{1, \ldots, s\}$ *and* m *is a monomial of degree* $D - d_i$*. The index are sorted by* increasing i *first, and then by* decreasing m*.*
- *such that* $\mathsf{Mac}_{\preceq,D}(\mathsf{F})_{(i,m),m'}$ *is equal to the coefficient of* m' *in the polynomial* $f_i \times m$*.*

This definition makes sense, since for every index (i, m), the polynomial $f_i m$ is homogeneous of degree D. If $D < d_i$, the block corresponding to f_i is empty. We now present algorithm 1.40 which was presented in [71]. With a slight abuse of notations, we identify a row $\widetilde{M}_{(i,f),.}$ with the polynomial $\sum_u \widetilde{M}_{(i,f),u}$, where the sum ranges over all monomials of $\mathbb{K}[X]$ of degree D.

Gaussian Elimination in Lazard/Matrix F_5 algorithms. Both Lazard and Matrix-F_5 algorithms are based on linear algebra. The idea is to build Macaulay's matrices and perform operations on them. In this thesis, we will present several variants of Matrix-F_5, but the routines of linear algebra that we use are the same: computing a row-echelon form through Gaussian Elimination. Since the columns of the matrices are associated to monomials sorted by decreasing order, operations on the columns are not allowed. All operations on the rows are allowed: permutations, transpositions, dilatations and cancellation of zero-rows.

Definition 1.37. *Let* M *be a matrix with coefficients in* $\mathbb{K}$*.* M *is said to be in row echelon form if*

- *all nonzero rows (rows with at least one nonzero element) of* M *are above any zero row (all zero rows, if any, belong at the bottom of the matrix).*
- *the leading coefficient (the first nonzero number from the left) of a nonzero row in* M *is always strictly to the right of the leading coefficient of the row above it.*
- *all entries in a column below a leading entry of* M *are zeroes.*

Here is an example of a 4×5 matrix in row echelon form:

$$\begin{pmatrix} 1 & a_0 & a_1 & a_2 & a_3 \\ 0 & 0 & 2 & a_4 & a_5 \\ 0 & 0 & 0 & 1 & a_6 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We will see that computing a row echelon form of a Macaulay's matrix (at a degree big enough) leads to a non-reduced Gröbner basis. In order to obtain a reduced Gröbner basis (definition 1.26), we have to compute a *reduced row echelon form* of the Macaulay's matrix.

Definition 1.38. *Let M be a matrix in row echelon form. M is said to be reduced if*
- *all leading coefficients are 1.*
- *M is full rank: zero-rows have been removed.*
- *the column of a leading coefficient has only one non-zero entry: this leading coefficient.*

Here is an example of a 3×5 matrix in reduced row echelon form:

$$\begin{pmatrix} 1 & a_0 & 0 & 0 & a_1 \\ 0 & 0 & 1 & 0 & a_2 \\ 0 & 0 & 0 & 1 & a_3 \end{pmatrix}$$

Row echelon and reduced row echelon forms can be computed by Gaussian elimination. The cost of this computation is well-handled, since the following theorem holds. In this thesis, ω is the exponent of linear algebra, that is the lower bound of reals γ such that the multiplication of two $N \times N$ matrices can be performed in $O(N^\gamma)$ arithmetic operations. The best known bound is $\omega < 2.3728639$, see [50]. The complexity studies presented in this thesis only count the number of operations in $\mathbb{K}$, namely additions, subtractions, multiplications and divisions.

Theorem 1.39. *Let M be a matrix with c rows, ℓ rows, rank r and coefficients in $\mathbb{K}$. Then, a Gaussian Elimination of M can be performed within $O(\ell c r^{\omega-2})$ arithmetic operations in $\mathbb{K}$.*

Proof. We refer to [97] for a proof. □

Lazard's algorithm. We now present the Lazard's algorithm 1.40, which computes a Gröbner basis up to a degree D by computing incrementally reduced row echelon forms of Macaulay's matrices.

Algorithm 1.40: Lazard algorithm

Input : A family of homogeneous polynomials $\mathsf{F} = (f_1, \ldots, f_s)$ with degrees $d_1 \leq \ldots \leq d_s$, an ordering $\preceq$, a maximal degree D
Output: A Gröbner basis of $(f_1, \ldots, f_s)$ up to degree D, with respect to $\preceq$
$G := \emptyset$;
for $d = 1$ *to* D **do**
  Compute the Macaulay's matrix $M = \mathsf{Mac}_{\preceq,d}(\mathsf{F})$ in degree d;
  Compute $\widetilde{M}$, the reduced row-echelon form of M;
  Add to G all rows of $\widetilde{M}$ not top-reducible by G.
return G

Theorem 1.41. *Algorithm 1.40 terminates and computes a D-Gröbner basis of $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$.*

Proof. It is straightforward that algorithm 1.40 terminates since the number of loops is finite, and that the output is in $\mathcal{I}$. Now, let $f \in \mathcal{I}$ be a polynomial of degree d less than or equal to D. Since $\mathcal{I}$ is generated by homogeneous polynomials, we might assume that f is homogeneous (this will be proved in a more general context in proposition 1.65). Then f can be written $\sum_{i=1}^{s} g_i f_i$. Since f is homogeneous, the g_i's can be taken homogeneous of degree $d - d_i$. It follows that f is a linear combination of rows of the matrix $M = \mathsf{Mac}_{\preceq,d}(\mathsf{F})$. Then, one row of $\widetilde{M}$ has the same leading monomial as f. Since we add to G all rows of $\widetilde{M}$ not top-reducible

by G, $\mathsf{LM}_{\preceq}(f)$ is divisible by $\mathsf{LT}_{\preceq}(g)$ for some $g \in G$. By definition 1.35, it follows that G is a D-Gröbner basis of $\langle f_1, \ldots, f_s \rangle$. □

Lazard's algorithm based on Macaulay's matrices allows easy rough complexity study, in terms of the maximal degree of a polynomial in the reduced Gröbner basis.

Theorem 1.42. *One can compute a D-Gröbner basis of an ideal $\mathcal{I} \subseteq \mathbb{K}[X]$, generated by homogeneous polynomials $f_1, \ldots, f_s$ of degrees $d_1, \ldots, d_s$ for a given ordering $\preceq$ within*

$$O\left(s\binom{n+D}{D}^{\omega}\right)$$

arithmetic operations in $\mathbb{K}$, using Lazard algorithm 1.40.

Proof. We use the fact that by theorem 1.39, a Gaussian Elimination of a matrix M with ℓ lines, c columns, rank r and coefficients in $\mathbb{K}$ can be computed within $O(\ell c r^{\omega-2})$ arithmetic operations in $\mathbb{K}$. Since $r \leq c$, $O(\ell c^{\omega-1})$ is also a bound for this computation. Applying this to the reduction of the Macaulay's matrices occuring in algorithm 1.40, we obtain the following bounds:

$$\begin{aligned}
\sum_{d=0}^{D}\left[\left(\sum_{i=1}^{s}\binom{n+d-d_i-1}{n-1}\right)\binom{n+d-1}{n-1}^{\omega-1}\right] &\leq \sum_{d=0}^{D} s\binom{n+d-1}{n-1}^{\omega} \\
&\leq s\left(\sum_{d=0}^{D}\binom{n+d-1}{n-1}\right)^{\omega} \quad \text{since } \omega > 1 \\
&\leq s\left((D+1)\binom{n+D-1}{n-1}\right)^{\omega} \\
\sum_{d=0}^{D}\left[\left(\sum_{i=1}^{s}\binom{n+d-d_i-1}{n-1}\right)\binom{n+d-1}{n-1}^{\omega-1}\right] &\leq s\binom{n+D}{n}^{\omega}
\end{aligned}$$

and the theorem is proved. □

Corollary 1.43. *Let $f_1, \ldots, f_s$ be homogeneous polynomials in $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[X]$. If the maximal degree in a Gröbner basis of $(f_1, \ldots, f_s)$ with respect to a graded ordering $\preceq$ is lower or equal than D, then one can compute a Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ within at most $O\left(s\binom{n+D}{D}^{\omega}\right)$ operations in $\mathbb{K}$.*

From previous corollary, we see that bounding the maximal degree in a reduced Gröbner basis is of crucial importance to estimate costs in Gröbner bases computations. This will be investigated in the next chapter.

As we have seen, the Lazard algorithm 1.40 allows an easy complexity study. However, many rows reduce to zero while computing the row-echelon form of the Macaulay's matrix, which indicates that some rows are useless. The following subsection presents an algorithm which removes several useless rows, and all of them if the input sequence is a *regular sequence*. This notion will be defined in the next section.

1.2.2 Matrix-F_5 algorithm

Let $f_1, \ldots, f_s$ be a sequence of homogeneous polynomials of degrees $d_1 \leq \cdots \leq d_s$ in $\mathbb{K}[X]$, and $\preceq$ be a graded ordering on $\mathbb{K}[X]$. Among the useless rows in the Macaulay's matrix $\mathsf{Mac}_{\preceq,d}(\mathsf{F})$, some of them are easy to identify: if m is a monomial of degree $D - d_s$, which is (top-)reducible by the Gröbner basis of $f_1, \ldots, f_{s-1}$, then the row indexed by (s, m) reduces to zero. All we have to do to check this reducibility is to compute a $(D - d_s)$-Gröbner basis of $f_1, \ldots, f_{s-1}$. This can be done easily whith a slight modification of Lazard's algorithm and we obtain a very simplified version of Faugère Matrix-F_5 algorithm. Note that in practice, the algorithm is not implemented in a so simple way, since it uses rewriting rules to construct smaller and sparser matrices, for details. Mixing this approach with critical pairs criterions (as in Buchberger's algorithm) leads to the so-called F_5-algorithm see [35, 63]. In particular with the F_5-algorithm no input degree D is needed.

Algorithm 1.44: Matrix-F_5 algorithm

Input : Homogeneous polynomials $f_1, \ldots, f_s$ of degrees $d_1, \ldots, d_s$, an ordering $\preceq$, a maximal degree D

Output: Gröbner Bases of $(f_1, \ldots, f_i)$ for $i = 1, \ldots, s$ up to degree D, with respect to $\preceq$

```
for i = 1 to s do  G_i := ∅ ;
for d = d_1 to D do
    M̃_{d,0} := ∅;
    for i = 1 to s do
        if d < d_i then
            M_{d,i} := M̃_{d,i-1}
        else
            M_{d,i} := matrix obtained by adding new rows m.f_i to M̃_{d,i-1}, for all
            monomials m of degree d − d_i that do not appear as leading monomial of a
            row of M̃_{d−d_i,i−1}.
        Compute M̃_{d,i} by Gaussian elimination from M_{d,i};
        Add to G_i all rows of M̃_{d,i} not top-reducible by G_i;
return G_1, ..., G_s
```

The principle of algorithm 1.44 is simple: for each d, we contruct several matrices instead of only one like in algorithm 1.40. These matrices can be seen as Macaulay's matrices in degree d of $f_1, \ldots, f_i$ for $i \in \{1, \ldots, s\}$, but with useless rows removed and part of the row-echelon form computation already performed. The correctness of algorithm 1.44 is highly based on lemma 1.45.

Lemma 1.45 (F_5-criterion)**.** *With the notations of Algorithm 1.44, if m is the leading monomial of a row in $\widetilde{M}_{d-d_i,i-1}$ then the polynomial mf_i belongs to the vector space*

$$\mathsf{Span}_{\mathbb{K}}(Rows(\widetilde{M}_{d,i-1}) \cup \{uf_i \mid u \text{ of degree } d - d_i \text{ and } u \prec m\})$$

Proof. The hypothesis is that $\widetilde{M}_{d-d_i,i-1}$ contains a row corresponding to a polynomial of the form $h = \lambda m + o_{\preceq}(m)$, where $\lambda \neq 0$ and $o_{\preceq}(m)$ is a linear combination of monomials of degree

$d - d_i$ lower than m. Since h is contained in $\langle f_1, \ldots, f_{i-1}\rangle$, hf_i also. Then the decomposition

$$mf_i = \underbrace{hf_i/\lambda}_{\in \mathsf{Span}_{\mathbb{K}}(Row(M_{d,i-1}))} + \underbrace{o_{\preceq}(m)f_i}_{\in \mathsf{Span}_{\mathbb{K}}(\{uf_i \mid u \text{ monomial of degree } d-d_i \text{ smaller than } m\}}$$

ends the proof. □

Theorem 1.46. *Algorithm 1.44 terminates and outputs D-Gröbner bases of $\langle f_1, \ldots, f_i\rangle$ for each $i \in \{1, \ldots, s\}$.*

Proof. The termination is clear. Morover, it follows from lemma 1.45 that the row span of each matrix $M_{d,i}$ is the same as $\mathsf{Mac}_{\preceq,d}(f_1, \ldots, f_i)$, and theorem 1.41 ends the proof. □

1.2.3 FGLM algorithm

FGLM algorithm [39] was published in 1993 and named by the four names of its authors Faugère, Gianni, Lazard and Mora. From a Gröbner basis $\mathcal{G}$ of a zero dimensional $\mathcal{I}$, FGLM algorithm returns the Gröbner basis for an other ordering $\preceq_2$. The idea is simple and powerful: since $\mathcal{I}$ is zero dimensional, the quotient algebra $\mathbb{K}[X]/\mathcal{I}$ is of finite dimension δ. Thus, if we pick monomials m by increasing ordering for $\preceq_2$, the knowledge of $\mathcal{G}$ allows us to compute $\mathsf{NF}_{\preceq}(m, \mathcal{G})$. With enough monomials, we obtain linear combinations between the normal forms, which give a Gröbner basis of $\mathcal{I}$ for $\preceq_2$. In order to compute efficiently these normal forms, the algorithm uses linear algebra: it first computes the matrices M_i of the maps $f \mapsto x_i f$ in $\mathbb{K}[X]/\mathcal{I}$ for each $i \in \{1, \ldots, n\}$, using algorithm 1.47.

In algorithm 1.47, we assume that $\mathcal{I}$ is not equal to $\mathbb{K}[X]$, which can be easily checked: in this case the reduced Gröbner basis $\mathcal{G}$ for $\preceq$ of $\mathcal{I}$ is equal to $\{1\}$. We now define the *staircase* and the *boundary* of $\mathcal{G}$:

Definition 1.48. *Let $\mathcal{G}$ be the reduced Gröbner basis for $\preceq$ of an ideal $\mathcal{I} \subsetneq \mathbb{K}[X]$. We define:*
- *the* staircase *$\mathcal{E}(\mathcal{G})$ of $\mathcal{G}$ is the basis of $\mathbb{K}[X]/\mathcal{I}$ given by monomials not top reducible by $\mathcal{G}$.*
- *the* boundary *$\mathcal{B}(\mathcal{G})$ of $\mathcal{G}$ is the set $\{x_i\epsilon_k \mid 1 \leq i \leq n \text{ and } \epsilon_k \in \mathcal{E}(\mathcal{G})\}\backslash\mathcal{E}(\mathcal{G})$.*

Since $\mathcal{I}$ is zero-dimensional, the staircase $\mathcal{E}(\mathcal{G}) = \{1 = \epsilon_1 \prec \cdots \prec \epsilon_\delta\}$ is finite of cardinal $\delta = \dim_{\mathbb{K}}(\mathbb{K}[X]/\mathcal{I})$. In this case, the following proposition characterizes $\mathcal{B}(\mathcal{G})$.

Proposition 1.49. *[39] Let $\mathcal{G}$ be the reduced Gröbner basis for $\preceq$ of a zero-dimensional ideal $\mathcal{I} \subsetneq \mathbb{K}[X]$. For every $m \in \mathcal{B}(\mathcal{G})$, one and only one of the following condition holds:*

1. *For each x_i dividing m, m/x_i belongs to $\mathcal{E}(\mathcal{G})$. This is the case if and only if m is the leading monomial of an element $g \in \mathcal{G}$.*
2. *m can be written $x_i\widetilde{m}$ for some i and some $\widetilde{m} \in \mathcal{B}(\mathcal{G})$.*

Proof. The equivalence in the first point follows directly from the definition of a reduced Gröbner basis. Assume that there exists x_i dividing m such that m/x_i does not belong to $\mathcal{E}(\mathcal{G})$. Since m belongs to $\mathcal{B}(\mathcal{G})$, m can also be written $x_j\epsilon$ with $\epsilon \in \mathcal{E}(\mathcal{G})$. It follows that $i \neq j$ and x_i divides ϵ. $\mathcal{E}(\mathcal{G})$ is obviously closed under division, so $\epsilon' = \epsilon/x_i \in \mathcal{E}(\mathcal{G})$. Thus $x_j\epsilon' \in \mathcal{B}(\mathcal{G})$ because $x_j\epsilon' = m/x_i \notin \mathcal{E}(\mathcal{G})$, and the proposition is proved. □

In order to fulfill the matrices M_i, we have to compute all normal forms $\mathsf{NF}_{\preceq}(x_i\epsilon_k, \mathcal{G})$ for $1 \leq i \leq n$ and $\epsilon_k \in \mathcal{E}$. To this end, we construct the list L of all $x_i\epsilon_k$ ordered for $\preceq$ and without duplicates, the elements of which are exactly $\mathcal{E}(\mathcal{G}) \cup \mathcal{B}(\mathcal{G})$. For an element $u \in L$, we have three possible cases:

Algorithm 1.47: Multi-Mat-building algorithm

Input : A reduced Gröbner basis $\mathcal{G}$ of a zero-dimensional ideal $\mathcal{I} \subsetneq \mathbb{K}[X]$,
$\mathcal{E}(\mathcal{G}) = \{1 = \epsilon_1 \prec \epsilon_2 \prec \cdots \prec \epsilon_\delta\}$ the basis of $\mathbb{K}[X]/\langle\mathcal{G}\rangle$ given by monomials, that are not (top-)reducible by $\mathcal{G}$.

Output: Multiplication matrices of the maps $f \mapsto x_i f$ in $\mathbb{K}[X]/\langle\mathcal{G}\rangle$

for $i := 1$ **to** n **do**
  M_i :=Square matrix of size $\delta \times \delta$ filled with zeros; `//The rows of` M_i `are indexed by` $[\epsilon_1 \prec \epsilon_2 \prec \cdots \prec \epsilon_\delta]$ `and the columns by` $[x_i\epsilon_1 \prec x_i\epsilon_2 \prec \cdots \prec x_i\epsilon_\delta]$

$L := [x_i\epsilon_j \mid 1 \le i \le n, \epsilon_j \in \mathcal{E}(\mathcal{G})]$, sorted by $\preceq$ and without duplicates;

for $u \in L$ **do**
  switch u **do**
    case u *in* $\mathcal{E}$:
      $M_i[u/x_i, u] := 1$ for all i such that $x_i|u$; `//the column of` M_i `indexed by` u `has only one non-zero entry corresponding to` u/x_i.
    case $u = \mathsf{LM}_\preceq(g)$ *for some* $g \in \mathcal{G}$:
      g can be written $u + \sum_{i=1}^{\delta} \alpha_i\epsilon_i$;
      $M_i[., u] := {}^t(-\alpha_1, \ldots, -\alpha_\delta)$ for all i such that $x_i|u$
    otherwise
      Find j such that $x_j|u$ and $v = u/x_j \in L\backslash\mathcal{E}(\mathcal{G})$;
      Find (ϵ, ℓ) such that $v = x_\ell\epsilon$ with $\epsilon \in \mathcal{E}(\mathcal{G})$;
      $V := M_\ell[., v]$; `//this column of` M_ℓ `contains the expression of` $\mathsf{NF}_\preceq(v, \mathcal{G})$ `in the basis` $\mathcal{E}(\mathcal{G})$.
      $W := M_j V$; `//`W `is the vector associated to` $\mathsf{NF}_\preceq(x_j v, \mathcal{G}) = \mathsf{NF}_\preceq(u, \mathcal{G})$.
      $M_i[., u] := W$ for all i such that $x_i|u$;

return $M_1, \ldots, M_n$

— $u \in \mathcal{E}(\mathcal{G})$: no computation is needed to compute $\mathsf{NF}_\preceq(u, \mathcal{G})$, since $\mathsf{NF}_\preceq(u, \mathcal{G}) = u$.
— u is the leading monomial of $g \in \mathcal{G}$: in this case, since $\mathcal{G}$ is reduced, $\mathsf{NF}_\preceq(u, \mathcal{G}) = u - g$ and no computation is needed to obtain $\mathsf{NF}_\preceq(u, \mathcal{G})$.
— otherwise, by proposition 1.49, u can be written $x_i v$ with $v \in \mathcal{B}(\mathcal{G})$. Since L is treated incrementally in algorithm 1.47, $\mathsf{NF}_\preceq(v, \mathcal{G}) = \sum_{k=1}^{\delta} \alpha_k\epsilon_k$ has already been computed. Moreover, if $\alpha_k \neq 0$ in the previous writing, the normal form $\mathsf{NF}_\preceq(x_i\epsilon_k, \mathcal{G})$ has been computed since $x_i\epsilon_k \prec u$. It follows that $\sum_{k=1}^{\delta} \alpha_k M_i[., \epsilon_k]$ is exactly $\mathsf{NF}_\preceq(u, \mathcal{G})$ in terms of the basis $\mathcal{E}(\mathcal{G})$.

From the previous discussion, we can conclude:

Theorem 1.50. *Algorithm 1.47 terminates and outputs the matrices M_i of multiplication by x_i in $\mathbb{K}[X]/\mathcal{I}$.*

We now investigate the complexity of algorithm 1.47.

Theorem 1.51. *[39] Let $\mathcal{G}$ be the reduced Gröbner basis for an ordering $\preceq$ of a zero-dimensional ideal $\mathcal{I} \subsetneq \mathbb{K}[X]$. In order to compute the matrices M_i with algorithm 1.47 in the basis $\mathcal{E}(\mathcal{G})$, $O(n\delta^3)$ arithmetic operations in $\mathbb{K}$ are needed, with $\delta = \dim_{\mathbb{K}}(\mathbb{K}[X]/\mathcal{I})$.*

Proof. The size of the list L is bounded by $n\delta$. Only the third case requires arithmetic operations, and these operations are a matrix vector product, whose complexity is in $O(\delta^2)$. Therefore the total complexity is in $O(n\delta^3)$. □

Algorithm 1.52: Matrix-FGLM algorithm

Input : Multiplication matrices $M_1, \ldots, M_n$ of size $\delta \times \delta$ corresponding to $f \mapsto x_i f$ in $\mathbb{K}[X]/\mathcal{I}$ in a basis $\mathcal{E}_1$, an ordering $\preceq_2$
Output: The Gröbner basis of $\mathcal{I}$ for $\preceq_2$
$S := [1]$; `//The staircase` $\mathcal{E}_2$ `for the ordering` $\preceq_2$.
$L := [(1,n),(1,n-1),\ldots,(1,1)]$; `//list of pairs` (j,i) `symbolizing the monomials` $S[j] \times x_i$, `ordered by increasing order for` $\preceq_2$.
$V := [{}^t(1,0,\ldots,0)]$; `//`$V$ `contains the expressions of` $\mathsf{NF}_{\preceq_1}(S[j], \mathcal{G}_{\preceq_1})$ `in` $\mathcal{E}_1$, `each vector in` V `has` δ `components.`
$G := [\,]$; `//The Gröbner basis for` $\preceq_2$
$Q := I_\delta$; `//identity matrix of size` $\delta \times \delta$
while $L \neq [\,]$ **do**
  $m := L[1]$; Remove m from L;
  $j := m[1]$; $i := m[2]$;
  $v := M_i V[j]$; `//components of` $\mathsf{NF}_{\preceq_1}(x_i S[j], \mathcal{G}_{\preceq_1})$ `in` $\mathcal{E}_1$
  $s := |S|$; `//number of elements in` S
  $\lambda = {}^t(\lambda_1, \ldots, \lambda_\delta) := Qv$;
  if $\lambda_{s+1} = \cdots = \lambda_\delta = 0$ **then**
    $G := G \cup \left[S[j]x_i - \sum_{j=1}^{s} \lambda_j \cdot S[j] \right]$;
  else
    $S := S \cup [S[j] \times x_i]$;
    $V := V \cup [v]$;
    $L := \mathrm{Sort}\left(L \cup [(s+1,i) \mid i = 1, \ldots, n], \preceq_2\right)$;
    Remove duplicates from L;
    Update(Q, s, λ); `// Now` $Qv = {}^t(0, \ldots, 0, \underset{s+1}{1}, 0, \ldots, 0)$.
  Remove from L all multiples of $\mathsf{LM}_{\preceq_2}(G)$;
return G

We now present the FGLM algorithm 1.52. It takes as input matrices $M_1, \ldots, M_n$ of endomorphisms of multiplication by the variables $x_1, \ldots, x_n$ in $\mathbb{K}[X]/\mathcal{I}$. Usually, these endomorphisms are given in the basis $\mathcal{E}_1$ given by monomials that are not top-reducible by a first reduced Gröbner basis $\mathcal{G}_{\preceq_1}$ for $\preceq_1$. The algorithm also needs a second ordering $\preceq_2$. With the matrices, normal forms $\mathsf{NF}_{\preceq_1}(x_i m, \mathcal{G}_{\preceq_1})$ can be computed efficiently by the product $M_i v$, if v is the vector corresponding to $\mathsf{NF}_{\preceq_1}(m, \mathcal{G}_{\preceq_1}) = \sum_{i=1}^{\delta} \alpha_i \epsilon_i$. The algorithm maintains two lists S and V. S is the new staircase in construction for $\preceq_2$ and V contains the normal forms of elements of S with respect to $\mathcal{G}_{\preceq_1}$, as column vectors of size δ. At the beginning, $S = [1]$ and V contains only the first unit vector e_1 since $\mathsf{NF}_{\preceq_1}(1, \mathcal{G}_{\preceq_1}) = 1$. L is the list of monomial that have to be examined, sorted by increasing order for $\preceq_2$. After that one element m is added to the staircase S, we add to L all multiples of m by a variable. Since we compute normal forms by matrix-vector product, the elements of L are pairs (j,i) symbolizing $S[j] \times x_i$. G is the new Gröbner basis in construction and Q is a base-change matrix between the new staircase and the old one. More precisely, the following invariant is maintained during the execution of algorithm 1.52.

Lemma 1.53. *On the top of the* **while** *loop in algorithm 1.52, Q is an invertible matrix with $s = |V| = |S|$, and $QV[i] = e_i$ for all i between 1 and s.*

Proof. This statement is true when the loop is entered for the first time since $s = 1, V = [e_1]$ and Q is the identity matrix. V, S and Q are modified only in the **else** case, when $\lambda = Qv$ lies in $\mathsf{Span}_{\mathbb{K}}(e_1, \ldots, e_s)$, which means that v lies in $\mathsf{Span}_{\mathbb{K}}(V)$ since Q is invertible. Lemma 1.55 ends the proof. □

Algorithm 1.54: Update Procedure

Input : A square matrix Q of size $\delta \times \delta$, an integer s, a vector λ.
Output: The matrix Q with $Qv = {}^t(0, \ldots, 0, \underset{s+1}{1}, 0, \ldots, 0)$

$k := \min\{j \in \{s+1, \ldots, \delta\} \mid \lambda_j \neq 0\}$;
if $k \neq s+1$ **then** $Q[k,.] \leftrightarrow Q[s+1,.]$; $\lambda_k \leftrightarrow \lambda_{s+1}$;
$Q[s+1,.] \leftarrow Q[s+1,.]/\lambda_{s+1}$;
for $j = 1$ **to** δ **do**
  if $j \neq s+1$ **then** $Q[j,.] \leftarrow Q[j,.] - \lambda_j Q[s+1,.]$;
return Q

We now prove that procedure 1.54 is correct.

Lemma 1.55. *Let $Q \in \mathcal{GL}_\delta(\mathbb{K})$, $v_1, \ldots, v_s$ be s linear independent vectors with $1 \leq s < \delta$ such that Qv_i is the i-th basis vector e_i for each i. Let v be a vector such that $\lambda = Qv \notin \mathsf{Span}_{\mathbb{K}}(e_1, \ldots, e_s)$. Then after the procedure 1.54, the matrix Q remains invertible and verifies that $Qv_i = e_i$ for $i \in \{1, \ldots, s\}$ and $Qv = e_{s+1}$.*

Proof. Assume first that $\lambda_{s+1} \neq 0$. Then the effect of procedure 1.54 is to left multiply Q by the matrix $T = (t_{i,j})_{1 \leq i,j \leq \delta} \in \mathcal{M}_\delta(\mathbb{K})$ with

$$t_{s+1,s+1} = 1/\lambda_{s+1}, \quad t_{i,s+1} = -\lambda_i/\lambda_{s+1} \text{ and } t_{i,i} = 1 \text{ for } i \neq s+1, \quad t_{i,j} = 0 \text{ otherwise.}$$

Since T is invertible, Q remains invertible after the procedure. Moreover, $Te_i = e_i$ for $1 \leq i \leq s$, hence the property $Qv_i = e_i$ for $i \leq s$ remains unchanged. The fact that $T\lambda = e_{s+1}$ ends the proof. Now, if $\lambda_{s+1} = 0$, the procedure looks for the first $k > s+1$ such that $\lambda_k \neq 0$ (which exists since Qv does not belong to $\mathsf{Span}_{\mathbb{K}}(e_1, \ldots, e_s)$) and exchanges the k-th and the $(s+1)$-th rows of Q and λ. All assumptions on Q and λ are kept, but now $\lambda_{s+1} \neq 0$ and the first point concludes. □

We are now able to prove the correctness of algorithm 1.52

Theorem 1.56. *Let $\mathcal{G}_{\preceq_1}$ be the reduced Gröbner basis of a zero-dimensional ideal $\mathcal{I} \subseteq \mathbb{K}[X]$ for an ordering $\preceq_1$. Let $M_1, \ldots, M_n$ be the multiplication matrices by the variables in $\mathbb{K}[X]/\mathcal{I}$, in the basis $\mathcal{E}_1$ of monomials that are not top reducible by $\mathcal{G}_{\preceq_1}$. If $\preceq_2$ is another monomial ordering, algorithm 1.52 terminates and outputs the reduced Gröbner basis of $\mathcal{I}$ for $\preceq_2$.*

Proof. First of all, each polynomial inserted in G belongs to $\mathcal{I}$, because at this point of the algorithm, $\mathsf{NF}_{\preceq_1}(S[j]x_i - \sum_{j=1}^s \lambda_j \cdot S[j], \mathcal{G}_{\preceq_1})$ is represented in $\mathcal{E}_1$ by the column vector $v - \sum_{j=1}^s \lambda_j v_j$, but Q is invertible and $Qv = \sum_{j=1}^s \lambda_j Q v_j$ by definition of λ. Let g be a polynomial in the reduced basis of $\mathcal{I}$ for $\preceq_2$. Observe that monomials removed from L are only those which are reducible by the leading monomial of a polynomial in G. Therefore, $m = \mathsf{LM}_{\preceq_2}(g)$ is entered in the loop as a product $S[j]x_i$. All monomials of g are smaller than m and belongs to the new staircase, so they have already been treated. It follows that a linear combination is found and g is entered in G. The termination is clear from the fact that $\delta = \dim_{\mathbb{K}}(\mathbb{K}[X]/\mathcal{I})$ is finite. □

We now investigate the complexity of algorithm 1.52 in terms of n and $\delta = \dim_{\mathbb{K}}(\mathbb{K}[X])$.

Theorem 1.57. *The reduced Gröbner basis of $\mathcal{I}$ for $\preceq_2$ is computed with algorithm 1.52 within $O(n\delta^3)$ arithmetic operations in $\mathbb{K}$.*

Proof. Let $\mathcal{G}_{\preceq_2}$ be the reduced Gröbner basis of $\mathcal{I}$ with respect to $\preceq_2$. All monomials m treated in the **while** loop belongs either to $\mathcal{B}(\mathcal{G}_{\preceq_2})$ or to $\mathcal{E}(\mathcal{G}_{\preceq_2})$. It follows by the definitions that the number of those monomials is bounded by $n\delta+\delta \in O(n\delta)$. The arithmetic operations needed in the algorithm are matrix-vector products (while computing $\lambda = Qv$) and elementary operations on Q in the procedure 1.54. In both cases, the number of arithmetic operations is in $O(\delta^2)$, and the conclusion follows. □

1.3 Extension to subalgebras

In this section, we extend the notion of Gröbner basis to ideals of subalgebras of $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$, and derive a very general variant of F_5-algorithm. The aim of this generalization is to keep *structures*. In section 4.3, we will work in the subalgebra of *invariant* polynomials under the action of a group, and in chapter 5, we will work in *monomial* subalgebras of $\mathbb{K}[X]$, that is subalgebras generated by monomials. In order to generalize Gröbner bases in this context, we introduce the notion of SAGBI bases.

1.3.1 SAGBI bases

In this subsection, we recall the definition of SAGBI bases which is an analogue of Gröbner bases for ideals in *subalgebras* [68].

Definition 1.58. *[88] Let $\mathcal{A}$ be a subalgebra of $\mathbb{K}[X]$. Let $\preceq$ be any monomial ordering on $\mathbb{K}[X]$. A subset $\mathcal{S}$ of $\mathcal{A}$ is called a* SAGBI basis *(SG-basis) for $\mathcal{A}$ (relative to $\preceq$), if $\mathsf{LM}_{\preceq}(\mathcal{S})$ generates $\mathsf{LM}_{\preceq}(\mathcal{A})$ as a monoid.*

Remark 1.59. *It is worth noticing that, in contrast to ordinary Gröbner basis theory, a finite SAGBI basis does not necessarily exist. For example, the algebra $\mathbb{K}[xy^\alpha \mid \alpha \geq 0]$ has no finite SAGBI basis for lexicographical ordering with $x \succ y$.*

Basic properties of SAGBI bases are presented in [88, 79]. Although SAGBI bases are usually defined for subalgebras of $\mathbb{K}[X]$, we are interested in SAGBI bases of *ideals in subalgebras*, the definition of which is very similar to 1.58. In order to give the definition, we first describe a notion of reduction in this context.

Definition 1.60. *Let $\mathcal{A}$ be a subalgebra of $\mathbb{K}[X]$. Let $f, g, h \in \mathcal{A}$ with $f, h \neq 0$ and let P be a finite subset of $\mathcal{A}$. Then we say that*

i) f SG-reduces *to g modulo h, if there exists t a term of f, $s \in \mathcal{A}$ and $\lambda \in \mathbb{K}$ such that $\lambda \mathsf{LM}_{\preceq}(s)\mathsf{LM}_{\preceq}(h) = t$ and $g = f - \lambda sh$.*

ii) f SG-reduces to g modulo P, if f SG-reduces to g modulo h for some $h \in P$.

From this we obtain straightforwardly the definition of the following concepts: SG-reducible, SG-top-reducible*(in point i), $t = \mathsf{LT}_{\preceq}(f)$ and* SG-NormalForm. *The SG-Normal Form of a polynomial f with respect to a set of polynomials F will be denoted $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(f, F)$.*

Definition 1.61. *Let $\mathcal{A}$ be a subalgebra of $\mathbb{K}[X]$, $\mathcal{I}^{\mathcal{A}}$ an ideal* in *$\mathcal{A}$, and let $\preceq$ be any monomial ordering on $\mathbb{K}[X]$. A subset $\mathcal{S}$ of $\mathcal{I}^{\mathcal{A}}$ is called a SG-basis for $\mathcal{I}^{\mathcal{A}}$ with respect to $\preceq$ if all polynomials in $\mathcal{I}^{\mathcal{A}}$ are SG-top-reducible by $\mathcal{S}$.*

Remark 1.62. *If $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]$, we recover the definition of a Gröbner basis.*

One fundamental property of SG-basis is the following, similar to the same property for Gröbner basis.

Proposition 1.63. *Let $\mathcal{A}$ be a subaglebra of $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. For a subset $\mathcal{S}$ of an ideal (in $\mathcal{A}$) $\mathcal{I}^{\mathcal{A}} \subseteq \mathcal{A}$ the following properties are equivalent :*

a) $\mathcal{S}$ is a SG-basis for $\mathcal{I}^{\mathcal{A}}$ with respect to $\preceq$.

b) For every $h \in \mathcal{I}^{\mathcal{A}}$, $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(h, \mathcal{S}) = 0$.

Corollary 1.64. *A SG-basis for $\mathcal{I}^{\mathcal{A}}$ generates $\mathcal{I}^{\mathcal{A}}$ as an ideal of $\mathcal{A}$.*

We now assume that the algebra $\mathcal{A}$ is non-negatively graded and connected, which means that $\mathcal{A}$ can be written (as the direct sum of $\mathbb{K}$-vector spaces) $\mathcal{A} = \oplus_{d=0}^{+\infty} \mathcal{A}_d$ with $\mathcal{A}_d \mathcal{A}_{d'} \subseteq \mathcal{A}_{d+d'}$ for all $d, d' \geq 0$, and $\mathcal{A}_0 = \mathbb{K}$. We say that an element of $\mathcal{A}_d$ is homogeneous of degree d. Furthermore, we assume that $\mathcal{A}$ is finitely generated: there exists a collection of elements $h_1, \ldots, h_r$ such that $\mathcal{A} = \mathbb{K}[h_1, \ldots, h_r]$. Such an algebra is always *Noetherian*, which means that every ideal $\mathcal{I}^{\mathcal{A}}$ of $\mathcal{A}$ is finitely generated and can be written $\mathcal{I}^{\mathcal{A}} = \langle f_1, \ldots, f_s \rangle_{\mathcal{A}}$. Before giving a variant of F_5-algorithm adapted to this context, we give the following proposition:

Proposition 1.65. *Let $f_1, \ldots, f_s$ be homogeneous polynomials of degrees $d_1, \ldots, d_s$ in $\mathcal{A} = \oplus_{d=0}^{+\infty} \mathcal{A}_d$. Let $\mathcal{I}^{\mathcal{A}} = \langle f_1, \ldots, f_s \rangle_{\mathcal{A}}$ be the ideal generated by $f_1, \ldots, f_s$ in $\mathcal{A}$. Let $f \in \mathcal{I}^{\mathcal{A}}$ and $\sum_{d=0}^{+\infty} f^{(d)}$ be its unique decomposition in homogeneous components, with $f^{(d)} \in \mathcal{A}_d$ (all $f^{(d)}$ but a finite number of them are equal to zero). Then, all $f^{(d)}$ belong to $\mathcal{I}^{\mathcal{A}}$.*

Proof. Since f lies in $\mathcal{I}^{\mathcal{A}}$, f can be written $f = \sum_{i=1}^{s} g_i f_i$ with $g_i \in \mathcal{A}$. Let $g_i^{(d)}$ be the component of g_i of degree d (all $g_i^{(d)}$ but a finite number of them are zero). Then $g_i = \sum_{d=0}^{\infty} g_i^{(d)}$ and

$$\sum_{d=0}^{+\infty} f^{(d)} = f = \sum_{i=1}^{s} g_i f_i = \sum_{i=1}^{s} \sum_{d=0}^{+\infty} g_i^{(d)} f_i = \sum_{d=0}^{+\infty} \left(\sum_{(\ell, d_i) \text{ such that } \ell + d_i = d} g_i^{(\ell)} f_i \right)$$

then $f^{(d)} = \sum_{\ell + d_i = d} g_i^{(\ell)} f_i$ is the homogeneous component of f of degree d, which belongs to $\mathcal{I}^{\mathcal{A}}$. □

An ideal generated by homogeneous polynomials is called homogeneous. For such an ideal, the proposition 1.63 above continues to hold if we restrict our discussion to SG-bases up to some degree D. Hence, only a SG-basis up to degree D of $\mathcal{I}^{\mathcal{A}}$ is needed to test the membership in $\mathcal{I}^{\mathcal{A}}$ for any polynomial f with $\deg(f) \leq D$.

Assume now that a basis $(b_i^d)_{d \geq 0, 1 \leq i \leq n_d}$ of the graded algebra $\mathcal{A}$ is given, such that two elements of this basis have distinct leading monomial.

Definition – Proposition 1.66. *A element (b_i^d) of the basis of $\mathcal{A}$ is called standard if $\mathsf{LM}_{\preceq}(b_i^d) \notin \mathsf{LM}_{\preceq}(\mathcal{I}^{\mathcal{A}})$. $\mathcal{A}$ is the direct sum of $\mathcal{I}^{\mathcal{A}}$ and the vector space spanned by the standard elements. Hence, the SG-NormalForm of an invariant f is necessarily a unique linear combination of standard elements (b_i^d).*

1.3.2 Matrix SAGBI-F5 algorithm

Now we give a description of the SAGBI-F_5 algorithm. We consider a graded subalgebra $\mathcal{A}$ of $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$, which is connected and finitely generated.

The SAGBI-F_5 algorithm is very close to the original F_5-algorithm, but it works in $\mathcal{A}$ instead of $\mathbb{K}[X]$. We present here a Matrix SAGBI-F_5 algorithm, which uses *SAGBI-Macaulay's matrices*. We use the same notations, $f_1, \ldots, f_s$ are homogeneous polynomials in $\mathcal{A}$ of degree $d_1 \leq \cdots \leq d_s$, and $\preceq$ is a graded ordering. We assume that in every component $\mathcal{A}_d$, a basis $(b_i^d)_{1 \leq i \leq n_d}$ of $\mathcal{A}$ as a $\mathbb{K}$-vector space has been computed, with $\mathsf{LM}_\preceq(b_1^d) \succ \mathsf{LM}_\preceq(b_2^d) \succ \cdots \succ \mathsf{LM}_\preceq(b_{n_d}^d)$.

Definition 1.67. *Let $F = f_1, \ldots, f_s \in \mathcal{A}$ be homogeneous polynomials of degrees $d_1, \ldots, d_s$ and $\preceq$ be an ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let D be an integer. The SAGBI-Macaulay's matrix $\mathsf{Mac}^{\mathcal{A}}_{\preceq,D}(F)$ is a matrix:*

- *with $\dim_{\mathbb{K}}(\mathcal{A}_D)$ columns, indexed by polynomials $(b_k^d)_{1 \leq k \leq n_d}$ sorted by $\preceq$ with decreasing order.*
- *with $\sum_{i=1}^{s} \dim_{\mathbb{K}}(\mathcal{A}_{D-d_i})$ rows, indexed by pairs $(i, b_j^{d-d_i})$, where $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, n_{d-d_j}\}$, so that $b_k^{d-d_j}$ ranges all the basis of $\mathcal{A}_{d-d_j}$. The indexes are sorted by* increasing *i first, and then by* decreasing *$b_j^{d-d_i}$.*
- *such that $\mathsf{Mac}^{\mathcal{A}}_{\preceq,D}(F)_{(i,b_j^\ell),b_k^D}$ is equal to the coefficient of α_k in the writing $f_i b_j^\ell = \sum_{k=1}^{n_D} \alpha_k b_k^D$.*

Just like the classical Matrix-F_5-algorithm 1.44, the SAGBI-F_5 algorithm constructs matrices incrementally degree by degree and equation by equation, and remove from the SAGBI-Macaulay matrix some useless rows. At each degree d the algorithm constructs a SAGBI-Macaulay's matrix $M_{d,i}$ and performs row reductions on it, the valid operations being to add to some row a linear combinations of rows situed above. The incremental step from $i-1$ to i introduces the rows corresponding to $b_j^{d-d_i} f_i$ for all polynomials of $(b_j^{d-d_i})$ in the basis of $\mathcal{A}_{d-d_j}$, except those having same leading monomial as a row of $\widetilde{M}_{d-d_i,i-1}$, where $d_i = \deg(f_i)$. This criterion is a variant of the F_5-criterion 1.45 and is explained in lemma 1.69. The algorithm stops when the current degree is equal to a given bound D.

Lemma 1.69. *[SAGBI-F_5 criterion] If $m = \mathsf{LM}_\preceq(b_\ell^{d-d_i})$ is the leading monomial of a row in $\tilde{M}_{d-d_i,i-1}$ then the polynomial $b_\ell^{d-d_i} f_i$ belongs to the vector space*

$$\mathsf{Span}_{\mathbb{K}}(Row(M_{d,i-1})) + \mathsf{Span}_{\mathbb{K}}(\{b_j^{d-d_i} f_i \mid j > \ell\})$$

Proof. The hypothesis is that $\tilde{M}_{d-d_i,i-1}$ contains a row corresponding to a polynomial of the form $h = \lambda b_\ell^{d-d_i} + o_\preceq(b_\ell^{d-d_i})$, where $\lambda \neq 0$ and $o_\preceq(b_\ell^{d-d_i})$ is a linear combination of polynomials in $\mathcal{A}_{d-d_i}$ of leading monomial lower than $\mathsf{LM}_\preceq(b_\ell^{d-d_i})$. Since h is contained in $\langle f_1, \ldots, f_{i-1} \rangle_{\mathcal{A}}$, hf_i also. Then the decomposition

$$b_\ell^{d-d_i} f_i = \underbrace{hf_i/\lambda}_{\in \mathsf{Span}_{\mathbb{K}}(Row(M_{d,i-1}))} + \underbrace{o_\preceq(b_\ell^{d-d_i}) f_i}_{\in \mathsf{Span}_{\mathbb{K}}(\{b_j^{d-d_i} f_i \mid j > \ell\})}$$

ends the proof. □

Theorem 1.70. *The SAGBI-F_5 algorithm computes the elements of degree at most D of the reduced SG-bases of $\langle f_1, \ldots, f_i \rangle_{\mathcal{A}}$, for $i = 1, \ldots, t$.*

Algorithm 1.68: Matrix SAGBI-F_5

Input : invariant homogeneous polynomials $f_1, \dots, f_s$ with degrees $d_1, \dots, d_s$, a maximal degree D, bases $(b_i^d)_{1 \le i \le n_d}$ of $\mathcal{A}_d$ for $0 \le d \le D$.
Output: SG-bases of $\langle f_1, \dots, f_i \rangle_{\mathcal{A}}$ for $i = 1, \dots, s$ up to degree D

```
for i = 1 to s do S_i := ∅ ;
for d = d_1 to D do
    M̃_{d,0} := ∅;
    for i = 1 to s do
        if d < d_i then
            M_{d,i} := M̃_{d,i-1}
        else
            M_{d,i} := matrix obtained by adding new rows b_j^{d-d_j}.f_i to M̃_{d,i-1}, for all
            polynomials in the basis (b_j^{d-d_i}) of A_{d-d_i} that do not have same leading
            monomial of a row of M̃_{d-d_i,i-1}.
        Compute M̃_{d,i} by Gaussian elimination from M_{d,i};
        Add to S_i all rows of M̃_{d,i} not SG-top reducible by S_i;
return S_1, ..., S_s
```

Proof. We will use induction on d and i. For $d = d_1$ and $i = 1$, the result is clear. Assuming the induction hypothesis, we now simply have to prove that the rows of $M_{d,i}$ generate $\langle f_1, \dots, f_i \rangle_d$. Then we can deduce that $\mathsf{LM}_{\preceq}(\tilde{M}_{d,i})$ generates $\mathsf{LM}_{\preceq}(\langle f_1, \dots, f_i \rangle_d)$ and the conclusion on $\mathcal{S}_i$ follows. It is thus sufficient to prove that for any polynomial $(b_\ell^{d-d_i})$ of the basis of $\mathcal{A}_{d-d_i}$, the polynomial $b_\ell^{d-d_i} f_i$ is generated by the rows of $M_{d,i}$. If $m \in \mathsf{LM}_{\preceq}(\tilde{M}_{d-d_i,i-1})$ it is clear by lemma 1.69 and construction of the matrix $M_{d,i}$. Otherwise, $b_\ell^{d-d_i} f_i$ is entered by the algorithm in $M_{d,i}$. This completes the proof of the theorem. □

This SAGBI-F_5 algorithm will be used in the sequel in two contexts: when $\mathcal{A}$ is the algebra of invariants on a finite group $\mathbf{G}$ (section 4.3) and when $\mathcal{A}$ is a monomial algebra (chapter 5). Notice that generalizing the Matrix-F_5 algorithm in this framework is easy, whereas giving a generalization of Buchberger algorithm is not: the notion of S-polynomials does not generalize easily. Even in monomial subalgebras, the notion of lowest common multiple of two monomials does not hold anymore and has to be replaced by a list of multiples.

Chapter 2

Commutative Algebra. Applications to Gröbner Bases

In this chapter, we first introduce classical results in commutative algebra. Then, we use these concepts to study the behavior of the SAGBI-F_5 algorithm with respect to *regular and semi-regular sequences*. As we have seen in theorem 1.42, it is crucial to bound the maximal degree reached during a Gröbner basis computation, since it appears in the complexity bound. In this section, we show how the maximal degree reached in a computation can be estimated.

2.1 Commutative Algebra and Hilbert series

Commutative algebra has been first introduced by Hilbert, in order to study the structure of the algebra of polynomial invariants under the action of a group that we will wiew in the next chapter. In this section, we first present basic tools of commutative algebra and then study gradings on subalgebras of the ring of Laurent polynomials, and introduce the concept of *Hilbert series*.

2.1.1 Algebraic tools.

In this subsection, we consider an algebra $\mathcal{A}$ which is non-negatively graded, connected and finitely generated, as in section 1.3. Thus $\mathcal{A}$ can be written $\oplus_{d=0}^{\infty}\mathcal{A}_d$ with $\mathcal{A}_0 = \mathbb{K}$ and $\mathcal{A}_d$ a $\mathbb{K}$-vector space of finite dimension for all $d \geq 0$. The notions introduced here can be found in several books, see for example Eisenbud [30] or Lang [70].

Krull dimension. Recall that an ideal $\mathcal{I}$ of $\mathcal{A}$ is said to be homogeneous if it is generated by homogeneous polynomials. In this case both $\mathcal{I}$ and $\mathcal{A}/\mathcal{I}$ are graded (see proposition 2.14).

$$\mathcal{I} = \oplus_{d=0}^{\infty}\mathcal{I}_d \qquad \text{and} \qquad \mathcal{A}/\mathcal{I} = \oplus_{d=0}^{\infty}\mathcal{A}_d/\mathcal{I}_d$$

Notice that $\mathcal{A}_+ = \oplus_{d=1}^{\infty}\mathcal{A}_d$ is the unique homogeneous maximal ideal of $\mathcal{A}$.

If $\mathfrak{P}$ is a prime ideal of $\mathcal{A}$, we define the *height* of $\mathfrak{P}$ to be the maximal length ℓ such that their exists a chain $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \cdots \subsetneq \mathfrak{P}_\ell = \mathfrak{P}$ of prime ideals of $\mathcal{A}$ contained in $\mathfrak{P}$. This number is denoted by $\text{height}(\mathfrak{P})$ and is extented to any ideal $\mathcal{I}$ of $\mathcal{A}$ by

$$\text{height}(\mathcal{I}) = \min\{\text{height}(\mathfrak{P}) \mid \mathcal{I} \subseteq \mathfrak{P} \quad \text{and} \quad \mathfrak{P} \text{ is prime}\}$$

Finally, the *Krull dimension* of $\mathcal{A}$ is defined by

$$\dim_{\text{Krull}}(\mathcal{A}) = \sup\{\ell \mid \mathfrak{P} \text{ is a prime ideal of } \mathcal{A} \text{ of height } \ell\}$$

Example 2.1. *A polynomial algebra $\mathbb{K}[x_1, \ldots, x_n]$ has Krull dimension n. The ring of invariants $\mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$ under a finite group $\mathbf{G}$ (see section 3.1) or a semigroup algebra $\mathbb{K}[S]$ with S a full rank semigroup of $\mathbb{Z}^n$ (see section 3.2) have also Krull dimension n.*

If $\mathcal{I}$ is a proper ideal of $\mathcal{A}$, one can consider the Krull dimension of the algebra $\mathcal{A}/\mathcal{I}$. This dimension is called the *dimension* of $\mathcal{I}$, denoted by $\dim(\mathcal{I})$. In several classical books, this dimension is called the codimension of $\mathcal{I}$, but this is not the common usage in Gröbner area.

Homogeneous Systems of parameters and Regular sequences. We now define what a *homogeneous system of parameters* (abbreviated hsop) of the algebra $\mathcal{A}$ is.

Definition 2.2. *Let n be the Krull dimension of $\mathcal{A}$. A homogeneous system of parameters of $\mathcal{A}$ is a set of n homogeneous elements $\{h_1, \ldots, h_n\}$ such that $\mathcal{A}$ is a a finitely generated module over the ring $\mathbb{K}[h_1, \ldots, h_n]$.*

The following result was first introduced by Hilbert, in order to study the algebra of invariants under the action of a group. Is was named after Emmy Noether proved it in [80].

Theorem 2.3 (Noether Normalization lemma)**.** *The algebra $\mathcal{A}$ has a homogeneous system of parameters.*

This theorem has useful applications in invariant theory of finite groups, see chapter 3.

We now define *regular sequences* in $\mathcal{A}$. These sequences are of great importance in Gröbner bases computations: for homogeneous such sequences in $\mathbb{K}[X]$, there are no reduction to zero in F_5-algorithm, and the maximal degree reached during the computation can be efficiently bounded, as we will see in the sequel.

Definition 2.4. *A sequence $(f_1, \ldots, f_s)$ in $\mathcal{A}$ is called a* regular sequence *if $\langle f_1, \ldots, f_s\rangle_{\mathcal{A}} \subsetneq \mathcal{A}$ and f_i does not divide zero in the ring $\mathcal{A}/\langle f_1, \ldots, f_{i-1}\rangle_{\mathcal{A}}$ for all $1 \leq i \leq s$. For $i = 1$, this means that f_1 is not a zero-divisor in $\mathcal{A}$, therefore is non-zero if $\mathcal{A}$ is a domain.*

Example 2.5. *In $\mathbb{K}[x_1, \ldots, x_n]$, $(x_1, \ldots, x_n)$ is a regular sequence.*

Remark 2.6. *The property of being regular for a sequence of polynomials strongly depends on the algebra to which they belong. For exemple, let $\mathbb{K}[X] = \mathbb{K}[x, y]$ and $\mathcal{A}$ the algebra generated in $\mathbb{K}[X]$ by x and xy. It is easy to prove that a monomial $x^\alpha y^\beta$ belongs to $\mathcal{A}$ if and only if $\beta \leq \alpha$. Then the sequence $(f_1, f_2) = (x, xy)$ is $\mathcal{A}$-regular but not regular:*

- *Let g_1, g_2 be such that $f_1 g_1 = f_2 g_2$. Since f_1 and f_2 are monomials we can assume that g_1 and g_2 also. Then g_1 is of the form $x^\alpha y^{\beta+1}$ and $g_2 = x^\alpha y^\beta$, with $\alpha \geq \beta + 1$. Therefore, $g_2 = f_1 x^{\alpha-1} y^\beta \in \langle f_1\rangle_{\mathcal{A}}$, and $g_2 = 0 \in \mathcal{A}/\langle f_1\rangle$ and f_2 does not divide 0 in $\mathcal{A}/\langle f_1\rangle$ so (f_1, f_2) is $\mathcal{A}$-regular.*
- *But $f_2 = 0 \in \mathcal{A}/\langle f_1\rangle$ so (f_1, f_2) is not $\mathbb{K}[X]$-regular.*

In the previous definition, the integer s is called the *length* of the sequence. If $\mathcal{A}$ is Noetherian, the sequence of ideals $\langle f_1\rangle_{\mathcal{A}} \subsetneq \langle f_1, f_2\rangle_{\mathcal{A}} \subsetneq \langle f_1, \ldots, f_s\rangle_{\mathcal{A}}$ is striclty increasing and so cannot be extended infinitely many times. A regular sequence that cannot be extended is called *maximal*.

In the definition of regular sequence, it seems that the order of the f_i matters. Indeed, a regular sequence does not necessarily remain regular when permuted, see [64, page 102]. However, this is the case for regular *homogeneous* sequences. This will be proved in the particular case $\mathcal{A} \subset \mathbb{K}[X^{\pm 1}]$ in the sequel. We refer to [16, chapter 2] for a general proof.

Cohen-Macaulay rings. Based on the definition of regular sequences, we now define Cohen-Macaulay rings. Working in those rings are of great importance since it ensures that being a maximal regular sequences is a *generic* property (see definition 1.10): roughly speaking, almost all sequences of length equal to the Krull dimension of the ring are regular.

Proposition – Definition 2.7. *Let $\mathcal{A} = \bigoplus_{d\in\mathbb{N}} \mathcal{A}_d$ be a graded connected finitely generated algebra. Let $\mathcal{I}$ be an ideal of $\mathcal{A}$. Then all maximal regular sequences lying in $\mathcal{I}$ have same length, called the* depth *of $\mathcal{I}$ and denoted by* $\operatorname{depth}(\mathcal{I})$. *The ideal $\mathfrak{m} = \bigoplus_{d\in\mathbb{N}^*} \mathcal{A}_d$ is a maximal ideal of $\mathcal{A}$. The* depth *of $\mathcal{A}$ is the maximal length of a regular sequence of $\mathcal{A}$ lying in $\mathfrak{m}$, denoted by* $\operatorname{depth}(\mathcal{A})$.

The following proposition relies the dimension of an ideal with its depth.

Proposition 2.8. *With notations of the previous propostion-definition, for any ideal $\mathcal{I}$ of $\mathcal{A}$,* $\operatorname{depth}(\mathcal{I}) \leq \dim(\mathcal{I})$, *where* $\dim(\mathcal{I})$ *is the Krull dimension of the algebra $\mathcal{A}/\mathcal{I}$.*

We are now able to give the definition of a Cohen-Macaulay algebra: equality holds in the previous proposition.

Definition 2.9. *With notations of proposition-definition 2.7, the algebra $\mathcal{A}$ is said to be* Cohen-Macaulay *if* $\operatorname{depth}(\mathfrak{m}) = \dim(\mathfrak{m})$ *for every maximal ideal $\mathfrak{m}$ of $\mathcal{A}$.*

Example 2.10. *The algebra $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ is Cohen-Macaulay, since $(x_1, \ldots, x_n)$ is a regular sequence. In the non-modular case, the ring of invariants $\mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$ under a finite group $\mathbf{G}$ is Cohen-Macaulay, see section 3.1. Hochster's theorem (see section 3.2) says for example that the algebra $\mathbb{K}[xy, xy^2, x^2y]$ is Cohen-Macaulay.*

Hilbert Syzygy theorem. We end up this subsection with the *Hilbert Syzygy theorem*, which is one of the fundamental theorem in commutative algebra. The grading on $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ is given by the classical total degree.

Theorem 2.11 (Hilbert Syzygy Theorem)**.** *[30, theorem 1.13] Let M be any finitely graded module over a polynomial ring $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]$. Then, there exists a* finite graded resolution *of M by free graded $\mathbb{K}[X]$-modules*

$$0 \to M_k \xrightarrow{\rho_k} M_{k-1} \xrightarrow{\rho_{k-1}} \cdots \xrightarrow{\rho_1} M_0 \xrightarrow{\rho_0} M \to 0,$$

that is an exact sequence*: $\ker(\rho_i) = \operatorname{im}(\rho_{i+1})$ for all $i \in \{0, \ldots, k-1\}$, ρ_k injective and ρ_0 surjective. The length k of the resolution can be chosen less than or equal to n.*

This theorem will we applied in the sequel, a consequence is that the *Hilbert series* of a ideal in $\mathbb{K}[X]$ is a rational fraction.

2.1.2 Gradings on subalgebras of $\mathbb{K}[X^{\pm 1}]$

In this thesis, we have to consider several algebras. In chapters 3 and 4, we will deal with $\mathbb{K}[X]^{\mathbf{G}}$, the algebra of invariants under the action of a finite group $\mathbf{G}$, which is a subalgebra of $\mathbb{K}[X]$, graded by the total degree on $\mathbb{K}[X]$. We will also have to consider the whole algebra $\mathbb{K}[X]$, but the action of an abelian group, joined to the total degree, gives a grading by the commutative monoid $\mathbb{N} \times \mathbf{X}(\mathbf{G})$ where $\mathbf{X}(\mathbf{G})$ is an abelian finite group. In chapter 5, we will study polynomial systems in $\mathbb{K}[S]$, a subalgebra of the ring of *Laurent polynomials* $\mathbb{K}[X^{\pm 1}]$, where S is a semigroup of $\mathbb{Z}^n$. This subalgebra will be graded by $\mathbb{N}$. Quasi-homogeneous and multihomogeneous gradings are also classical gradings on $\mathbb{K}[X]$, given by $\mathbb{N}$ or $\mathbb{N}^\ell$.

In order to give a theoretical framework, which is valid for all these algebras, we fix a commutative monoid $\mathbb{M}$ with neutral e, which can be seen as one of the mentioned monoids.

Definition 2.12. *Let $\mathcal{A}$ be a subalgebra of $\mathbb{K}[X^{\pm 1}]$. A grading indexed by $\mathbb{M}$ on $\mathcal{A}$ is a decomposition of $\mathcal{A}$ into graded components $(\mathcal{A}_d)_{d\in\mathbb{M}}$ such that:*
- *$\mathcal{A}_e = \mathbb{K}$.*
- *$\mathcal{A} = \bigoplus_{d\in\mathbb{M}} \mathcal{A}_d$ as a $\mathbb{K}$ vector space.*
- *Let $d, d' \in \mathbb{M}$ and $(f, h) \in \mathcal{A}_d \times \mathcal{A}_{d'}$. Then $fh \in \mathcal{A}_{d+d'}$.*

A polynomial f in a component $\mathcal{A}_d$ is said to be $\mathbb{M}$-homogeneous of $\mathbb{M}$-degree d.

We fix such a subalgebra $\mathcal{A}$ graded by $\mathbb{M}$ and see how this grading can be transfered on homogeneous ideals of $\mathcal{A}$ and associated quotient algebras.

Definition 2.13. *An ideal $\mathcal{I} \subseteq \mathcal{A}$ is said to be $\mathbb{M}$-homogeneous if it is generated by homogeneous elements.*

Proposition 2.14. *Let $\mathcal{I}$ be a $\mathbb{M}$-homogeneous ideal of $\mathcal{A}$. Then, both $\mathcal{I}$ and $\mathcal{A}/\mathcal{I}$ have a decomposition into graded components:*

$$\mathcal{I} = \bigoplus_{d\in\mathbb{M}} \mathcal{I}_d \qquad \text{and} \qquad \mathcal{A}/\mathcal{I} = \bigoplus_{d\in\mathbb{M}} (\mathcal{A}/\mathcal{I})_d$$

Proof. For $\mathcal{I}$, it simply comes from the fact that the homogeneous components of a polynomial in $\mathcal{I}$ belong to $\mathcal{I}$, and the proof is identitical to proposition 1.65. For $\mathcal{A}/\mathcal{I}$, we have a surjective map $\varphi : \mathcal{A} \to \oplus_{d\in\mathbb{M}}(\mathcal{A}_d/\mathcal{I}_d)$. Clearly, $\ker(\varphi) \subseteq \mathcal{I}$, and the reverse inclusion comes from the previous point. □

From now on, until the end of the subsection, we consider gradings on the polynomial ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. A very interesting case is when a basis (as a $\mathbb{K}$-vector space) of each component $\mathbb{K}[X]_d$ is given by monomials. In this case the computation of Gröbner bases preserves this grading, in the following sense.

Proposition 2.15. *Assume that $\mathbb{K}[X]$ is graded by a monoid $\mathbb{M}$ as in definition 2.12, and that $\mathbb{K}[X]_d$ is generated by monomials for each d. Then for each monomial m of degree d_m and $\mathbb{M}$-homogeneous polynomials f and h of degrees d_f and d_h:*
- *the polynomial mf is $\mathbb{M}$-homogeneous of degree $d_m + d_f$.*
- *$\mathsf{Spol}(f, g)$, the S-polynomial (see definition 1.29) of f and g, is $\mathbb{M}$-homogeneous of same degree as $\mathsf{LM}_{\preceq}(f) \vee \mathsf{LM}_{\preceq}(g)$*

Proof. This is obvious with the definition of the $\mathbb{M}$-degree. □

We review in the following some classical gradings on $\mathbb{K}[X]$, here $\mathbb{M}$ is equal to $\mathbb{N}^\ell$, with $\ell \geq 1$.

Definition 2.16. *We define quasi-homogeneous and multi-homogeneous gradings*
- *Let $\mathbf{w} = (w_1, \ldots, w_n) \in (\mathbb{N}^*)^n$ and for all $d \in \mathbb{N}$, let*

$$\mathbb{K}[X]_d^{\mathbf{w}} = \mathsf{Span}_K(\{x^\alpha \text{ monomial } \mid \deg_{\mathbf{w}}(x^\alpha) = d\})$$

  This component (which can be reduced to $\{0\}$) is said to be the quasi-homogeneous component of degree d associated to $\mathbf{w}$. A polynomial is said to be quasi-homogeneous of degree d (with respect to $\mathbf{w}$) if it lies in $\mathbb{K}[X]_d^{\mathbf{w}}$.
- *Let $n_1, \ldots, n_\ell \in \mathbb{N}^*$ such that $\sum n_i = n$, and $X = X_1 \cup \cdots \cup X_\ell$ be a partition of the set of variables $X = \{x_1, \ldots, x_n\}$. Then, for all $\mathbf{d} = (d_1, \ldots, d_\ell) \in \mathbb{N}^\ell$, let*

$$\mathbb{K}[X]_{\mathbf{d}} = \mathbb{K}[X_1]_{d_1} \otimes \cdots \otimes \mathbb{K}[X_\ell]_{d_\ell}$$

  This component is said to be the multi-homogeneous component of $\mathbb{K}[X]$ of multi-degree $\mathbf{d}$, with respect to the partition $X = X_1 \cup \cdots \cup X_\ell$

Note that, with $\mathbf{w} = (1, \dots, 1)$ *in the first case, or* $X = X_1$ *and* $\mathbf{d} = (1)$ *in the last case, we recover the standard homogeneous grading on* $\mathbb{K}[X]$.

For ideals in $\mathbb{K}[X]$, we deduce from proposition 2.14 the following definitions:

Definition 2.17. *With notations of definition 2.16, and ideal* $I \subset \mathbb{K}[X]$ *is called*
- quasi-homogeneous *with respect to* $\mathbf{w} \in \mathbb{N}^n$ *if* $\mathcal{I} = \oplus_{d=0}^{\infty} \mathcal{I}_d^{\mathbf{w}}$, *where* $\mathcal{I}_d^{\mathbf{w}} = \mathbb{K}[X]_d^{\mathbf{w}} \cap \mathcal{I}$.
- multi-homogeneous *with respect to a partition* $X = \cup_{i=1}^{\ell} X_i$ *if* $\mathcal{I} = \oplus_{\mathbf{d} \in \mathbb{N}^\ell} \mathcal{I}_{\mathbf{d}}$, *where* $\mathcal{I}_{\mathbf{d}} = \mathbb{K}[X]_{\mathbf{d}} \cap \mathcal{I}$.

We are now interested in giving estimations on the dimensions (as $\mathbb{K}$-vector spaces) of the components that appear in proposition 2.14. To this end, we introduce *Hilbert functions and Hilbert series*.

2.1.3 Hilbert Function and Hilbert Series

The Hilbert Series of a graded algebra is a fundamental object in commutative algebra, since a lot of informations can be read from it. From now on, we assume that the monoid $\mathbb{M}$ is $\mathbb{N}$, although the following notions can be extended to other monoids (in order to handle various gradings as multi-homogeneous gradings or gradings given by the product $\mathbb{N} \times \mathbf{X}(\mathbf{G})$ where $\mathbf{X}(\mathbf{G})$ is a finite group).

An element is said to be homogeneous if it is homogeneous for the grading given by $\mathbb{N}$. We start by giving a general definition, and then we give explcitely classical series associated to the homogeneous and quasi-homogeneous gradings on $\mathbb{K}[X] = \mathbb{K}[x_1, \dots, x_n]$.

Definition 2.18. *The formal power series ring* $\mathbb{Z}[[z]]$ *is defined as follows.*
- $\mathbb{Z}[[z]]$ *is equal to* $\mathbb{Z}^{\mathbb{N}}$ *as a commutative group. The element of* $\mathbb{Z}[[z]]$ *mapping* $d \in \mathbb{N}$ *to* $a_d \in \mathbb{Z}$ *is denoted* $\sum_{d \in \mathbb{N}} a_d z^d$.
- *The product of two elements of* $\mathbb{Z}[[z]]$ *is given by the Cauchy rule:*

$$\left(\sum_{d \in \mathbb{N}} a_d z^d\right) \times \left(\sum_{d \in \mathbb{N}} b_d z^d\right) = \sum_{d \in \mathbb{N}} \left(\sum_{(\ell, \ell') \in \mathbb{N}^2,\, \ell + \ell' = d} a_\ell b_{\ell'} \right) z^d$$

This product is well defined since only a finite number of pairs (ℓ, ℓ') *verify* $\ell + \ell' = d$ *which gives to* $\mathbb{Z}[[z]]$ *a commutative ring structure.*

The element z^0 *is a neutral for the multiplication law and will be denoted 1. Notice that for all* $d \in \mathbb{N}^*$, *the series* $(1 - z^d)$ *is invertible, with inverse* $\sum_{k=0}^{+\infty} z^{kd}$.

In addition with the hypothesis of definition 2.12 (with $\mathbb{M} = \mathbb{N}$), we also assume that the components $\dim_{\mathbb{K}}(\mathcal{A}_d)$ are of finite dimension for all $d \geq 0$.

Definition 2.19. *Let* $\mathcal{A}$ *be a* $\mathbb{N}$*-graded algebra, and* $\mathcal{I}$ *a homogeneous ideal of* $\mathcal{A}$. *The Hilbert function and the Hilbert series of* $\mathcal{A}/\mathcal{I}$ *are defined by*

$$\mathsf{HF}_{\mathcal{A}/\mathcal{I}}(d) = \dim_{\mathbb{K}}(\mathcal{A}_d/\mathcal{I}_d) \qquad \text{and} \qquad \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z) = \sum_{d \in \mathbb{N}} \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(d) z^d$$

As an example, we review here the Hilbert functions and series associated to the classical gradings on $\mathbb{K}[X]$.

Definition 2.20. *[30] Let* $\mathcal{A} = \mathbb{K}[X]$.

— *Let $\mathcal{I} \subset \mathbb{K}[X]$ be a homogeneous ideal. The Hilbert function $\mathit{HF}_{\mathbb{K}[X]/\mathcal{I}} : \mathbb{N} \to \mathbb{N}$ and the Hilbert series $\mathit{HS}_{\mathbb{K}[X]/\mathcal{I}} \in \mathbb{N}[[z]]$ of the quotient ring $\mathbb{K}[X]/\mathcal{I}$ are defined by:*

$$\mathit{HF}_{\mathbb{K}[X]/\mathcal{I}}(d) = \dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) \qquad \text{and} \qquad \mathit{HS}_{\mathbb{K}[X]/\mathcal{I}}(z) = \sum_{d=0}^{\infty} \mathit{HF}_{\mathbb{K}[X]/\mathcal{I}}(d)t^d$$

— *Let $\mathcal{I} \subset \mathbb{K}[X]$ be a quasi-homogeneous ideal with respect to $\mathbf{w} = (w_1, \ldots, w_n)$. The weighted Hilbert function $\mathit{HF}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}} : \mathbb{N} \to \mathbb{N}$ and the weighted Hilbert series $\mathit{HS}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}} \in \mathbb{N}[[z]]$ of the quotient ring $\mathbb{K}[X]/\mathcal{I}$ are defined by:*

$$\mathit{HF}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}}(d) = \dim_{\mathbb{K}}(\mathbb{K}[X]_d^{(\mathbf{w})}/\mathcal{I}_d) \qquad \text{and} \qquad \mathit{HS}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}}(z) = \sum_{d=0}^{\infty} \mathit{HF}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}}(d)t^d$$

In the case where f does not divide zero in the ring $\mathcal{A}/\mathcal{I}$, it is easy to give relations between the Hilbert series of $\mathcal{A}/\mathcal{I}$ and $\mathcal{A}/\left(\mathcal{I} + \langle f \rangle\right)$.

Proposition 2.21. *Let $\mathcal{I} \subset \mathcal{A}$ be a homogeneous ideal of $\mathcal{A}$ and $f \in \mathcal{A}_d$ be a homogeneous polynomial of degree $d \in \mathbb{N}$. If f does not divide 0 in the ring $\mathcal{A}/\mathcal{I}$, then*

$$\mathit{HS}_{\mathcal{A}/(\mathcal{I}+\langle f \rangle)}(z) = (1 - z^d)\, \mathit{HS}_{\mathcal{A}/\mathcal{I}}(z)$$

Proof. For every $\ell \in \mathbb{N}$, consider the following sequence of $\mathbb{K}$-vector spaces:

$$0 \longrightarrow \mathcal{A}_\ell/\mathcal{I}_\ell \xrightarrow{\times f} \mathcal{A}_{\ell+d}/\mathcal{I}_{\ell+d} \overset{\pi}{\twoheadrightarrow} \mathcal{A}_{\ell+d}/(\mathcal{I} + \langle f \rangle)_{\ell+d} \longrightarrow 0,$$

where π is the canonical projection ($\twoheadrightarrow$ is a surjective map). Since f does not divide 0 in $\mathcal{A}/\mathcal{I}$, this sequence is exact. Therefore the alternate sum of the dimensions of these vector spaces is equal to 0. Consequently, $\mathsf{HF}_{\mathcal{A}/\mathcal{I}}(\ell) - \mathsf{HF}_{\mathcal{A}/\mathcal{I}}(\ell + d) + \mathsf{HF}_{\mathcal{A}/(\mathcal{I}+\langle f \rangle}(\ell + d) = 0$, thus multiplying this relation by z^ℓ and summing over ℓ yields to:

$$z^d\, \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z) - \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z) + \mathsf{HS}_{\mathcal{A}/(\mathcal{I}+\langle f \rangle)}(z) = 0.$$

□

Therefore, the Hilbert series of a ring $\mathcal{A}/\left(\mathcal{I} + \langle f \rangle\right)$ is very easy to deduce from the Hilbert series of $\mathcal{A}/\mathcal{I}$ if f does not divide zero in $\mathcal{I}$. It follows from the definition of a regular sequence (definition 2.4) that one can compute easily the Hilbert series of an ideal generated by a regular sequence, knowing the Hilbert series of the algebra $\mathcal{A}$.

Proposition 2.22. *Let $\mathcal{I} \subset \mathcal{A}$ be a homogeneous ideal of $\mathcal{A}$ generated by a regular sequence $F = (f_1, \ldots, f_s)$ of homogeneous polynomials of degrees $d_1, \ldots, d_s$. Then*

$$\mathit{HS}_{\mathcal{A}/\mathcal{I}}(z) = \prod_{i=1}^{s}(1 - z^{d_i}) \times \mathit{HS}_{\mathcal{A}}(z)$$

Proof. We just have to apply $s - 1$ times the proposition 2.21. □

From previous proposition, with $\mathcal{A} = \mathbb{K}[X]$, $\mathcal{I}$ a homogeneous or quasi-homogeneous ideal and f a homogeneous or quasi-homogeneous polynomial, we obtain:

Corollary 2.23. — *If $\mathcal{I}$ is a homogeneous ideal generated by a regular sequence $(f_1, \ldots, f_s)$, then $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(z) = \prod_{i=1}^{s}(1 - z^{d_i}) \times \mathsf{HS}_{\mathbb{K}[X]}(z)$*
— *If $\mathcal{I}$ is a quasi-homogeneous ideal with respect to $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{N}^n$, generated by a regular sequence $(f_1, \ldots, f_s)$, then $\mathsf{HS}^{(\mathbf{w})}{}_{\mathbb{K}[X]/\mathcal{I}}(z) = \prod_{i=1}^{s}(1 - z^{d_i}) \times \mathsf{HS}^{(\mathbf{w})}{}_{\mathbb{K}[X]}(z)$*

We are now able to give the Hilbert series and weighted Hilbert of $\mathbb{K}[X]$.

Proposition 2.24. *The Hilbert series and weighted Hilbert series of $\mathbb{K}[X]$ are given by*
— $\mathsf{HS}_{\mathbb{K}[X]}(z) = \dfrac{1}{(1-z)^n}$
— $\mathsf{HS}^{(\mathbf{w})}{}_{\mathbb{K}[X]}(z) = \dfrac{1}{\prod_{i=1}^{n}(1 - z^{w_i})}$

Proof. We just have to apply corollary 2.23 to $\langle x_1, \ldots, x_n\rangle$. This is possible since $(x_1, \ldots, x_n)$ is a regular sequence in $\mathbb{K}[X]$. We also need the series associated to $\mathbb{K}[X]/\langle x_1, \ldots, x_n\rangle$, which is simply 1. The degrees are given below:
— in the homogeneous case, the degree of each indeterminate x_i is 1.
— in the quasi-homogeneous case, with respect to the weights $\mathbf{w} = (w_1, \ldots, w_n)$, the degree of x_i is w_i.

□

We now explain why the relation 2.22 fails if the sequence $(f_1, \ldots, f_s)$ is not regular. We start by giving a more precise result than proposition 2.21.

Proposition 2.25. *Let $\mathcal{I}$ be a homogeneous ideal of $\mathcal{A}$, and $f \in \mathcal{A}_d$ a homogeneous polynomial of degree d. Then,*

$$\mathsf{HS}_{\mathcal{A}/(\mathcal{I}+\langle f\rangle)}(z) = \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z) - z^d\,\mathsf{HS}_{\mathcal{A}/(\mathcal{I}:f)}$$

where $(I : f) = \{g \in \mathcal{A} \mid gf \in \mathcal{I}\} \supseteq \mathcal{I}$.

Proof. Note that this property is classical in the algebra $\mathbb{K}[X]$, see for example [9]. In the same way we proved proposition 2.21, we introduce an exact sequence for each $d, \ell \in \mathbb{N}$.

$$0 \longrightarrow (\mathcal{I} : f)_\ell/\mathcal{I}_\ell \xrightarrow{\iota} \mathcal{A}_\ell/\mathcal{I}_\ell \xrightarrow{\times f} \mathcal{A}_{\ell+d}/\mathcal{I}_{\ell+d} \xrightarrow{\pi} \mathcal{A}_{\ell+d}/(\mathcal{I} + \langle f\rangle)_{\ell+d} \longrightarrow 0$$

To see that this sequence is exact, we have to prove that $\ker(f) = (\mathcal{I} : f)_\ell/\mathcal{I}_\ell$. Hence, the kernel of the map $\mathcal{A}_\ell \to \mathcal{A}_{\ell+d}/\mathcal{I}_{\ell+d}$ is precisely $(\mathcal{I} : f)_\ell$. Quotienting by $\mathcal{I}_\ell$ yields the result. Since this sequence is exact, the alternating sum of the dimensions of these $\mathbb{K}$-vector spaces is zero. Noticing that $\dim((\mathcal{I} : f)_\ell/\mathcal{I}_\ell) - \dim(\mathcal{A}_\ell/\mathcal{I}_\ell) = -\dim(\mathcal{A}_\ell/(\mathcal{I} : f)_\ell)$, we obtain that

$$-\dim(\mathcal{A}_\ell/(\mathcal{I} : f)_\ell) + \dim(\mathcal{A}_{\ell+d}/\mathcal{I}_{\ell+d}) - \dim(\mathcal{A}_{\ell+d}/(\mathcal{I} + f)_{\ell+d})$$

and the result by multiplying this equality by $z^{\ell+d}$ and summing over ℓ. □

It follows from the previous result that proposition 2.21 holds in both directions: the Hilbert series of $\mathcal{A}/(\mathcal{I} + \langle f\rangle)$ and $\mathcal{A}/\mathcal{I}$ are equal if and only if $(\mathcal{I} : f) = \mathcal{I}$. Notice that otherwise, $(\mathcal{I} : f) \supsetneq \mathcal{I}$ and $\mathsf{HS}_{\mathcal{A}/(\mathcal{I}:f)}(z) < \mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z)$, in the following sense: $[z^d]\,\mathsf{HS}_{\mathcal{A}/(\mathcal{I}:f)}(z) \leq [z^d]\,\mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z)$ for all $d \in \mathbb{N}$, and the equality does not hold at least for one d. Hence, we have the following corollary:

Corollary 2.26. *Let $\mathcal{I} \subset \mathcal{A}$ be a homogeneous ideal of $\mathcal{A}$ generated by a sequence $\mathsf{F} = (f_1, \ldots, f_s)$ of homogeneous polynomials of degrees $d_1, \ldots, d_s$. Then F is regular if and only if*

$$\mathsf{HS}_{\mathcal{A}/\mathcal{I}}(z) = \frac{\mathsf{HS}_{\mathcal{A}}(z)}{\prod_{i=1}^{s}(1 - z^{d_i})}$$

From corollary 2.26, we can easily deduce the result stated in subsection 2.1.1.

Corollary 2.27. *If F is a regular sequence of homogeneous polynomials, then any permutation of the sequence is also a regular sequence.*

Regular sequences and behavior of the SAGBI-F_5 algorithm. Regular sequences is an important family of polynomial systems: in $\mathbb{K}[X]$, we will see that they are *generic* (if the length of the sequence does not exceed n), and from an algorithmic point of view, the behavior of the F_5-algorithm 1.44 on such a sequence is optimal: there are no *reductions to zero*. More precisely, we will see that a reduction to zero occuring in a Gröbner (SAGBI) basis computation comes from a *non-principal syzygy*, the definition of which is given below.

Definition 2.28. *Let $\mathsf{F} = (f_1, \ldots, f_s) \in \mathcal{A}^s$ be a sequence of polynomials in a graded algebra, and let $(\mathbf{E}_1, \ldots, \mathbf{E}_s)$ be the canonical basis of the free $\mathcal{A}$-module $\mathcal{A}^s$. Now consider the following evaluation morphism:*

$$\begin{array}{rccc} \varphi_{\mathsf{F}}: & \mathcal{A}^s & \longrightarrow & \mathcal{A} \\ & (g_1, \ldots, g_s) & \longmapsto & \displaystyle\sum_{i=1}^{s} g_i f_i \end{array}$$

The syzygy module *of F in $\mathcal{A}$ is the submodule $\mathbf{Syz}(\mathsf{F}) = \varphi^{-1}(0)$. A syzygy is an element of this kernel, such a syzygy is usually denoted $\sum_{i=1}^{s} g_i \mathbf{E}_i$.*

It is easy to see that with notations of the previous definition, $f_j\mathbf{E}_i - f_i\mathbf{E}_j$ is always a syzygy. This observation leads to the following definition:

Definition 2.29. *With notations of definition 2.28, the submodule of $\mathbf{Syz}(\mathsf{F})$ generated by $(f_j\mathbf{E}_i - f_i\mathbf{E}_j)_{i,j}$ is called the module of* principal syzygies *and is denoted by $\mathbf{PSyz}(\mathsf{F})$.*

We now explain the link between definition 2.4 and 2.29.

Proposition 2.30. *In $\mathcal{A}$, a sequence $\mathsf{F} = (f_1, \ldots, f_s)$ is a regular sequence if and only if $\mathbf{PSyz}(\mathsf{F}) = \mathbf{Syz}(\mathsf{F})$ in $\mathcal{A}^s$.*

Proof. For both directions, the proof is done by induction on s.

— The case $s = 1$ is easy: $\mathbf{PSyz}(f_1) = \{0\}$ and the following equivalences are clear:

$$\mathbf{Syz}(f_1) = \{0\} \quad \Longleftrightarrow \quad f_1 \text{ is non-zero} \quad \Longleftrightarrow \quad (f_1) \text{ is a regular sequence}$$

— ($\Rightarrow$) : Assume that $(f_1, \ldots, f_s)$ is a regular sequence in $\mathcal{A}$ with $s \geq 2$, and let $\mathbf{S} = \sum_{i=1}^{s} g_i\mathbf{E}_i$ be a syzygy. Then, $\sum_{i=1}^{s-1} g_i f_i = -g_s f_s$, which means that g_s belongs to the colon ideal $\langle f_1, \ldots, f_{s-1}\rangle : (f_s)$. Since f_s does not divide zero in $\langle f_1, \ldots, f_{s-1}\rangle$ by definition of a regular sequence, $g_s \in \langle f_1, \ldots, f_{s-1}\rangle$. Hence, g_s can be written $\sum_{i=1}^{s-1} h_i f_i$. Then,

$$\begin{aligned} \mathbf{S} &= \sum_{i=1}^{s} g_i\mathbf{E}_i \\ &= \sum_{i=1}^{s-1} g_i\mathbf{E}_i + \left(\sum_{i=1}^{s-1} h_i f_i\right)\mathbf{E}_s \\ \mathbf{S} &= \sum_{i=1}^{s-1} h_i(f_i\mathbf{E}_s - f_s\mathbf{E}_i) + \sum_{i=1}^{s-1}(g_i + h_i f_s)\mathbf{E}_i \end{aligned}$$

Consequently, $\mathbf{S}$ can be written as a sum of a principal syzygy and a syzygy involving only the $(s-1)$ first elements of the canonical basis of $\mathcal{A}^s$. Since $(f_1, \ldots, f_{s-1})$ is also a regular sequence, by induction $\sum_{i=1}^{s-1}(g_i + h_i f_s)\mathbf{E}_i$ belongs to $\mathbf{PSyz}(f_1, \ldots, f_{s-1}) \subset \mathbf{PSyz}(\mathsf{F})$. We conclude that $\mathbf{S}$ also belongs to $\mathbf{PSyz}(\mathsf{F})$.

— ($\Leftarrow$) : Assume now that $\mathbf{PSyz}(\mathsf{F}) = \mathbf{Syz}(\mathsf{F})$ with $s \geq 2$. By induction, $(f_1, \ldots, f_{s-1})$ is a regular sequence. Now let g be a polynomial in the colon ideal $(\langle f_1, \ldots, f_{s-1}\rangle : f_s)$. Then there exist $g_1, \ldots, g_{s-1} \in \mathcal{A}$ such that $\mathbf{S} = \sum_{i=1}^{s-1} g_i \mathbf{E}_i + g\mathbf{E}_s$ is a syzygy. Since $\mathbf{PSyz}(\mathsf{F}) = \mathbf{Syz}(\mathsf{F})$, $\mathbf{S}$ can also be written $\sum_{1\leq i<j\leq s} h_{i,j}(f_j\mathbf{E}_i - f_i\mathbf{E}_j)$. It follows that $g = -\sum_{i=1}^{s-1} h_{i,s} f_i \in \langle f_1, \ldots, f_{s-1}\rangle$ and F is a regular sequence.

□

We now prove that they are no reduction to zero in the SAGBI matrix-F_5 algorithm 1.68, if the input sequence is a regular sequence of homogeneous polynomials in $\mathcal{A}$. This proposition generalizes the result given by Faugère in [35] on the classical F_5 algorithm.

Proposition 2.31. *Let $\mathsf{F} = (f_1, \ldots, f_s)$ be a regular sequence of homogeneous polynomials in a graded subalgebra $\mathcal{A}$ of $\mathbb{K}[X]$. There are no reductions to zero in the SAGBI-F_5 algorithm 1.68 while computing a SAGBI basis of $\langle \mathsf{F}\rangle_{\mathcal{A}}$ up to a given degree D. In other words, the matrices builded in Matrix SAGBI-F_5 algorithm are full rank.*

Proof. Recall that with notations of algorithm 1.68, $(b_i^d)_{1\leq i\leq n_d}$ is the basis of the $\mathbb{K}$-vector space $\mathcal{A}_d$. A reduction to zero corresponds to a writing $b_\ell^{d-d_i} f_i = \sum_{j=1}^{i-1} g_j f_j + \sum_{k<\ell} c_k b_k^{d-d_i} f_i$ where $g_j \in \mathcal{A}_{d-d_j}$ and $c_k \in \mathbb{K}$. Since the sequence F is $\mathcal{A}$-regular, the sequence $\mathsf{F}_i = (f_1, \ldots, f_i)$ also and $\sum_{k\leq\ell} c_k b_k^{d-d_i} \in \langle f_1, \ldots, f_{i-1}\rangle_{\mathcal{A}}$, with $c_\ell = -1 \neq 0$. Let $\lambda = \mathrm{Min}\{k \leq \ell \mid c_k \neq 0\}$. Then, there is a row in the matrix $M_{d-d_i,i-1}$ with leading monomial equal to $\mathsf{LM}_{\preceq}(b_\lambda^{d-d_i})$. So by SAGBI-$F_5$ criterion (lemma 1.69), the row corresponding to $b_\lambda^{d-d_i} f_i$ in $M_{d,i}$ should has been removed and the writing $b_\ell^{d-d_i} f_i = \sum_{j=1}^{i-1} g_j f_j + \sum_{k<\ell} c_k b_k^{d-d_i} f_i$ is absurd. □

2.2 Applications in $\mathbb{K}[X]$

We now focus on the case where $\mathcal{A} = \mathbb{K}[X]$, graded with the standard homogeneous grading. In this section, we explain how to bound in advance the maximal degree, that can be reached during the computation of a Gröbner basis. In particular, it provides a bound for the maximal degree D used in the Matrix-F_5 algorithm 1.44 and can be used to obtain complexity bounds for solving a polynomial system, depending on the degrees of the polynomials and regularity assumptions.

2.2.1 Bounds on the degrees

Proposition 2.32. *Let $\mathcal{I}$ be a homogeneous ideal of $\mathcal{A} = \mathbb{K}[X]$. There exists a polynomial $N(z) \in \mathbb{Z}(z)$ such that the Hilbert Series of $\mathcal{I}$ can be written*

$$\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(z) = \frac{N(z)}{(1-z)^n}$$

Proof. By Hilbert Szyzygy theorem 2.11, $\mathbb{K}[X]/\mathcal{I}$ has a graded free resolution, of length $r \leq n$. Hence, for any $d \geq 0$, there exists an exact sequence of $\mathbb{K}$-vector spaces

$$0 \to M_k \xrightarrow{\rho_k} \cdots M_{k-1} \xrightarrow{\rho_{k-1}} \cdots \xrightarrow{\rho_1} M_0 \xrightarrow{\rho_0} \mathbb{K}[X]/\mathcal{I} \to 0$$

where M_i is a free $\mathbb{K}[X]$-module of finite rank. Since $\mathbb{K}[X]/\mathcal{I}$ is a graded algebra, we deduce that for all $d \geq 0$, there exists an exact sequence

$$0 \to \bigoplus_{j=1}^{i_r} \mathbb{K}[X]_{d-d_{r,j}} \to \cdots \to \bigoplus_{j=1}^{i_0} \mathbb{K}[X]_{d-d_{0,j}} \to \mathbb{K}[X]_d/I_d \to 0$$

where all integers $d_{i,j}$ are less than or equal to d. Since the alternate sums of the dimensions of vector spaces in an exact sequence is equal to zero, it follows that

$$\left(\sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} \dim_{\mathbb{K}}(\mathbb{K}[X]_{d-d_{i,j}})\right) - \dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) = 0$$

Hence,

$$\begin{aligned}
\dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) &= \textstyle\sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} \dim_{\mathbb{K}}(\mathbb{K}[X]_{d-d_{i,j}}) \\
&= \textstyle\sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} [z^{d-d_{i,j}}] \left(\frac{1}{1-z^n}\right) \\
&= \textstyle\sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} [z^{d}] \left(\frac{z^{d_{i,j}}}{1-z^n}\right) \\
\dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) &= [z^d]\left(\frac{\sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} z^{d_{i,j}}}{1-z^n}\right)
\end{aligned}$$

and the proposition is proved by taking $N(z) = \sum_{i=0}^{r}(-1)^i \sum_{j=1}^{i_r} z^{d_{i,j}}$.

□

With the previous proposition, we see that the Hilbert function of a homogeneous ideal matches a polynomial function, except for a finite number of integers:

Corollary 2.33. *Let $\mathcal{I}$ be a homogeneous ideal of $\mathcal{A} = \mathbb{K}[X]$. There exists a polynomial (denoted $\mathsf{HP}_{\mathbb{K}[X]/\mathcal{I}}$) and an integer $d_0 \geq 0$ such that the Hilbert function of $\mathbb{K}[X]/\mathcal{I}$, defined by $\mathsf{HF}_{\mathbb{K}[X]/\mathcal{I}}(d) = \dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d)$ coincides with $\mathsf{HP}_{\mathbb{K}[X]/\mathcal{I}}$ for all $d \geq d_0$.*

Proof. From proposition 2.32, the Hilbert series of $\mathbb{K}[X]/\mathcal{I}$ can be written $N(z)/(1-z)^n$. Then, the partial fraction expansion of $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}$ is equal to $P(z) + \sum_{i=1}^{n} \frac{a_i}{(1-z)^i}$ for some polynomial P and integers $(a_i)_{1\leq i\leq n}$. Let d_0 be the degree of P (we set $d_0 = -1$ if $P = 0$). Since for all $i \geq 1$,

$$\frac{1}{(1-z)^i} = \sum_{d=0}^{+\infty} \binom{d+i-1}{d} z^d = \sum_{d=0}^{+\infty} \underbrace{\frac{(d+i-1)\times\cdots\times(d+1)}{(i-1)!}}_{P_i(d)} z^d$$

where $P_i(d)$ is a polynomial, we have $\mathsf{HF}_{\mathbb{K}[X]/\mathcal{I}}(d) = [z^d]P(z) + \sum_{i=1}^{n} a_i P_i(d)$ which coincides with $\mathsf{HP}_{\mathbb{K}[X]/\mathcal{I}}(d) = \sum_{i=1}^{n} a_i P_i(d)$ for all $d \geq \deg(P) + 1 = d_0$. □

It turns on that the dimension of the ideal $\mathcal{I}$ can be read from the expression deduced in proposition 2.32, which leads to the following proposition.

Proposition 2.34. *let $\mathcal{I}$ be a homogeneous proper ideal of $\mathbb{K}[X]$, and let $\frac{N(z)}{(1-z)^d}$ be the expression of the Hilbert series of the quotient algebra $\mathbb{K}[X]/\mathcal{I}$, assumed to be reduced (N is not divisible by $z-1$). Then the dimension of $\mathcal{I}$ is equal to d. Moreover, if $d = 0$, then the Hilbert series $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}$ is a polynomial and $\mathsf{DEG}(\mathcal{I})$ is equal to $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(1)$.*

Proof. Rewriting the proof of corollary 2.33 with $\frac{N(z)}{(1-z)^d}$ and $N(1) \neq 0$ leads to an expression of $\mathsf{HP}_{\mathbb{K}[X]/\mathcal{I}}$ as a polynomial of degree exactly $d-1$ since the polynomial P_i has degree $i-1$ (with the convention that the zero polynomial has degree -1). It is proved in [25, page 464] that the degree of the Hilbert polynomial of $\mathbb{K}[X]/\mathcal{I}$ is equal to the projective dimension of $\mathcal{I}$, which is $\dim(\mathcal{I})-1$. Therefore, $\dim(\mathcal{I}) = d$. If $d = 0$, the Hilbert polynomial is equal to 0, and $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(1) = \sum_{i=0}^{+\infty} \dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) = \dim_{\mathbb{K}}(\mathbb{K}[X]/\mathcal{I}) = \mathsf{DEG}(\mathcal{I})$. □

Definition 2.35. *Let $\mathcal{I}$ be a homogoneous ideal of $\mathbb{K}[X]$. From proposition 2.33, the Hilbert series and the Hilbert polynomial of $\mathbb{K}[X]/\mathcal{I}$ coincide for all d greater than or equal to an integer $d_0 \geq 0$. The smallest possible d_0 is called the* index of regularity *of $\mathcal{I}$, denoted by $\mathsf{i}_{\mathsf{reg}}(\mathcal{I})$.*

If $\mathcal{I}$ is a zero-dimensional ideal, the index of regularity is easy to read from the Hilbert series, since this series is a polynomial. By definition the index of regularity is equal to $\deg(\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}) + 1$. It is worth to notice that this integer bounds the degree reached during a computation of a Gröbner basis.

Proposition 2.36. *Let $\preceq$ be any ordering on $\mathbb{K}[X]$, and $\mathcal{I} \subseteq \mathbb{K}[X]$ a zero-dimensional homogeneous ideal. Then all polynomials in the reduced Gröbner basis of $\mathcal{I}$ have a total degree less than or equal to $\mathsf{i}_{\mathsf{reg}}(\mathcal{I})$.*

Proof. Let $\mathcal{G}$ be the reduced Gröbner basis of $\mathcal{I}$ for $\preceq$. By definition of $\mathsf{i}_{\mathsf{reg}}(\mathcal{I})$, $\dim_{\mathbb{K}}(\mathbb{K}[X]_d/\mathcal{I}_d) = 0$ for all $d \geq \mathsf{i}_{\mathsf{reg}}(\mathcal{I})$. Hence, all monomials of degree less than or equal to $\mathsf{i}_{\mathsf{reg}}(\mathcal{I})$ are in $\mathcal{I}$ and are reducible by a polynomial in $\mathcal{G}$. Therefore, any homogeneous polynomial h of degree greater than d has its leading monomial that can be written $\mathsf{LM}_{\preceq}(g) \times m$ with m a monomial different from 1 and g a polynomial in $\mathcal{G}$. Consequently, h does not belong to $\mathcal{G}$. □

A homogeneous regular sequence of length n in $\mathbb{K}[X]$ generates a zero-dimensional ideal. We now give bounds on the index of regularity and degree of such ideal.

Proposition 2.37. *Let $\mathsf{F} = (f_1, \ldots, f_n)$ be a regular sequence of homogeneous polynomials of degrees $(d_1, \ldots, d_n)$ in $\mathbb{K}[X]$, generating the ideal $\mathcal{I}$. Then:*
- *the index of regularity of $\mathcal{I}$ is equal to $1 + \sum_{i=1}^{n}(d_i - 1)$, called the Macaulay bound.*
- *the degree of $\mathcal{I}$ is given by $\prod_{i=1}^{n} d_i$, called the Bézout bound.*

Proof. Since F is a regular sequence, by proposition 2.22, the Hilbert series of $\mathcal{I}$ is equal to

$$\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(z) = \frac{\prod_{i=1}^{n}(1-z^{d_i})}{(1-z)^n} = \prod_{i=1}^{n}\left(\sum_{j=0}^{d_i-1} z^j\right)$$

It follows that $\mathsf{i}_{\mathsf{reg}}(\mathcal{I}) = \deg(\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}) + 1 = 1 + \sum_{i=1}^{n}(d_i - 1)$ and $\mathsf{DEG}(\mathcal{I}) = \mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}(1) = \prod_{i=1}^{n} d_i$. □

2.2.2 Genericity of regular sequences. Semi-regular sequences.

We have seen that regular sequences have a good behavior with Gröbner bases computations and that Hilbert series of the associated ideals are easy to describe. But do regular sequences of a given sequence of a degrees necessarily exist ? We have seen that in $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$, the length of a regular sequence cannot be greater than n. We now

see that being a regular sequence is a *Zariski open condition* for generic sequences of length $s \leq n$, and that the associated Zariski open-subset is non-empty.

We assume that $\mathbb{K}$ is an infinite field. Let s be a positive integer, $d_1, \ldots, d_s$ be a sequence of positive integers and $f_1, \ldots, f_s$ be a sequence of homogeneous polynomials in $\mathbb{K}[X]$ having degrees $d_1, \ldots, d_s$. Finally, we denote by $\mathcal{I}$ the ideal $\langle f_1, \ldots, f_s \rangle$. We start with the following lemma, emphasing the fact that allmost all choices on the coefficients of the sequence lead to the same Hilbert series $\mathsf{HS}_{\mathbb{K}[X]/\mathcal{I}}$.

Lemma 2.38. *There exists a non-empty Zariski open subset U in $\mathbb{K}[X]_{d_1} \times \cdots \times \mathbb{K}[X]_{d_s}$ such that for all sequences $\mathsf{F} = (f_1, \ldots, f_s)$ in U, the number $\mathsf{HS}_{\mathbb{K}[X]/\langle f_1,\ldots,f_s\rangle}(d)$ does not depend on F for all $d \in \mathbb{N}$, and is the smallest among all sequences in $\mathbb{K}[X]_{d_1} \times \cdots \times \mathbb{K}[X]_{d_s}$.*

Sketch of proof. [85] The proof is classical: assume first that $s \geq n$. We are looking for sequences of length s such that the component $\mathcal{I}_d$ of $\mathcal{I}$ has as large dimension as possible. Failure arises if and only if some minors of the maps

$$\varphi_{i,j} : \mathbb{K}[X]_j/\langle f_1, \ldots, f_{i-1}\rangle_j \xrightarrow{\times f_i} \mathbb{K}[X]_{j+d_i}/\langle f_1, \ldots, f_{i-1}\rangle_{j+d_i}$$

vanish. Therefore, for a given d, the fact that $\mathsf{HS}_{\mathbb{K}[X]/\langle f_1,\ldots,f_s\rangle}(d)$ is the smallest among all possible value is an open condition, and is valid for the sequences in a non-empty Zariski open subset U_d of $\prod_{i=1}^{s} \mathbb{K}[X]_{d_i}$. An intersection of an infinite number of open subsets is not necessarily open, but the trick is to see that intersecting only a finite number of these sets yields the result: if $f_i = x_i^{d_i}$ for $1 \leq i \leq n$, then $\mathcal{I}_d = \mathbb{K}[X]_d$ for all $d \geq D = 1 + \sum_{i=1}^{n}(d_i - 1)$. Then $U = \cap_{d=0}^{\infty} U_d = \cap_{d=0}^{D} U_d$ is a non-empty Zariski open subset.

If $s < n$, $f_1, \ldots, f_s$ is a regular sequence if and only if there exists $(n - s)$ linear forms $(\ell_i)_{s+1 \leq i \leq n}$ such that $(f_1, \ldots, f_s, \ell_{s+1}, \ldots, \ell_n)$ is a regular sequence, which is true on a non-empty Zariski open subset U of $(\prod_{i=1}^{s} \mathbb{K}[X]_{d_i}) \times \mathbb{K}[X]_1^{n-s}$. The projection of U on $(\prod_{i=1}^{s} \mathbb{K}[X]_{d_i})$ contains also a non-empty Zariski open subset. □

In particular, the previous lemma shows that regular sequences are generic. We have seen that regular sequences of length $s > n$ do not exist. However, a generalization of this notion is *semi-regular sequences* and we explain it now.

Notations 2.39. *For $H = \sum_{d=0}^{\infty} h_d z^d$ a power series in $\mathbb{Z}[[z]]$, we denote by $[H]_+$ the series H truncated at its first negative coefficient. More precisely, $[H]_+$ is defined by:*

$$[z^d][H]_+ = \begin{cases} h_d & \text{if } h_i \geq 0 \text{ for } 0 \leq i \leq d \\ 0 & \text{otherwise} \end{cases}$$

The idea behind the following definition of semi-regular sequences is that their behavior under Gröbner basis algorithms looks like there were regular. We first comme back to the definitions of syzygies in the case $\mathcal{A} = \mathbb{K}[X]$.

Definition 2.40. *With notations of definition 2.28 and in the case $\mathbb{R} = \mathbb{K}[X]$, if $\mathbf{S} = \sum_i g_i \mathbf{E}_i$ is a non-zero syzygy, $\deg(S) = \max_i(\deg(g_i) + \deg(f_i))$ is called the degree of the syzygy, where the degree of polynomials in $\mathbb{K}[X]$ is the standard total degree.*

The following proposition-definition relates the degree of the Hilbert polynomial and syzygies to define semi-regular sequences.

Proposition – Definition 2.41. *[4, 5, 6] Let $\mathsf{F} = (f_1, \ldots, f_s) \in \mathbb{K}[X]^s$ be a sequence of homogeneous polynomials generating a zero-dimensional ideal. The two following statements are equivalent:*

— *the Hilbert series of* $\mathbb{K}[X]/\langle \mathsf{F} \rangle$ *is given by*

$$HS_{\mathbb{K}[X]/\langle \mathsf{F} \rangle}(z) = \left[\frac{\prod_{i=1}^{s}(1 - z^{\deg(f_i)})}{(1-z)^n} \right]_+$$

— *every syzygy of* F *of degree at most* $\deg(HS_{\mathbb{K}[X]/\langle \mathsf{F} \rangle}) + 1$ *is in the module generated by the trivial syzygies.*

A sequence F *verifying these properties is called* semi-regular.

The definition above shows that, while computing a Gröbner basis of an ideal generated by a homogeneous semi-regular sequence, no reduction to zero occures, just like regular sequences. Semi-regular sequences can also be defined in terms of applications as regular sequences, as shown is the following proposition.

Proposition 2.42. *[85] A sequence of homogeneous polynomials* $(f_1, \ldots, f_s)$ *of degrees* $d_1, \ldots, d_s$ *is semi-regular if and only if the maps*

$$\mathbb{K}[X]_d/\langle f_1, \ldots, f_{i-1}\rangle_d \xrightarrow{\times f_i} \mathbb{K}[X]_{d+d_i}/\langle f_1, \ldots, f_{i-1}\rangle_{d+d_i}$$

are of maximal rank, i.e either injective or surjective.

Semi-regular sequences are conjectured to be *generic*, as regular sequences are, since it seems to be the case in practice. More precisely, Fröberg's conjecture is expressed in the following way:

Conjecture 2.43 (Fröberg conjecture)**.** *Let* $d_1, \ldots, d_s$ *be a sequence of integers and* $\mathbb{K}$ *be an infinite field. Then the* $\mathbb{K}$*-vector space of homogeneous sequence of polynomials* $\mathsf{F} = (f_1, \ldots, f_s)$ *of degrees* $d_1, \ldots, d_s$*, that are semi-regular, contains a Zariksi-open subset in its interior.*

We refer to [85] for reformulations of this famous conjecture. It has been proved in several cases, see [4] and references therein for details.

2.2.3 Affine case.

From an algorithmic point of view, it is possible to compute a Gröbner basis for an ideal generated by inhomogeneous polynomials by applying variants of the Lazard/Matrix-F_5-algorithms seen in chapter 1: the columns of the matrices are indexed by all monomials of degree less than or equal to the current degree D instead of monomials of degree D only. The drawback of this method is that we do not take profit of *degree falls*, which can produce polynomials of lower degree than D. Hence, the *normal strategy*[34] for F_4/F_5 algorithms is to perform computations at the smallest possible degree: critical pairs are considered by increasing degree first.

From a complexity point of view, it is not easy to handle these degree falls in a complexity analysis. We now analyse the strategy of computing a Gröbner basis of the homogenized system and deshomogeneization.

Assume that we want to compute a Gröbner basis for the DRL ordering of an ideal $\mathcal{I}$ generated by an affine sequence of polynomials $\mathsf{F} = (f_1, \ldots, f_s)$ of degrees $(d_1, \ldots, d_s)$ in $\mathbb{K}[X]$. Let h be a new indeterminate. We denote by:

— $\mathsf{F}^{(h)}$ the sequence $(f_1^{(h)}, \ldots, f_s^{(h)})$ of polynomials in $\mathbb{K}[X]$, such that $f_i^{(h)}$ is the component of degree d_i of f_i.
— $\widetilde{\mathsf{F}}$ the sequence $(\tilde{f}_1, \ldots, \tilde{f}_s)$ of polynomials in $\mathbb{K}[X,h] = \mathbb{K}[x_1, \ldots, x_n, h]$, such that $\tilde{f}_i$ is the homogeneization of f_i (obtained by multiplying any monomial m in f_i by $h^{d_i - \deg(m)}$).

We denote by $\preceq$ both DRL orderings on $\mathbb{K}[X]$ and $\mathbb{K}[X,h]$. The following lemma proves that a Gröbner basis of F (non-necessarily reduced) can be obtained from $\widetilde{\mathcal{G}}$ and deshomogeneization. Notice that this lemma is specific to the DRL ordering.

Lemma 2.44. *Let $\mathcal{G}$ be a homogeneous Gröbner basis for DRL ordering of an ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \ldots, x_n, h]$ and $\lambda \in \mathbb{K}$. Then $\mathcal{G}_\lambda = \{g(x_1, \ldots, x_n, \lambda) \mid g \in \mathcal{G}\}$ is a Gröbner basis for DRL ordering in $\mathbb{K}[x_1, \ldots, x_n]$ of the ideal $\mathcal{I}_\lambda = \{f(x_1, \ldots, x_n, \lambda) \mid f \in \mathcal{I}\}$.*

Proof. We denote by φ_λ the following morphism.

$$\begin{array}{rccc} \varphi_\lambda : & \mathbb{K}[X,h] & \longrightarrow & \mathbb{K}[X] \\ & f & \longmapsto & f(x_1, \ldots, x_n, \lambda) \end{array}$$

It is clear that the ideal generated by $\mathcal{G}_\lambda$ is $\mathcal{I}_\lambda$. Then, assume first that $\lambda \neq 0$ and let $f \in \mathcal{I} \backslash \{0\}$. Therefore, there exists a polynomial $g \in \mathcal{G}$ such that $\mathsf{LM}_\preceq(g) | \mathsf{LM}_\preceq(f)$. By property of the DRL ordering, if γ is the power of h in $m = \mathsf{LM}_\preceq(g)$, all monomials in g are divisible by h^γ, and therefore $\varphi_\lambda(m) = \lambda^\gamma \mathsf{LM}_\preceq(\varphi_\lambda(g))$, which divides $\mathsf{LM}_\preceq(\varphi_\lambda(f))$, and $\mathcal{G}_\lambda$ is a Gröbner basis. Now if $\lambda = 0$, by property of the DRL ordering, a non-zero polynomial in $\mathcal{I}$ is mapped to 0 through φ_λ if and only if its leading monomial is divisible by h. Therefore, the same proof is still valid, but we only have to consider polynomials $f \in \mathcal{I}$ that are not divisible by h. □

With the previous lemma, we are able to compare the maximal degree arising in the reduced Gröbner bases of the system/ the homogenized system. We also compare them with the maximal degree in the reduced Gröbner basis of the homogeneous parts of higher degree.

Proposition 2.45. *Let $\mathcal{G}, \mathcal{G}^{(h)}$ and $\widetilde{\mathcal{G}}$ be the reduced Gröbner bases of $\mathsf{F}, \mathsf{F}^{(h)}$ and $\widetilde{\mathsf{F}}$ for $\preceq$. Then*

$$\max\{\deg(g) \mid g \in \mathcal{G}\} \leq \max\{\deg(g) \mid g \in \mathcal{G}^{(h)}\} \leq \max\{\deg(g) \mid g \in \widetilde{\mathcal{G}}\}$$

Proof of proposition 2.45. By previous lemma, $\varphi_1(\widetilde{\mathcal{G}})$ and $\varphi_0(\widetilde{\mathcal{G}})$ are Gröbner bases of $\langle \mathsf{F} \rangle$ and $\langle \mathsf{F}^{(h)} \rangle$. It follows that

$$\begin{cases} \max\{\deg(g) \mid g \in \mathcal{G}\} \leq \max\{\deg(g) \mid g \in \widetilde{\mathcal{G}}\} & \text{and} \\ \max\{\deg(g) \mid g \in \mathcal{G}^{(h)}\} \leq \max\{\deg(g) \mid g \in \widetilde{\mathcal{G}}\} \end{cases}$$

Moreover, since $\widetilde{\mathcal{G}}$ is reduced, it follows that the non-zero elements of $\varphi_0(\widetilde{\mathcal{G}})$ forms the reduced Gröbner basis of $\langle \mathsf{F}^{(h)} \rangle$. Now, denote by $\chi(f)$ the homogeneization of a polynomial f in $\mathbb{K}[X]$. Let g be a polynomial in $\mathcal{G}$. Then, there exists a relation $g = \sum_{i=1}^s f_i p_i$ with $p_i \in \mathbb{K}[X]$. Since $\chi(g_i) = \sum_{i=1}^s \chi(f_i)\chi(p_i)$, $\chi(g)$ belongs to $\langle \widetilde{\mathsf{F}} \rangle$ and its leading monomial is divisible by the leading monomial of a polynomial $\tilde{g}$ in $\widetilde{\mathcal{G}}$. $\tilde{g}$ is not divisible by h, therefore $\varphi_0(\tilde{g})$ belongs to $\mathcal{G}^{(h)}$, and has same leading monomial as g. Hence,

$$\max\{\deg(g) \mid g \in \mathcal{G}\} \leq \max\{\deg(g) \mid g \in \mathcal{G}^{(h)}\}$$

and the proposition is proved. □

Example 2.46. *The inequalities in proposition 2.45 can be strict. For example, let* $f_1 = x^2$ *and* $f_2 = x + 1$ *in* $\mathbb{K}[x]$*. Then,*

$$\mathcal{G} = \{1\}, \qquad \mathcal{G}^{(h)} = \{x\} \qquad \text{and} \qquad \widetilde{\mathcal{G}} = \{x + h, h^2\}$$

From proposition 2.45, we see that while studying the complexity of computing a Gröbner basis of an affine system, having informations on the sequence of the homogeneous parts of the polynomials in the system could be useful. Hence, in several papers [4, 5, 6, 93], the authors define *semi-regular sequences of affine polynomials* as sequences such that the homogeneous parts of higher degree is semi-regular. It seems that the following complexity bound can be obtained (but does not appear in the litterature yet).

Theorem 2.47. *Let* $\mathsf{F} = (f_1, \ldots, f_s) \in \mathbb{K}[X]^s$ *be a polynomial family and let* $\mathsf{F}^{(h)}$ *be the family of homogeneous components of highest degree. If* $\langle \mathsf{F}^{(h)} \rangle$ *is* 0*-dimensional, then the complexity of computing a Gröbner basis of* F *for the DRL ordering is bounded by*

$$O\left(s\binom{n + i_{reg}(\mathsf{F}^{(h)})}{i_{reg}(\mathsf{F}^{(h)})}^{\omega}\right)$$

Chapter 3

Invariant Theory and Monomial Algebras

The aim of this thesis is to use the struture of an input system, in order to speed up the computations. Hence, we have to consider some algebras, that are not the whole ring $\mathbb{K}[X]$. In this chapter, we present algebras that will be used in chapters 4 and 5. The first section is dedicated to the study of the action of a finite group on polynomials, which leads to the study of the ring of *invariants*. We also study *semi-invariants* through the representation of finite groups.

The second section deals with monomial algebras, namely algebras generated by monomials. We do not only consider monomials of $\mathbb{K}[x_1, \ldots, x_n]$ but also monomials of the ring of Laurent polynomials $\mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

3.1 Invariant Theory

In this section, X denotes the set of indeterminates $\{x_1, \ldots, x_n\}$ for a given $n \geq 1$, $\mathbb{K}$ is a given field, and $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. We will present the action of groups on polynomials, and we restrict our discussion to *finite groups*.

The aim of the section is twofold: on the first hand, explaining the classical strategies used to solve systems of polynomial equations which are stable under the action of a finite group. These strategies are related to the *invariant theory of finite groups*. On the other hand, we prepare the reader to chapter 4: computations of a basis of all invariants of a given degree will be needed before applying the SAGBI Matrix-F_5 algorithm 1.68 in section 4.3. In order to design an approach that solves polynomial systems of systems *globally* invariant under the action of an abelian group in section 4.2, we present representations and groups and the gradation on $\mathbb{K}[X]$ induced by *irreducible chracters*. Finally, to give complexity bounds for these variants, we need to estimate the dimensions of the components occuring in the previous gradation.

The section is organized as follows: we first present the action of groups on polynomials and explain how to compute invariants. Then, we present Molien's theorem which is a formula giving the Hilbert series of the ring of invariants. The third subsection is devoted to classical approaches solving systems of invariant equations. Then, we present representations of groups: the ring of invariants appears to be an *isotypic component* of $\mathbb{K}[X]$ viewed as a representation, and we give a generalization of Molien's formula to all components. The final subsection gives estimates on the dimensions of the isotypic components.

3.1.1 Action of Groups on Polynomials. Computation of Invariants

In this subsection, we define the invariants of a finite group $\mathbf{G}$, and explain how to compute them.

Action of Groups on Polynomials. Let V be the vector space spanned by $X = \{x_1, \ldots, x_n\}$ on $\mathbb{K}$. The linear group $\mathcal{GL}_n(\mathbb{K})$ acts linearly on V^n: for $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{GL}_n(\mathbb{K})$ and $L = (\ell_1, \ldots \ell_n) \in V^n$, we set

$$A.L = \left(\sum_{i=1}^{n} a_{i,j} \ell_i \right)_{1 \leq j \leq n}$$

This action extends to polynomials in $\mathbb{K}[X]$ in the following way. For $f \in \mathbb{K}[X]$ and $A \in \mathcal{GL}_n(\mathbb{K})$, we set f^A the polynolmial $f(A.X)$.

Proposition 3.1. *The action of $\mathcal{GL}_n(\mathbb{K})$ on $\mathbb{K}[X]$ given by $(A, f) \mapsto f^A$ is a* right *action of $\mathcal{GL}_n(\mathbb{K})$ on $\mathbb{K}[X]$.*

Proof. For $f \in \mathbb{K}[X]$ and $A, B \in \mathcal{GL}_n(\mathbb{K})$, we have $(f^A)^B = f(A.(B.X)) = f^{AB}$. Moreover, $f^{I_n} = f$. □

Remark 3.2. *In several classical books [100, 16], the authors choose to make $\mathcal{GL}_n(\mathbb{K})$ acting on $\mathbb{K}[X]$ by $f^A = f(A^{-1}X)$ to ensure a left action. We make another choice here, in order to keep the relation $(f^A)^B = f^{AB}$.*

Now $\mathbf{G}$ will denote a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$. The group $\mathbf{G}$ acts also on $\mathbb{K}[X]$, and we now define invariants under the action of $\mathbf{G}$.

Definition 3.3. *A polynomial $f \in \mathbb{K}[X]$ is said to be $\mathbf{G}$-invariant, if $f^A = f$ for all A in $\mathbf{G}$.*

If $f \in \mathbb{K}[X]$ satisfies $f^A = f$ for some $A \in \mathcal{GL}_n(\mathbb{K})$, it is easy to prove that $f^B = f$ for all B in the subgroup generated by A in $\mathcal{GL}_n(\mathbb{K})$. This result has an obvious generalization, as says the following proposition:

Proposition 3.4. *Let $S(\mathbf{G})$ be a* generating set *of $\mathbf{G}$. Then $f \in \mathbb{K}[X]$ belongs to $\mathbb{K}[X]^{\mathbf{G}}$ if and only if $f^A = f$ for all A in $S(\mathbf{G})$.*

Example 3.5. *Consider the cyclic matrix group $\mathbf{G}$ generated by the matrix $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ Denote by f the polynomial $x_1^2 + x_2^2$ and by g the polynomial $x_1 x_2$. Then $f^A = x_2^2 + (-x_1)^2 = f$ and $g^A = x_2(-x_1) = -g$. Therefore, f is $\mathbf{G}$-invariant, while on a field of characteristic different from 2, g is not.*

The set of all $\mathbf{G}$-invariants will be denoted by $\mathbb{K}[X]^{\mathbf{G}}$. It is easy to see that the sum and product of invariants are also invariants. Moreover, if m is a monomial of degree d in $\mathbb{K}[X]$, and $A \in \mathcal{GL}_n(\mathbb{K})$, the polynomial m^A is homogeneous of degree d. Therefore, the following proposition holds:

Proposition 3.6. *The set $\mathbb{K}[X]^{\mathbf{G}}$ is a graded subalgebra of $\mathbb{K}[X]$. More precisely, we have the decomposition $\mathbb{K}[X]^{\mathbf{G}} = \oplus_{d=0}^{+\infty} \mathbb{K}[X]_d^{\mathbf{G}}$, where $\mathbb{K}[X]_d^{\mathbf{G}}$ is the set of invariant homogeneous polynomials of degree d.*

Computation of Invariants We now answer the question of computing invariants. More precisely, we want to compute all invariants of a given degree d.

Linear algebra technique. [67] A first, costly technique, is to use linear algebra: all we have to do is to solve the system $\{f^A = f \mid \forall A \in \mathbf{G}\}$ on $\mathbb{K}[X]_d$. Proposition 3.4 shows that this system is equivalent to $\{f^A = f \mid \forall A \in S(\mathbf{G})\}$, where $S(\mathbf{G})$ is a minimal generating set of $\mathbf{G}$. The idea is to introduce the following exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{K}[X]_d^{\mathbf{G}} & \longrightarrow & \mathbb{K}[X]_d & \xrightarrow{\phi_d} & \bigoplus_{A\in S(\mathbf{G})} \mathbb{K}[X]_d \\ & & & & f & \longmapsto & (f^A - f)_{A\in S(\mathbf{G})} \end{array}$$

A basis of $\mathbb{K}[X]_d^{\mathbf{G}}$ can be computed as a basis of the kernel of ϕ_d. This leads to the algorithm 3.7.

Algorithm 3.7: ComputeBasisLinear algorithm

Input : The group $\mathbf{G}$, given by a minimal set of generators $S(\mathbf{G})$, an integer d, an ordering $\preceq$ and the lists B_d of monomials of degree d, sorted by decreasing order for $\preceq$.
Output: A basis of $\mathbb{K}[X]_d^{\mathbf{G}}$
$M :=$ Matrix with $\binom{n+d-1}{d}$ columns corresponding to the monomials of degree d of $\mathbb{K}[X]$, sorted by $\preceq$ with decreasing order, and $|S(\mathbf{G})|\binom{n+d-1}{d}$ rows;
Fill the matrix M to obtain the matrix of the map ϕ_d;
Compute a Gaussian-Reduction of M; `// Row-Echelon Reduction with permutations of rows and cancellation of zero-lines`
Join vertically to M an identity block of size $\binom{n+d-1}{d} \times \binom{n+d-1}{d}$;
Compute a Gaussian-Reduction of M; `// Column-Echelon Reduction of the top block`
$L :=$ list of polynomials corresponding to a column of M, the first block of which is zero;
return L

The following proposition can be found in [67], but we give a more precise result, based on the theorem 1.39.

Proposition 3.8. *The complexity of computing a basis of $\mathbb{K}[X]_d^{\mathbf{G}}$ with algorithm 3.7 can be done with $O\left(|S(\mathbf{G})|\binom{n+d-1}{d}^{\omega}\right)$ operations in $\mathbb{K}$, with $S(\mathbf{G})$ a set of generators of G and ω the exponent of linear algebra.*

Proof. To fill the matrix M in algorithm 3.7, we have to apply the group generators $S(\mathbf{G})$ to all monomials of degree d. For each $A \in S(\mathbf{G})$ and each monomial m of degree d, we have to compute the product of d linear forms. This can be done basically by computing the product of a polynomial of degree i with a linear form for each i between 1 and $d-1$, so the cost is:

$$O\left(n\sum_{i=1}^{d-1}\binom{n+i-1}{n-i}\right) = O\left(d\binom{n+d-1}{d}\right)$$

This cost is negligible, compared to the cost of computing the Gaussian elimination: we have a system of $\binom{n+d-1}{n-1}$ unknows and $S(\mathbf{G})\binom{n+d-1}{n-1}$ columns, and rank bounded by the number of unknows. From theorem 1.39, it is possible to perform the Gaussian elimination on a matrix

of size $\ell \times c$ and rank r in $O(\ell c r^{\omega-2})$ operations in $\mathbb{K}$. Therefore, we need $O\left(S(\mathbf{G})\binom{n+d-1}{n-1}^{\omega}\right)$ operations in $\mathbb{K}$ to compute a basis of all invariants of degree d. □

The non-modular case. When the characteristic of the field $\mathbb{K}$ divides the cardinal of the group $\mathbf{G}$, we say that we are in *the modular case*. This case is much more complicated than the non-modular case. As we will see in the sequel, many results available in the non-modular case do not extend to the modular case. First, in the non-modular case, it is possible to average with the action of G:

Definition 3.9. *Assume that* $\mathsf{char}(\mathbb{K}) \nmid |\mathbf{G}|$. *The* Reynolds operator *of* $\mathbf{G}$ *is the map*

$$\begin{array}{rccc} \Re_{\mathbf{G}} : & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & f & \longmapsto & \dfrac{1}{|\mathbf{G}|}\displaystyle\sum_{A\in\mathbf{G}} f^A \end{array}$$

The indice $\mathbf{G}$ will be omitted if it is clear. We recall the following properties of the Reynolds operator:

Proposition 3.10. *[25] Let* $\Re$ *be the Reynolds operator of the finite matrix group* $\mathbf{G}$.

(i) $\Re$ *is* $\mathbb{K}$*-linear.*

(ii) *If* $f \in \mathbb{K}[X]$, *then* $\Re(f) \in \mathbb{K}[X]^{\mathbf{G}}$.

(iii) *If* $f \in \mathbb{K}[X]^{\mathbf{G}}$, *then* $\Re(f) = f$. *Therefore,* $\Re$ *is a projection onto* $\mathbb{K}[X]^{\mathbf{G}}$.

(iv) *Every* A *in* $\mathbf{G}$, *viewed as a linear isomorphism on* $\mathbb{K}[X]$, *verifies* $A \circ \Re = \Re \circ A = \Re$.

Proof. Points (i) and (iii) are obvious. For point (ii), we just have to see that if $B \in \mathbf{G}$, $A \mapsto AB$ is a bijection on $\mathbf{G}$, Therefore, $\Re(f)^B = \frac{1}{|G|}\sum_{A\in G} f^{AB} = \Re(f)$, and $\Re(f)$ belongs to $\mathbb{K}[X]^{\mathbf{G}}$. For point (iv), $A \circ \Re = \Re$ comes from the fact that the image of $\Re$ is $\mathbb{K}[X]^{\mathbf{G}}$, and $\Re \circ A = \Re$ can be proved with the same argument given for point (ii). □

The Reynolds operator allows us to compute a basis of $\mathbb{K}[X]_d^{\mathbf{G}}$: all we have to do is to apply it to all monomials of degree d, and perform a Gaussian elimination on a matrix to obtain the basis. This leads to algorithm 3.11.

Algorithm 3.11: ComputeBasisNonModular algorithm

Input : The group $\mathbf{G}$ and the Reynolds Operator $\Re$ on $\mathbf{G}$, an integer d, an ordering $\preceq$ and the list B_d of monomials of degree d, sorted by decreasing order for $\preceq$.
Output: A basis of $\mathbb{K}[X]_d^{\mathbf{G}}$
M :=Square matrix with of size $\binom{n+d-1}{d} \times \binom{n+d-1}{d}$ corresponding to the monomials of degree d of $\mathbb{K}[x_1, \ldots, x_n]$, sorted by $\preceq$ with decreasing order;
Fill M with the rows corresponding to $\Re(m)$ for all monomials m in B_d;
Compute a Gaussian-Reduction of M; `//Row-Echelon Reduction with permutations of rows and cancellation of zero-lines`
$L :=$ list of polynomials corresponding to a row of M;
return L

The arithmetic complexity of algorithm 3.11 is better than those of algorithm 3.7, as shows the following proposition.

Proposition 3.12. *To compute a basis of $\mathbb{K}[X]_d^{\mathbf{G}}$ in the non-modular case with algorithm 3.11, at most*

$$O\left(d|\mathbf{G}|\binom{n+d-1}{n-1}^2+\binom{n+d-1}{n-1}^{\omega}\right)$$

arithmetic operations in $\mathbb{K}$ are needed.

Proof. The proof is very similar to the proof of proposition 3.10. Since we have to apply all elements of $|\mathbf{G}|$ to a monomial, $\Re(m)$ can be computed within $O\left(d|\mathbf{G}|\binom{n+d-1}{n-1}\right)$ operations in $\mathbb{K}$. We have to apply it $\binom{n+d-1}{n-1}$ times and the other term in the formula is the cost of computing the Gaussian elimination on M. □

In practice, we do not have to apply the Reynolds Operator to all monomials of degree d, if we know in advance the dimension of $\mathbb{K}[X]_d^{\mathbf{G}}$. This can be computed by Molien's formula, see next subsubsection.

Special case: G is a subgroup of the group of generalized permutation matrices. The group of generalized permutation matrices is the subgroup of $\mathcal{GL}_n(\mathbb{K})$, the matrices of which only have one non-zero coefficient per row and column. We recall here the structure of this group, and we start by the classical permutation matrix group.

Proposition 3.13. *The symmetric group $\mathfrak{S}_n$ can be embedded in $\mathcal{GL}_n(\mathbb{K})$.*

Proof. To the permutation σ we associate the matrix $M_\sigma = (m_{i,j})_{1\leq i,j\leq n}$, where $m_{i,j} = 1$ if $\sigma(j) = i$ and 0 otherwise. □

In the sequel, we will always identify a permutation $\sigma \in \mathfrak{S}_n$ with the matrix M_σ given by the proof of proposition 3.13.

Proposition 3.14. *The set of all matrices of $\mathcal{GL}_n(\mathbb{K})$ having one and only one element non equal to zero in each row and each column is a subgroup equal to the semidirect product $D_n(\mathbb{K}^*) \rtimes \mathfrak{S}_n$, where $D_n(\mathbb{K}^*)$ is the subgroup of diagonal matrices in $\mathcal{GL}_n(\mathbb{K})$.*

Proof. Is is clear that this set of matrices is the direct product of the set $D_n(\mathbb{K}^*)$ and the set $\mathfrak{S}_n$, viewed as a set of matrices. Moreover, for each $M_\sigma \in \mathfrak{S}_n$ and each $D \in D_n(\mathbb{K}^*)$, $M_\sigma D M_\sigma^{-1} \in D_n(\mathbb{K}^*)$, so $D_n(\mathbb{K}^*)$ is normal in the group generated by $D_n(\mathbb{K}^*)$ and $\mathfrak{S}_n$. Finally, $D_n(\mathbb{K}^*) \cap \mathfrak{S}_n = \{I_n\}$ and the proposition is proved. □

In the sequel, the notation $D_n(\mathbb{K}^*) \rtimes \mathfrak{S}_n$ will always refer to the generalized permutations matrix group. When $\mathbf{G}$ is a finite subgroup of $D_n(\mathbb{K}^*) \rtimes \mathfrak{S}_n$, we do not need to use linear algebra to compute invariants, since *orbit sums* of monomials can be used instead, which leads only to combinatorial tools.

Definition – Proposition 3.15. *[16] Let m be a monomial of degree d, we denote by $\mathbf{G}_m$ the* stabilizer *of m in $\mathbf{G}$, namely the subgroup of $\mathbf{G}$ given by $\{A \in \mathbf{G} \mid m^A = m\}$. Then we choose a fixed set of left coset representatives $\mathbf{G}/\mathbf{G}_m = \{A_1, \ldots, A_r\}$ and computes the* orbit *$\Omega_m = \{m^{A_i} \mid 1 \leq i \leq r\}$, which is independent of the choice of the set $\{A_i\}$. Therefore the invariant $Tr_{\mathbf{G}_m}^{\mathbf{G}}(m) = \sum_{i=1}^r m^{A_i}$ is independent of the choice of $\{A_i\}$ and will be called the* orbit sum *of m.*

Example 3.16. *Let* $\mathbf{G}$ *be the cyclic matrix group of order* 4 *generated by* $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *on a field of characteristic different from 2 and* $\mathbb{K}[X] = \mathbb{K}[x, y]$*. Then :*

— $\mathbf{G}_x = \{I_2\}$ *so* $\mathbf{G}/\mathbf{G}_x = \mathbf{G}$ *and* $\{x^A \mid A \in \mathbf{G}\} = \{x, y, -x, -y\}$*: the orbit sum of* x *is zero.*

— $\mathbf{G}_{x^3y} = \{\pm I_2\}$ *and we can take* $\mathbf{G}/\mathbf{G}_{x^3y} = \{I_2, A\}$*. The orbit sum of* x^3y *is* $x^3y - xy^3$*.*

Remark 3.17. *In the non-modular case, the* orbit sum *is very close to the* Reynolds Operator*, since for each monomial* m*,* $\Re(m) = \frac{|\mathbf{G}_m|}{|\mathbf{G}|} Tr^{\mathbf{G}}_{\mathbf{G}_m}(m)$*.*

We now give a special name to leading monomials of invariants.

Definition 3.18. *Let* $\preceq$ *be an ordering on* $\mathbb{K}[X]$*. For every finite group* $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{K})$*, if* m *is the leading monomial of an invariant in* $\mathbb{K}[X]^{\mathbf{G}}$*, we call* m *an initial monomial.*

Example 3.19. *Let* $\mathbf{G}$ *be the alternate group* $\mathfrak{A}_3$ *of order 3, acting on* $R = \mathbb{Q}[x, y, z]$ *with graded lexicographical ordering such that* $x > y > z$*. The Reynolds operator is given by* $\Re(f) = (f(x, y, z) + f(y, z, x) + f(z, x, y))/3$*. Then* $u = x^2y + y^2z + xz^2 \in \mathbb{K}[X]^{\mathbf{G}}$ *is the orbit sum of* x^2y*, which is an initial monomial while* y^2z *and* xz^2 *are not.*

Theorem 3.20. *If* $\mathbf{G}$ *is a finite subgroup of* $D_n(\mathbb{K}^*) \rtimes \mathfrak{S}_n$*, the orbit sums of all initial monomials of degree* d *form a basis of* $\mathbb{K}[X]^{\mathbf{G}}_d$*.*

Proof. Let m be a monomial of some degree d. Then the orbit $\Omega(m) = \{m^{A_i} \mid 1 \leq i \leq r\}$ consists in terms of the form $\xi m'$, with $\xi \in \mathbb{K}^*$ and m' a monomial of same degree d. Let $\xi m'$ be one of these terms. Clearly, $\Omega(m') = \{\xi^{-1} m^{A_i}\}$, so $Tr^{\mathbf{G}}_{\mathbf{G}_{m'}}(m') = \xi^{-1} Tr^{\mathbf{G}}_{\mathbf{G}_m}(m)$. Now, let $f \in \mathbb{K}[X]^{\mathbf{G}}_d \backslash \{0\}$ and $m = \mathsf{LM}_{\preceq}(f)$. Then $Tr^{\mathbf{G}}_{\mathbf{G}_m}(m) \neq 0$ and $f - \frac{\mathsf{LC}_{\preceq}(f)}{\mathsf{LC}_{\preceq}(Tr^{\mathbf{G}}_{\mathbf{G}_m}(m))} Tr^{\mathbf{G}}_{\mathbf{G}_m}(m)$ belongs to $\mathbb{K}[X]^{\mathbf{G}}_d$ and has a smaller leading monomial. The proof follows by induction. □

From theorem 3.20, we deduce the algorithm 3.21 that computes a basis of $\mathbb{K}[X]^{\mathbf{G}}$ up to some degree D.

Algorithm 3.21: ComputeBasisGeneralizedPermutation algorithm

Input : The group $\mathbf{G} \subset D_n(\mathbb{K}^*) \rtimes \mathfrak{S}_n$, an integer d, an ordering $\preceq$ and the list B_d of monomials of degree d, sorted by decreasing order for $\preceq$.
Output: A basis of $\mathbb{K}[X]^{\mathbf{G}}_d$
while $B_d \neq \emptyset$ **do**
  m :=First(B_d);
  Compute Ω_m, the orbit of m;
  if $Tr^{\mathbf{G}}_{\mathbf{G}_m}(m) = \sum_{t \in \Omega_m} t \neq 0$ **then** add $Tr^{\mathbf{G}}_{\mathbf{G}_m}(m)$ to L;
  Remove from B_d all monomials that appear in Ω_m, up to multiplication by a scalar;
return L

For every monomial m of degree d, at most $dn|\mathbf{G}|$ operations in $\mathbb{K}$ are needed to compute Ω_m. Therefore, the following theorem holds:

Theorem 3.22. *A basis of each component* $\mathbb{K}[X]^{\mathbf{G}}_d$ *can be computed in* $O\left(dn|\mathbf{G}|\binom{d+n-1}{d}\right)$ *operations in* $\mathbb{K}$*, using algorithm 3.21.*

Remark 3.23. *This approach by orbit sums is classical when* $\mathbf{G} \subseteq \mathfrak{S}_n$ *(see for example [100, 67]). In this case, the* **if** *condition in algorithm 3.21 is automatically satisfied and can be omitted. Moreover, no arithmetic operations in* $\mathbb{K}$ *are needed.*

3.1.2 Molien's Theorem

In this subsection, we introduce the Hilbert series of the algebra of invariants $\mathbb{K}[X]^{\mathbf{G}}$, which can be easily computed, at least in the non-modular case. A generalization of this formula will be seen in subsection 3.1.4. It will be useful to give estimates on the dimension $\dim_{\mathbb{K}}(\mathbb{K}[X]_d^{\mathbf{G}})$ of the vector space of invariant polynomials of a given degree d, see 3.1.5.

Definition 3.24. *The Hilbert Series (see definition 2.19) of the algebra $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$, equal to $HS_{\mathbb{K}[X]^{\mathbf{G}}}(z) = \sum_{d=0}^{+\infty} \dim_{\mathbb{K}}(\mathbb{K}[X]_d^{\mathbf{G}}) z^d$, is called the Molien Series of $\mathbf{G}$.*

For $A \in \mathbf{G}$, the characteristic polynomial of A given by $\det(I_n - zA)$ is a polynomial with a non-zero constant coefficient. Therefore, the formal series given by $1/\det(I_n - zA)$ is well defined. The following result of Molien relates these series with the Molien series of $\mathbf{G}$, on a field of zero characteristic.

Theorem 3.25 (Molien)**.** *[100] Let $\mathbf{G}$ be a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$ with $\mathbb{K}$ a field of zero characteristic. Then*

$$HS_{\mathbb{K}[X]^{\mathbf{G}}}(z) = \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{1}{\det(I_n - zA)}$$

We follow the proof of Sturmfels [100]. In order to prove theorem 3.25, we first give a lemma.

Lemma 3.26. *Let $m \geq 1$ and $\mathbb{K}$ be a field of zero characteristic. Let $\mathbf{H}$ be a finite subgroup of $\mathcal{GL}_m(\mathbb{K})$. We define the invariant subspace of $\mathbb{K}^m$ under $\mathbf{H}$ by*

$$V^{\mathbf{H}} = \{\mathbf{v} \in \mathbb{K}^m \mid A\mathbf{v} = \mathbf{v} \text{ for all } A \text{ in } \mathbf{H}\}$$

Then, $\dim_{\mathbb{K}}(V^{\mathbf{H}}) = \frac{1}{|\mathbf{H}|} \sum_{A \in \mathbf{H}} \operatorname{trace}(A)$.

Proof. We introduce the average operator $P_{\mathbf{H}}$ on $\mathbb{K}^m$, defined by $P_{\mathbf{H}} = \frac{1}{|\mathbf{H}|} \sum_{A \in \mathbf{H}} A$. We claim that this operator is a projection onto $V^{\mathbf{H}}$. This concludes the proof since the rank of a projection is equal to its trace. It is easy to see that $P_{\mathbf{H}}$ is a projector: Again by the fact that if $B \in \mathbf{H}$, $A \mapsto AB$ is a bijection on $\mathbf{H}$, we see that $P_{\mathbf{H}}(\mathbb{K}^m) \subseteq V^{\mathbf{H}}$, and its clear that $P_{\mathbf{H}}(\mathbf{v}) = \mathbf{v}$ for all $v \in V^{\mathbf{H}}$. □

Proof of theorem 3.25. $\mathbb{K}[X]_d$ is a $\mathbb{K}$ vector space of dimension $\binom{n+d-1}{n-1}$, and every $A \in \mathbf{G}$ induces a linear transformation on $\mathbb{K}[X]_d$, denoted by $A^{(d)}$. With this notation, $\mathbb{K}[X]_d^{\mathbf{G}}$ becomes exactly the invariant subspace of $\mathbb{K}[X]_d$ under the group $\mathbf{H} = \{A^{(d)} \mid A \in \mathbf{G}\}$. We are now interested in the values of $\operatorname{trace}(A^{(d)})$. The trace of an operator is invariant under field extensions, therefore we might assume that $\mathbb{K}$ is algebraically closed. Let $\ell_{A,1}, \ldots, \ell_{A,n}$ be the eigenvectors of $A^{(1)} = A$ on $\mathbb{K}[X]_1 \simeq \mathbb{K}^n$, associated to the eigenvalues $\lambda_{A,1}, \ldots, \lambda_{A,n}$. Then, $\{\ell_{A,1}, \ldots, \ell_{A,n}\}$ is a basis of $\mathbb{K}[X]_1$, therefore

$$\left\{ \ell_{A,1}^{\alpha_1} \cdots \ell_{A,n}^{\alpha_n} \;\middle|\; (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \text{ and } \sum_{i=1}^{n} \alpha_i = d \right\}$$

is a basis of $\mathbb{K}[X]_d \simeq \mathbb{K}[X]_1 \otimes \cdots \otimes \mathbb{K}[X]_1$. Moreover, these products of linear forms are eigenvectors of $A^{(d)}$ associated to the eigenvalues $\lambda_{A,1}^{\alpha_1} \cdots \lambda_{A,n}^{\alpha_n}$ where $\sum \alpha_i = d$. It follows that

$$\operatorname{trace}(A^{(d)}) = \sum_{\alpha_1 + \cdots \alpha_n = d} \lambda_{A,1}^{\alpha_1} \cdots \lambda_{A,n}^{\alpha_n}$$

Finally, using lemma 3.26 and the definition of the Molien Series of $\mathbf{G}$, we obtain:

$$\begin{aligned}
\mathsf{HS}_{\mathbb{K}[X]^{\mathbf{G}}}(z) &= \sum_{d=0}^{+\infty} \dim_{\mathbb{K}}(\mathbb{K}[X]_d^{\mathbf{G}}) z^d \\
&= \sum_{d=0}^{\infty} \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \left(\sum_{\alpha_1 + \cdots \alpha_n = d} \lambda_{A,1}^{\alpha_1} \cdots \lambda_{A,n}^{\alpha_n} \right) z^d \\
\mathsf{HS}_{\mathbb{K}[X]^{\mathbf{G}}}(z) &= \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n} \lambda_{A,1}^{\alpha_1} \cdots \lambda_{A,n}^{\alpha_n} \quad z^{\alpha_1 + \cdots + \alpha_n} \\
&= \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{1}{(1 - z\lambda_{A,1}) \times \cdots \times (1 - z\lambda_{A,n})} \\
\mathsf{HS}_{\mathbb{K}[X]^{\mathbf{G}}}(z) &= \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{1}{\det(I_n - zA)}
\end{aligned}$$

□

It is possible to extend Molien's theorem in several ways. First, observe that lemma 3.26 is still valid if $\mathbb{K}$ is a field of finite characteristic, which does not divide $|\mathbf{H}|$, but only modulo the characteristic of the field $\mathrm{char}(\mathbb{K})$. Consequently, the following theorem holds.

Theorem 3.27. *Let $\mathbf{G}$ be a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$ with $\mathbb{K}$ a field of characteristic $p = \mathrm{char}(\mathbb{K})$ such that $p \nmid |\mathbf{G}|$. Then*

$$\overline{HS_{\mathbb{K}[X]^{\mathbf{G}}}(z)}^{p} = \frac{1}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{1}{\det(I_n - zA)} \in \mathbb{F}_p[[z]]$$

where $\overline{HS_{\mathbb{K}[X]^{\mathbf{G}}}(z)}^{p}$ is the reduction of $HS_{\mathbb{K}[X]^{\mathbf{G}}}(z)$ modulo p through the morphism $\mathbb{Z}[[z]] \to \mathbb{F}_p[[z]]$.

Then, if $\mathrm{char}(\mathbb{K})$ is big enough, it is possible to know enough terms of $\mathsf{HS}_{\mathbb{K}[X]^{\mathbf{G}}}(z)$ to know it exactly.

Another possible extension is the following: assume that $\mathbf{G}$ is a finite subgroup of the generalized permutations subgroup, with coefficients in a finite field $\mathbb{K}$. Since $\mathbb{K}$ is a finite field, the group $\mathbb{K}^*$ is cyclic, therefore there is an embedding of $\mathbb{K}^*$ into $\mathbb{C}^*$, which gives an embedding of $\mathbf{G}$ into $\mathcal{GL}_n(\mathbb{C})$. Denote by $\tilde{\mathbf{G}}$ the resulting group in $\mathcal{GL}_n(\mathbb{C})$. Appying algorithm 3.21 with $\mathbf{G}$ or $\tilde{\mathbf{G}}$ produces exactly the same result, up to the embedding $\mathbb{K}^* \hookrightarrow \mathbb{C}^*$. In particular, the Hilbert series of $\mathbb{K}[X]^{\mathbf{G}}$ and $\mathbb{C}[X]^{\mathbf{G}}$ are the same, and the Molien series of $\mathbb{K}[X]^{\mathbf{G}}$ can be computed with Molien's formula. Finally, we will see in subsection 3.1.4 a generalization of this formula to *isotypic components* of $\mathbb{K}[X]$, $\mathbb{K}[X]^{\mathbf{G}}$ being one of these components.

3.1.3 Structure of the algebra of invariants, and classical strategies

In this subsection, we recall classical results on the structure of the algebra of invariants $\mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}} = \mathbb{K}[X]^{\mathbf{G}}$. Then, we explain the classical strategies used to solve a system of invariant equations.

Structure of the Algebra of Invariants. We start by giving a famous theorem due to Hilbert, which states that the ring of invariants is finitely generated.

Theorem 3.28. *[55] Let $\mathbf{G} \subset GL_n(\mathbb{K})$. Then, there exist a finite number of invariants $h_1, \ldots, h_r$ such that $\mathbb{K}[X]^{\mathbf{G}} = \mathbb{K}[h_1, \ldots, h_r]$.*

Proof. Hilbert's proof was restricted to the case $\mathrm{char}(\mathbb{K}) = 0$. Emmy Noether proved this result without assumption on the characteristic in [80]. □

Definition 3.29. *Following notations of previous theorem, such a set of invariants $\{h_1, \ldots, h_r\}$ is called a set of* fundamental invariants.

It is interesting to give bounds on the degree we have to reach until we find a set of generators. The bound $|\mathbf{G}|$ in characteristic zero has been proved by Noether and advances on this topic have been made until recently and are summarized in [16]. We recall here the most interesting to our purpose.

Theorem 3.30. *Let $\mathbb{K}$ be a field, and $\mathbf{G}$ a non-trivial finite subgroup of $GL_n(\mathbb{K})$ with $n > 1$.*
- *[80, 47, 48] If $\mathrm{char}(\mathbb{K})$ does not divide $|\mathbf{G}|$, then $\mathbb{K}[X]^{\mathbf{G}}$ is generated by invariants of degree at most $|\mathbf{G}|$.*
- *[65, 103] If $\mathrm{char}(\mathbb{K})$ divides $|\mathbf{G}|$ and $\mathbb{K}$ is finite, then $\mathbb{K}[X]^{\mathbf{G}}$ is generated by invariants of degree at most $n(|\mathbf{G}| - 1)$.*

Usually, the minimal size r of a set of fundamental invariants can increase dramatically, compared to n, the rank of $\mathbb{K}[X]^{\mathbf{G}}$. Kemper and Steel gave algorithms to find a minimal set of fundamental invariants in [67]. As an example, we report in table 3.31 the size r of a minimal set for the cyclic group $C_n \subset \mathcal{GL}_n(\mathbb{K})$ given by the standard representation of the n-cycle $(1, 2, \ldots, n)$, together with the maximal degree of a polynomial in such a set. These invariants are computed with MAGMA, on two fields for each n: $\mathbb{F}_{65521}$ and a field $\mathbb{F}_p$ with p the smallest prime dividing n. Notice that the computation is much more difficult in the modular case (the computation has been stopped after 24 hours for boxes with interrogation marks).

$\mathbb{K}$	n	3	4	5	6	7	8	9	10
$\mathbb{F}_{65521}$	Number of Invariants	4	7	15	20	48	65	119	166
	Maximal degree of an invariant	3	4	5	6	7	8	9	10
$\mathbb{F}_p, p\|n$	Number of Invariants	4	8	21	23	?	?	?	?
	Maximal degree of an invariant	3	5	7	6	?	?	?	?

Table 3.31 – Computation of Fundamental Invariants

A dimension argument shows that $r \geq n$. An interesting question is to characterize the groups where r can be taken equal to n. We now recall some classical results about the well known *symmetric group* and *symmetric polynomials*. The group $\mathfrak{S}_n$ is viewed as a subgroup of $\mathcal{GL}_n(\mathbb{K})$ through the morphism in proposition 3.13.

Definition 3.32. *A polynomial $f \in \mathbb{K}[X]$ is said to be symmetric if it is invariant under the symmetric group $\mathfrak{S}_n$.*

The coefficients of the polynomial $f(z) = (z+x_1)\cdots(z+x_n) = z^n + \sigma_1 z^{n-1} + \cdots + \sigma_n$ with respect to the new variable z are the so called *elementary symmetric polynomials*. From the elementary symmetric polynomials, we can construct other symmetric polynomials by taking polynomials in $\sigma_1, \ldots, \sigma_n$. This leads to the well known theorem.

Theorem 3.33. *(Gauss)Every symmetric polynomial in $\mathbb{K}[X]$ can be written uniquely as a polynomial in the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$.*

An obvious consequence of the above theorem is that $\mathbb{K}[x_1, \ldots, x_n]^{\mathfrak{S}_n} = \mathbb{K}[\sigma_1, \ldots, \sigma_n]$. Therefore, in the case of the symmetric group, the minimal number of fundamental invariants is n. At least in the non-modular case, this fact can be generalized to reflection groups.

Definition 3.34. *A reflection s (sometimes called pseudo-reflection) of $\mathcal{GL}_n(\mathbb{K})$ is a matrix such that $Ker(s - id)$ has codimension 1. A finite subgroup $\mathbf{G}$ of $\mathcal{GL}_n(\mathbb{K})$ is said to be a reflection group if it is generated by reflections.*

Example 3.35. *The symmetric group $\mathfrak{S}_n$ is a reflection group in any characteristic, since it is generated by transpositions: if* $\mathrm{char}(\mathbb{K}) \neq 2$*, the element in $\mathcal{GL}_n(\mathbb{K})$ associated to a transposition is similar to a diagonal matrix with eigenvalues $(1, \ldots, 1, -1)$, whereas it is similar to a shear matrix if* $\mathrm{char}(\mathbb{K}) = 2$*. In both cases, those matrices are reflections.*

The theorem below explains why reflection groups are interesting: the number of fundamental invariants in the invariant algebra is as low as possible.

Theorem 3.36. Shephard-Todd, Chevalley, Serre,*[92, 22, 90] Assume that* $\mathrm{char}(\mathbb{K})$ *does not divide $|\mathbf{G}|$. Then $\mathbb{K}[X]^{\mathbf{G}}$ is generated by only n fundamental invariants if and only if $\mathbf{G}$ is a reflection group.*

Remark 3.37. *Notice that the* only if *part of previous theorem is actually verified even in the modular case.*

In this case, the polynomials $h_1, \ldots, h_n$ are algebraically independent, and the multiset $\{\deg(h_i)\}$ is unique. Moreover $\prod \deg(h_i) = |\mathbf{G}|$ and there are $\sum(\deg(h_i) - 1)$ reflections in $\mathbf{G}$. When dealing with a polynomial system of equations lying in $\mathbb{K}[X]^{\mathbf{G}}$ with $\mathbf{G}$ a reflection group, it is very interesting to reformulate the equations as polynomials in the polynomial ring $\mathbb{K}[h_1, \ldots, h_n]$. We have seen in chapter 2 that the complexity of solving a zero-dimensional system of polynomial equations is related to the sum of the degrees of the polynomials and the number of solutions of the system. The reformulation here leads to a system with the same number of variables but both degrees of equations and number of solutions decrease. Hence, using invariants in the framework of systems of equations individually invariant under a reflection group is very interesting.

Example 3.38. *Let $n_1, \ldots, n_k$ be positive integers such that $n = n_1 + \cdots + n_k$. Then, the direct product $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_k}$, which can be viewed as a subgroup of $\mathfrak{S}_n \subset \mathcal{GL}_n(\mathbb{K})$, is a reflection group with generators given by the symmetric polynomials in each set of n_i variables.*

These subgroups are actually the only reflection subgroups of $\mathfrak{S}_n$. In subsection 4.3.3, we will see other reflection groups, which are generalized permutations subgroups. We continue this subsection by describing primary and secondary invariants of an invariant algebra.

Definition 3.39. *Let $\mathbf{G}$ be a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$. A set of n algebraically independent polynomials in $\mathbb{K}[X]^{\mathbf{G}}$ is called a set of* primary invariants.

Such a set exists by Noether Normalization lemma (theorem 2.3). Denote by $\theta_1, \ldots, \theta_n$ a set of *primary invariants*. A dimension argument proves that $\mathbb{K}[X]^{\mathbf{G}}$ is a finitely generated module over the algebra $\mathbb{K}[\theta_1, \ldots, \theta_n]$. It is still an open question to give a necessary and sufficient condition on $\mathbf{G}$ for $\mathbb{K}[X]^{\mathbf{G}}$ to be a *free module* over $\mathbb{K}[\theta_1, \ldots, \theta_n]$ in the modular case, but the answer is much simpler in the non-modular case and is given in theorem 3.41.

Theorem 3.40. *If* $\mathrm{char}(\mathbb{K})$ *does not divide* $|\mathbf{G}|$, $\mathbb{K}[X]^{\mathbf{G}}$ *is a* Cohen-Macaulay *algebra (see definition 2.9).*

Proof. We refer to [57] for the proof. The main tool is the Reynolds Operator $\Re$ (definition 3.9) □

From the Cohen-Macaulayness of the ring of invariants in the non-modular case, one can prove that the following decomposition holds.

Theorem 3.41. *[100, 16] Assume that* $\mathrm{char}(\mathbb{K})$ *does not divide* $|\mathbf{G}|$, *and let* $\theta_1, \ldots, \theta_n$ *be a set of primary invariants of* $\mathbb{K}[X]^{\mathbf{G}}$. *Then, there exists a set of* secondary invariants $\{\eta_1, \ldots, \eta_t\}$ *such that* $\mathbb{K}[X]^{\mathbf{G}} = \oplus_{i=1}^{t} \eta_i \mathbb{K}[\theta_1, \ldots, \theta_n]$.

Corollary 3.42. *In the case of Cohen-Macaulayness of the ring of invariants, the Hilbert Series of* $\mathbb{K}[X]^{\mathbf{G}}$ *is given by*

$$HS_{\mathbb{K}[X]^{\mathbf{G}}}(z) = \frac{\sum_{j=0}^{t} z^{\deg(\eta_j)}}{\prod_{i=1}^{n}(1 - z^{\deg(\theta_i)})}$$

with (θ_i) *and* (η_j) *the sets of primary and secondary invariants associated to* $\mathbb{K}[X]^{\mathbf{G}}$.

Many authors gave algorithms to compute such a set of secondary invariants, see for example [67]. However, the number of secondary invariants can be very huge (it is greather than or equal to the minimal number of fundamental invariants). Hence, in the sequel we will try to avoid such a computation.

Classical approach to solve Invariant Systems. We now give classical algorithms to reformulate a given system in terms of invariants. We also explain the underlying geometric view. We introduce the definition and the associated notions of Gröbner basis in some invariant ring. This kind of Gröbner basis is the classical object that we want to compute while solving a polynomial system with symmetries, see [100, 27, 25]. We recall here the usual strategy presented by these authors. Let $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{K})$ be a finite group. We denote by $\mathbb{A}(\mathbb{K}^n)$ the affine space associated to $\mathbb{K}^n$.

Definition – Proposition 3.43. *From the action of* $\mathbf{G}$ *on* $\mathbb{K}^n$, *we deduce an action on the affine space* $\mathbb{A}(\mathbb{K}^n)$. *The orbit of a point* $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{A}(\mathbb{K}^n)$ *is the set* $\mathbf{G}.\mathbf{a} = \{g.\mathbf{a} \mid g \in \mathbf{G}\}$ *and is called the* $\mathbf{G}$*-orbit of* $\mathbf{a}$. *The set of all* $\mathbf{G}$*-orbits in* $\mathbb{A}(\mathbb{K}^n)$ *is denoted by* $\mathbb{A}(\mathbb{K}^n)/\mathbf{G}$ *and is called the* orbit space *of* $\mathbf{G}$.

Definition 3.44. *Let* $F = \{f_1, \ldots, f_s\}$ *be a set of polynomials. If the variety* $\mathbb{V}(\mathcal{I})$ *associated to the ideal* $\mathcal{I} = \langle F \rangle$ *is stable under the action of* $\mathbf{G}$ *on* $\mathbb{A}(\mathbb{K}^n)$, *we define the* orbit variety $\mathbb{V}(\mathcal{I})/\mathbf{G} \subset \mathbb{A}(\mathbb{K}^n)/\mathbf{G}$, *whose points are the* $\mathbf{G}$*-orbits of zeroes of* $\mathcal{I}$.

A sufficient condition for $\mathbb{V}$ to be a $\mathbf{G}$-stable variety is that all polynomials $f_1, \ldots, f_s$ belong to $\mathbb{K}[X]^{\mathbf{G}}$. Intuitively the idea is to compute a Gröbner basis associated with the relative orbit variety $\mathbb{V}(\mathcal{I})/\mathbf{G}$ instead of a Gröbner basis associated to $\mathbb{V}(\mathcal{I})$ itself. We now explain the classical way to compute a Gröbner basis associated to $\mathbb{V}(\mathcal{I})/\mathbf{G}$. We have seen in the previous subsection that Hilbert's theorem states that $\mathbb{K}[X]^{\mathbf{G}}$ is finitely generated. According to this point of view, we can introduce the following definition.

Definition 3.45. *Let $h_1, \ldots, h_r$ be a set of fundamental invariants of $\mathbb{K}[X]^{\mathbf{G}}$. Let $\mathcal{I}$ be an ideal generated by $\mathbf{G}$-invariant polynomials. We introduce r new variables $H_1, \ldots, H_r$, each H_i corresponding to a polynomial h_i, and we consider in the ring $\mathbb{K}[x_1, \ldots, x_n, H_1, \ldots, H_r]$, the following ideal:*

$$\tilde{\mathcal{J}} = \mathcal{I} + \langle H_1 - h_1(x_1, \ldots, x_n), \ldots, H_r - h_r(x_1, \ldots, x_n)\rangle$$

Then, a Gröbner basis $G_{\mathbb{K}[H_1,\ldots,H_r]}(\mathcal{I}, \preceq_H)$ of $\mathcal{J} = \tilde{\mathcal{J}} \cap \mathbb{K}[H_1, \ldots, H_r]$ with respect to some ordering $\preceq_H$ is said to be an invariant Gröbner basis *of $\mathcal{I}$ in the invariant ring $\mathbb{K}[h_1, \ldots, h_r]$.*

Proposition 3.46. *The map*

$$\begin{array}{rccc} P_{\mathbf{h}}: & \mathbb{V}(\mathcal{I}) & \twoheadrightarrow & \mathbb{V}(\langle G_{\mathbb{K}[H_1,\ldots,H_r]}(\mathcal{I}, \preceq_H)\rangle) \\ & \mathbf{a} = (a_1, \ldots, a_n) & \mapsto & (h_1(\mathbf{a}), \ldots, h_r(\mathbf{a})) \end{array}$$

is onto. Moreover, given a point $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{V}(\mathcal{I})$, the set $P_{\mathbf{h}}^{-1}(P_{\mathbf{h}}(\mathbf{a}))$ is exactly $\mathbf{G}.\mathbf{a}$.

The global usual strategy to solve systems of polynomials lying in $\mathbb{K}[X]^{\mathbf{G}}$ proceeds in two steps [100]. Fist, "preprocess" the group $\mathbf{G}$ with algorithm 3.47, and then compute a relative orbite variety with algorithm 3.48. Proposition 3.46 shows that the variety $\mathbb{V}(\mathcal{I})$ can be easily obtained with the relative orbite variety $\mathbb{V}(\mathcal{I})/\mathbf{G}$. In practice, it is possible to use the Gröbner basis $\mathcal{G}_0$ computed by Preprocessing algorithm 3.47: the points in the orbit of $\mathbf{a} = (a_1, \ldots, a_n)$ can be computed by substituting the coordinates of $\mathbf{h} = (h_1(\mathbf{a}), \ldots, h_r(\mathbf{a}))$ in the variables $H_1, \ldots, H_r$ in $\mathcal{G}_0$.

Algorithm 3.47: Preprocessing algorithm

Input : $\mathbf{G}$, a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$.
Output: A Gröbner basis.
Compute a set of fundamental invariants $h_1, \ldots, h_r$ of $\mathbf{G}$;
Compute $\mathcal{G}_0$, a Gröbner basis of the ideal

$$\langle H_1 - h_1(x_1, \ldots, x_n), \ldots, H_r - h_r(x_1, \ldots, x_n)\rangle$$

with respect to the block graded reverse lexicographic ordering such that $x_1 \succ \cdots \succ x_n \succ H_1 \succ \cdots \succ H_r$;
return $\mathcal{G}_0$

Algorithm 3.48: ComputeRelativeOrbiteVariety algorithm

Input : Polynomials $\mathsf{F} = f_1, \ldots, f_s$ invariant under $\mathbf{G}$, a finite subgroup of $\mathcal{GL}_n(\mathbb{K})$.
Output: The relative orbite variety $\mathbb{V}(\langle \mathsf{F}\rangle)/\mathbf{G}$
$\mathcal{G}_0 :=$ the Gröbner basis obtained by preprocessing of $\mathbf{G}$ with algorithm 3.47;
$\mathcal{G}_1 :=$ the Gröbner basis of $\mathcal{G}_0 \cup \mathsf{F}$ with respect to the block graded reverse lexicographic ordering such that $x_1 \succ \cdots \succ x_n \succ H_1 \succ \cdots \succ H_r$;
return $\mathcal{G}_1 \cap \mathbb{K}[H_1, \ldots, H_r]$

In practice, to compute the Gröbner basis $\mathcal{G}_0$ in algorithm 3.47, we would choose a weighted monomial, blockwise-lexicographical ordering in $\mathbb{K}[x_1, \ldots, x_n, H_1, \ldots, H_r]$, with weights 1 on x_i and $\deg(h_i)$ on H_i, in order to speed up the computations. However, we have seen in the

previous subsection that the size of a minimal set of fundamental invariants could be huge, so both detailed steps could be difficult.

In subsection 4.3, we propose an approach to overcome the difficulties explained above, in order to compute the relative orbit variety.

3.1.4 Representation Theory of finite groups

In this subsection, we briefly recall classical results in representation theory. We will see that the action of $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{K})$ of groups induces for each d a decomposition of $\mathbb{K}[X]_d$ into subvector spaces $\mathbb{K}[X]_{\chi,d}$ called the *isotypic components* of $\mathbb{K}[X]_d$, associated to the *characters* of *irreducible representations* of $\mathbf{G}$. In order to derive the complexity of variants of the Matrix-F_5 algorithm in the next part (sections 4.2 and 4.3), we will be mainly interested in estimates of the dimensions of $\mathbb{K}[X]_{\chi,d}$, when $\mathbf{G}$ is an abelian group or when χ is the trivial character (in this case $\mathbb{K}[X]_{\chi,d}$ is equal to $\mathbb{K}[X]_d^{\mathbf{G}}$). The theory of representations is the theoretical framework that encompasses both cases.

Except at the very end of the subsection, the field $\mathbb{K}$ is the field of complex numbers $\mathbb{C}$, and $\mathbf{G}$ denotes a finite group. The complex conjugate of an element u will be denoted $\overline{u}$.

Irreducible representations. We start by recalling the classical definitions of representations and irreducible representations.

Definition 3.49. *A linear representation of* $\mathbf{G}$ *is a pair* (V, ρ)*, where* $V \neq \{0\}$ *is a* $\mathbb{K}$*-vector space of finite dimension* $n \geq 1$ *and* ρ *is a group homomorphism* $\mathbf{G} \longrightarrow \mathcal{GL}(V)$*. The integer* n *is called the* degree *of the representation.*

With a slight abuse of language, we say that V is a representation of $\mathbf{G}$. In the previous definition, V is assumed to be finite dimensional. However, this is not a huge restriction, since irreducible representations of finite groups are finite dimensional, as we will see later.

Example 3.50. *As an example in this subsection, we will study the representations of the* abstract *group* $\mathfrak{S}_3$*, which is the smallest non-abelian group. The usual embedding of* $\mathfrak{S}_3$ *in* $\mathcal{GL}_3(\mathbb{C})$ *given by* $\sigma \mapsto M_\sigma$ *(see proposition 3.13) is a representation of degree 3, which will be denoted* ρ_3*. The* signature $\sigma \mapsto \epsilon(\sigma) \in \{\pm 1\}$ *or the trivial representation* $\sigma \mapsto 1$ *are two representations of degree 1.*

Proposition – Definition 3.51. *Let* $\rho : \mathbf{G} \longrightarrow \mathcal{GL}(V)$ *be a representation, and* W *be a subvector space of* V*. We say that* W *is invariant under* $\mathbf{G}$ *if* $\rho(g)(W) \subseteq W$ *for all* $g \in \mathbf{G}$*. Then, the map*

$$\begin{array}{rccc} \rho^W : & \mathbf{G} & \longrightarrow & \mathcal{GL}(W) \\ & g & \longmapsto & \rho(g)_{|W} \end{array}$$

gives a representation of $\mathbf{G}$ *in* $\mathcal{GL}(W)$*. We say that this is a sub-representation of* V*.*

Two representations (ρ, V) and (ρ, V') of $\mathbf{G}$ are said to be *isomorphic*, if there exists a linear isomorphism $\tau : V \to V'$ such that $\tau \circ \rho(g) = \rho'(g) \circ \tau$ for all g in $\mathbf{G}$. If $W \subsetneq V$ is a subrepresentation of $\mathbf{G}$, one can ask if we can find a vector space W' such that $W \oplus W' = V$ and W' is a also a subrepresentation of $\mathbf{G}$. The answer is yes, according to the following theorem.

Theorem 3.52 (Maschke)**.** *Let* $\rho : \mathbf{G} \longrightarrow \mathcal{GL}(V)$ *be a representation, and* W *be an* $\mathbf{G}$*-invariant subvector space of* V*. Then, there exists* $W' \subseteq V$ *such that* $W \oplus W' = V$ *and* W' *is also* $\mathbf{G}$*-invariant.*

Proof. See [91], theorem 1. □

In the previous theorem, we say that the representation V is the direct sum of the representations W and W', which leads to the following definition:

Definition 3.53. *If a representation V of $\mathbf{G}$ cannot be decomposed in the same way as in theorem 3.52, except with the trivial decomposition $V = V \cup \{0\}$, we say that the representation is* irreducible. *Otherwise, the representation is* reducible.

Example 3.54 (Continuation of example 3.50)**.** *The two representations of $\mathfrak{S}_3$ of degree 1 given in the previous example are obviously irreducible. The representation ρ_3 is not, since the vector subspace $W = \mathsf{Span}({}^t(1\ 1\ 1))$ is invariant under all matrices M_σ. The orthogonal complement $W^\perp$ of W is the (unique in this case) complement given by theorem 3.52. The representation $\sigma \mapsto M_\sigma|_{W^\perp}$ of degree 2 will be denoted ρ_2.*

Conversely, from any representations $V_1, \ldots, V_\ell$ (irreducible or not), it is possible to construct the *direct sum of the representations*, which is defined by $V_1 \oplus \cdots \oplus V_\ell$. The following theorem follows easily by induction from Maschke's theorem.

Theorem 3.55. *[91] Every representation is a direct sum of irreducible representations.*

The following lemma is of main interest in the study of irreducible representations.

Proposition 3.56 (Schur's lemma)**.** *Let (ρ, V) and (ρ', V') be two irreducible representations of $\mathbf{G}$. Let $f : V \to V'$ be a linear map such that $\rho'(g) \circ f = f \circ \rho(g)$ for all $g \in \mathbf{G}$. Then*

1. *If ρ and ρ' are not isomorphic, then $f = 0$.*
2. *If $(\rho, V) = (\rho', V')$, then f is a uniform scaling.*

Characters of a representation Although a group might have infinitely many representations, we will see that only a finite number of non-isomorphic irreducible representations remains. Moreover, they can be characterized by their *characters*[1].

Definition 3.57. *Let (ρ, V), be a representation of $\mathbf{G}$. Its character is defined by:*

$$\begin{array}{rccc} \chi_\rho : & \mathbf{G} & \longrightarrow & \mathbb{C} \\ & g & \longmapsto & \mathrm{trace}(\rho(g)) \end{array}$$

The character of a representation has the following properties:

Proposition 3.58. *[91] If χ is the character of a representation ρ of $\mathbf{G}$ of degree n, then:*
— *$\chi(1) = n$,*
— *for all $g \in \mathbf{G}$, $\chi(g^{-1}) = \overline{\chi(g)}$ (the complex conjugate of $\chi(g)$),*
— *for all $g, h \in \mathbf{G}$, $\chi(hgh^{-1}) = \chi(g)$.*

The third point shows that the character takes the same value on a conjugacy class of $\mathbf{G}$. It is straightforward to see that the character of a direct sum of representations is the sum of the characters. For any pair (ϕ, φ) of complex functions, the inner product of ϕ and φ is defined by:

$$(\phi|\varphi) = \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} \overline{\phi(g)} \varphi(g)$$

Using Schur's lemma (proposition 3.56), we successively prove the items of the following theorem.

1. This is actually why the word "character" is used!

Theorem 3.59. *[91] Let W be an irreducible representation of $\mathbf{G}$ with character χ.*
- *χ is of norm 1: $(\chi|\chi) = 1$,*
- *if W' is an other irreducible representation of $\mathbf{G}$, with character χ', non-isomorphic to W, then χ and χ' are* orthogonal*: $(\chi|\chi') = 0$,*
- *if V is a representation of $\mathbf{G}$, with character φ and $V = \oplus_{i=1}^{\ell} W_i$ is a decomposition of V into a direct sum of irreducible representations, the number of W_i isomorphic to W is given by $(\chi|\varphi)$.*

Example 3.60. *The characters of the representations $\mathbf{1}, \epsilon, \rho_2$ and ρ_3 of $\mathfrak{S}_3$ are reported in table 3.61. Since a character χ takes the same value on a conjugacy class, we only indicate the value on the three conjugacy class of $\mathfrak{S}_3$ given by $\{id\}$, the 3-cycles $\{(1\ 2\ 3), (1\ 3\ 2)\}$ and the transpositions $\{(1\ 2), (1\ 3), (2\ 3)\}$.*

representation ρ	id	3-cycle	transposition	norm $\sqrt{(\chi_\rho\|\chi_\rho)}$
$\mathbf{1}$	1	1	1	1
ϵ	1	1	-1	1
ρ_2	2	-1	0	1
ρ_3	3	0	1	$\sqrt{2}$

Table 3.61 – Characters of representations of $\mathfrak{S}_3$

It follows from the previous theorem, that in a decomposition of a representation V into a direct sum of irreducible representations, the number of representations isomorphic to a given irreducible representation does not depend on the chosen decomposition. It follows that two representations are isomorphic if and only if they have same character, and a representation V of character φ is irreducible if and only if $(\varphi|\varphi) = 1$.

With the previous theorem, we see in particular that the characters of irreducible representations of a groupe $\mathbf{G}$ form an orthogonal sequence for the inner product. There is a more precise result: let $\mathcal{C}(\mathbf{G})$ denotes the $\mathbb{C}$-vector space of *central functions* from $\mathbf{G}$ to $\mathbb{C}$, namely the functions $f : \mathbf{G} \to \mathbb{C}$ satisfying $f(ghg^{-1}) = f(g)$ for all g, h in $\mathbf{G}$. We have seen in proposition 3.58 that characters are central functions. More precisely:

Theorem 3.62. *The characters of irreducible representations of $\mathbf{G}$ form an orthogonal basis of the $\mathbb{C}$-vector space $\mathcal{C}(\mathbf{G})$.*

Corollary 3.63. *The number of irreducible representations (up to isomorphism) of a group $\mathbf{G}$ is equal to the number of conjugacy classes of $\mathbf{G}$.*

Example 3.64. *The group $\mathfrak{S}_3$ has 3 irreducible representations, $\mathbf{1}, \epsilon$ and ρ_2. The representation ρ_3 is the direct sum of $\mathbf{1}$ and ρ_2.*

It follows from the previous corollary that the number of irreducible representations of $\mathbf{G}$ is less than or equal to the cardinality of $\mathbf{G}$, and that equality holds if and only if $\mathbf{G}$ is abelian. We will that in this case, the set of irreducible representations forms a group isomorphic to $\mathbf{G}$.

Canonical decomposition of a representation. We now present a very important property for our purpose. We have seen that a representation can be decomposed into a direct sum of irreducible representations. However, this decomposition is neither unique, nor canonical. We will define a less precise decomposition, but this one will be unique. Let $W_1, \ldots, W_k$ be the irreducible representations of $\mathbf{G}$ (up to isomorphism). Let $V = \oplus_{i=1}^{\ell} U_i$ be a decomposition of a given representation V into irreducible representations. For each $i \in \{1, \ldots, k\}$, let V_i be the direct sum of each U_j isomorphic to W_i. Clearly, $V = V_1 \oplus \cdots \oplus V_k$. This is the canonical decomposition we have in mind:

Theorem 3.65. *[91] Let V be a representation of $\mathbf{G}$, we use the previous notations for the decompositions of V. Then*

- *the decomposition $V = V_1 \oplus \cdots \oplus V_k$ does not depend on the decomposition $V = \oplus_{i=1}^{\ell} U_i$ initially chosen.*
- *the projection p_i from V to V_i associated to this decomposition is*

$$p_i = \frac{n_i}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} \overline{\chi_i(g)} \rho_g$$

where n_i (resp. χ_i) is the degree (resp. the character) of the (unique up to isomorphism) irreducible representation, that appears in V_i.

The components V_i that appear in the previous theorem are called the *isotypic components* of V.

Example 3.66. *$\rho_3 = \mathbf{1} \oplus \rho_2$ is the decomposition of ρ_3 into isotypic components. We will see more complicated examples in the sequel.*

The case of abelian groups. We assume here that $\mathbf{G}$ is abelian, and we denote by $\widehat{\mathbf{G}}$ the set of characters of $\mathbf{G}$. We have already seen that $|\widehat{\mathbf{G}}| = |\mathbf{G}|$ since $|\widehat{\mathbf{G}}|$ is equal to the number of conjugacy classes of $\mathbf{G}$. We will see that $\widehat{\mathbf{G}}$ has a group structure, and that $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$ (but this isomorphism is not canonical).

Lemma 3.67. *$\widehat{\mathbf{G}}$ has a structure of group.*

Proof. Since all irreducible representations of $\mathbf{G}$ have degree 1, they are morphisms from $\mathbf{G}$ to $\mathbb{C}^*$, that can be identified with their characters. Given two such representations ρ_1 and ρ_2, the map

$$\begin{array}{ccc} \mathbf{G} & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & \rho_1(g)\rho_2(g) \end{array}$$

is also a linear representation of $\mathbf{G}$ of degree 1, and therefore a character, denoted by $\rho_1\rho_2$. We construct similarly the inverse ρ^{-1} of a character. It is obvious that with these definitions $\widehat{\mathbf{G}}$ is a group, with identity given by the trivial character $g \mapsto 1$, simply denoted by $\mathbf{1}$. □

The group $\widehat{\mathbf{G}}$ is often called the *dual* of $\mathbf{G}$. We are now interested in products of groups.

Lemma 3.68. *If $\mathbf{G}_1$ and $\mathbf{G}_2$ are two abelian groups, then $\widehat{\mathbf{G1} \times \mathbf{G_2}}$ is isomorphic to $\widehat{\mathbf{G}}_1 \times \widehat{\mathbf{G}}_2$.*

Proof. Let ρ_1 and ρ_2 be irreducible representations of G_1 and G_2. We define:

$$\begin{array}{rccc} \rho_1 \otimes \rho_2 : & (\mathbf{G}_1, \mathbf{G}_2) & \longrightarrow & \mathbb{C}^* \\ & (g_1, g_2) & \longmapsto & \rho_1(g_1)\rho_2(g_2) \end{array}$$

Straightforwardly, the map:

$$\begin{array}{rccc} \widehat{\mathbf{G}}_1 \times \widehat{\mathbf{G}}_2 : & \longrightarrow & \widehat{\mathbf{G_1} \times \mathbf{G_2}} \\ (\rho_1, \rho_2) & \longmapsto & \rho_1 \otimes \rho_2 \end{array}$$

is a group morphism. Moreover, this morphism is injective since $\rho_1 \otimes \rho_2 = \mathbf{1}$ if and only if $\rho_1 = \mathbf{1}$ and $\rho_2 = \mathbf{1}$. Since the two groups $\widehat{\mathbf{G1} \times \mathbf{G_2}}$ and $\widehat{\mathbf{G}}_1 \times \widehat{\mathbf{G}}_2$ have same cardinality, it is also an isomorphism. □

Notice that it is possible to generalize the construction $\rho_1 \otimes \rho_2$ for product of groups that are not necessary abelian. The result is the *tensor product* of two representations, see [91, theorem 10] for details and results. We now consider the case of a cyclic group.

Lemma 3.69. *Let $\ell \geq 1$. Then $\widehat{\mathbb{Z}/\ell\mathbb{Z}}$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$.*

Proof. Let ξ denotes a primitive ℓ-root of 1 in $\mathbb{C}$, for example $\xi = e^{2\imath\pi/\ell}$, where $\imath^2 = -1$. Then the morphisms

$$\begin{array}{rccc} \rho_j : & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & \mathbb{C}^* \\ & u & \longmapsto & \xi^{ju} \end{array}$$

form a set of ℓ distinct representations of $\mathbb{Z}/\ell\mathbb{Z}$. There are well defined since $\xi^v = \xi^{v'}$ if v and v' are two integers equal modulo ℓ. Hence, we have described all elements of $\widehat{\mathbb{Z}/\ell\mathbb{Z}}$, which is clearly generated by ρ_1. □

Putting all the previous lemmas together, we obtain the following result:

Theorem 3.70. *Let $\mathbf{G}$ be an abelian group, and $\widehat{\mathbf{G}}$ be the set of characters of $\mathbf{G}$. Then $\widehat{\mathbf{G}}$ has a group structure, and $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$.*

Proof. From lemma 3.67, $\widehat{\mathbf{G}}$ has a group structure. It follows from the structure of abelian groups that $\mathbf{G}$ is isomorphic to a product $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}$ (we can assume that $p_1 | \cdots | p_\ell$, but we do not require this assumption here). By lemma 3.69, $\widehat{\mathbb{Z}/p_i\mathbb{Z}}$ is isomorphic to $\mathbb{Z}/p_i\mathbb{Z}$ for each $i \in \{1, \ldots, \ell\}$. Applying $(\ell - 1)$ times lemma 3.68 ends the proof. □

We have said that this isomorphism is not *canonical*. Indeed, the isomorphism between a cyclic group and its characters in lemma 3.69 is not. Contrariwise, there exists a canonical isomorphism between an abelian group $\mathbf{G}$ and its *bidual* $\widehat{\widehat{\mathbf{G}}}$.

Grading on $\mathbb{C}[X]$ given by a representation. We now fix a finite matrix group $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{C})$, and see $\mathbb{C}[X]$ as a representation of $\mathbf{G}$. We will see that the action of $\mathbf{G}$ on $\mathbb{C}[X]$ induces a decomposition of $\mathbb{C}[X]$, indexed by the irreducible representations of $\mathbf{G}$. This decomposition will be a grading when $\mathbf{G}$ is abelian.

Notations 3.71. *In this paragraph, we denote by $\mathbf{X}(\mathbf{G})$ the set of irreducible characters of $\mathbf{G}$. When $\mathbf{G}$ is abelian, this set is denoted by $\widehat{\mathbf{G}}$, as previously.*

If f is a homogeneous polynomial of degree d and $A \in \mathbf{G}$, f^A is also homogeneous of degree d. Therefore, $\mathbf{G}$ acts also on $\mathbb{C}[X]_d$, and $\mathbb{C}[X]_d$ can be seen as a representation of $\mathbf{G}$. For $\chi \in \mathbf{X}(\mathbf{G})$, we denote by $\mathbb{C}[X]_{d,\chi}$ the isotypic component associated to χ. The vector space

$\mathbb{C}[X]_{d,\mathbf{1}}$ is no more than $\mathbb{C}[X]_d^{\mathbf{G}}$, the set of homogeneous polynomials of degree d invariant under $\mathbf{G}$. The usual decomposition of $\mathbb{C}[X]$ into graded components extends to:

$$\mathbb{C}[X] = \bigoplus_{d=0}^{+\infty} \bigoplus_{\chi \in \mathbf{X}(\mathbf{G})} \mathbb{C}[X]_{d,\chi} = \bigoplus_{\chi \in \mathbf{X}(\mathbf{G})} \bigoplus_{d=0}^{+\infty} \mathbb{C}[X]_{d,\chi} = \bigoplus_{\chi \in \mathbf{X}(\mathbf{G})} \mathbb{C}[X]_{\chi}$$

where $\mathbb{C}[X]_\chi = \bigoplus_{d=0}^{+\infty} \mathbb{C}[X]_{d,\chi}$ is the isotypic component of $\mathbb{C}[X]$ associated to χ.

Example 3.72. *The abstract group $\mathfrak{S}_3$ acts on $\mathbb{C}[X] = \mathbb{C}[x_1, x_2, x_3]$ through the representation ρ_3 associating to σ the matrix $M_\sigma = (m_{i,j})_{1 \leq i,j \leq 3}$ defined by $m_{i,j} = 1$ if $\sigma(j) = i$ and 0 otherwise. For example, $\mathbb{C}[X]_1, \mathbb{C}[X]_2$ and $\mathbb{C}[X]_3$ are representations of $\mathfrak{S}_3$ of degrees $3, 6$ and 10.*

One can ask is Molien's formula given in theorem 3.25 can be generalized to $\mathbb{C}[X]_\chi$. This is the case, since the following theorem holds:

Theorem 3.73 (Generalization of Molien's formula)**.** *[94] Let $\mathbf{G}$ be a finite subgroup of $\mathcal{GL}_n(\mathbb{C})$, and χ be an irreducible character of $\mathbf{G}$. Then*

$$HS_{\mathbb{C}[X]_\chi}(z) = \frac{n_\chi}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{\overline{\chi(A)}}{\det(I_n - zA)}$$

where n_χ is the degree of the irreducible character χ.

Proof. The proof can be found for example in [94]. The idea of the proof is very similar to the proof of Molien's formula given in theorem 3.25, but uses the projection on $\mathbb{C}[X]_\chi$ instead of the projection on $\mathbb{C}[X]_{\mathbf{1}} = \mathbb{C}[X]^{\mathbf{G}}$ given by the Reynolds Operator. This projection was explicitly given in theorem 3.65. Notice that in the case $\chi = \mathbf{1}$, this projection is exactly the Reynolds Operator. □

Example 3.74. *The Molien series associated to the characters of the irreducible representations $\mathbf{1}, \epsilon$ and ρ_2 of $\mathfrak{S}_3$ can be easily computed (we use the same name for an irreducible representation and its character). We also indicate the Hilbert series of the whole ring $\mathbb{C}[X]$ which is the sum of the Hilbert series associated to irreducible characters.*

$$\begin{aligned}
HS_{\mathbb{C}[X]_{\mathbf{1}}}(z) &= \tfrac{1}{6}\left[\tfrac{1}{(1-z)^3} + \tfrac{2}{1-z^3} + \tfrac{3}{(1-z)(1-z^2)}\right] = \tfrac{1}{1-z-z^2+z^4+z^5-z^6} \\
&= 1 + z + 2z^2 + 3z^3 + 4z^4 + 5z^5 + 7z^6 + 8z^7 + 10z^8 + 12z^9 + O(z^{10}) \\
HS_{\mathbb{C}[X]_{\epsilon}}(z) &= \tfrac{1}{6}\left[\tfrac{1}{(1-z)^3} + \tfrac{2}{1-z^3} - \tfrac{3}{(1-z)(1-z^2)}\right] = \tfrac{z^3}{1-z-z^2+z^4+z^5-z^6} \\
&= z^3 + z^4 + 2z^5 + 3z^6 + 4z^7 + 5z^8 + 7z^9 + O(z^{10}) \\
HS_{\mathbb{C}[X]_{\rho_2}}(z) &= \tfrac{2}{6}\left[\tfrac{2}{(1-z)^3} - \tfrac{2}{1-z^3}\right] = \tfrac{2z}{1-2z+z^2-z^3+2z^4-z^5} \\
&= 2z + 4z^2 + 6z^3 + 10z^4 + 14z^5 + 18z^6 + 24z^7 + 30z^8 + 36z^9 + O(z^{10}) \\
HS_{\mathbb{C}[X]}(z) &= \tfrac{1}{(1-z)^3} = HS_{\mathbb{C}[X]_{\mathbf{1}}}(z) + HS_{\mathbb{C}[X]_{\epsilon}}(z) + HS_{\mathbb{C}[X]_{\rho_2}}(z) \\
&= 1 + 3z + 6z^2 + 10z^3 + 15z^4 + 21z^5 + 28z^6 + 36z^7 + 45z^8 + 55z^9 + O(z^{10})
\end{aligned}$$

Projections onto isotypic components can be used to compute explicitely bases (as $\mathbb{C}$-vector space) of isotypic components, leading to a variant of algorithm 3.11 which was able to compute a basis of $\mathbb{K}[X]_d^{\mathbf{G}} = \mathbb{K}[X]_{d,\mathbf{1}}$ for a given d in the non-modular case, using the Reynolds Operator.

Example 3.75. *Table 3.76 gives bases of isotypic components of $\mathbb{C}[x_1, x_2, x_3]_d$ under the action of $\mathfrak{S}_3$ (given by the representation ρ_3). The second column describes the decomposition of $\mathbb{C}[x_1, x_2, x_3]_d$ as a direct sum of irreducible components (isomorphic to $\mathbf{1}$, ϵ or ρ_2). The last column describes a triangular basis of each isotypic component. Monomials are sorted by grevlex ordering with $x_1 \succ x_2 \succ x_3$ and two polynomials in the basis have distinct leading monomial. Since ρ_2 has degree 2, for each ρ_2 appearing in the decomposition of $\mathbb{C}[x_1, x_2, x_3]_d$ in irreducible representations, there are two polynomials in the basis of $\mathbb{C}[x_1, x_2, x_3]_{\rho_2,d}$. These dimensions are coherent with the first terms of the partial fraction expansions of the series $\mathsf{HS}_{\mathbb{C}[X]_\chi}$ given in the previous example.*

3.1.5 Estimates of Dimensions of Isotypic Components

In this subsection, we use previous generalization of Molien's formula to give estimates of the numbers $\dim(\mathbb{C}[X]_{\chi,d})$ where $\mathbf{G}$ is a finite matrix group and χ is an irreducible character of $\mathbf{G}$. These estimates will be useful in chapter 4, in order to study the complexity of variants of the F_5-algorithm 1.44. Since we will be interested in the ratios between $\dim(\mathbb{C}[X]_{\chi,d})$ and $\dim(\mathbb{C}[X]_d)$ and also between $\oplus_{d=0}^{D} \dim(\mathbb{C}[X]_{\chi,d})$ and $\oplus_{d=0}^{D} \dim(\mathbb{C}[X]_d)$, the following definition will be useful:

Definition 3.77. *We define the density of $\mathbb{C}[X]_{\chi,d}$ in $\mathbb{C}[X]_d$ and the density of $\mathbb{C}[X]_\chi$ in $\mathbb{C}[X]$ by*

$$\Delta(\mathbb{C}[X]_{\chi,d}) = \frac{\dim(\mathbb{C}[X]_{\chi,d})}{\dim(\mathbb{C}[X]_d)} \qquad \text{and} \qquad \Delta(\mathbb{C}[X]_\chi) = \lim_{D \to +\infty} \frac{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_{\chi,d})}{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_d)}$$

Notice that it is yet unclear that the limit is well-defined. This will be proved below.

We are particularly interested in the cases where $\Delta(\mathbb{C}[X]_{\chi,d})$ has a limit when d grows to infinity. The following theorem is the most important of this subsection.

Theorem 3.78. *Assume that the matrix group $\mathbf{G}$ contains no uniform scalings except I_n. Then the density $\Delta(\mathbb{C}[X]_{\chi,d})$ has the limit $n_\chi^2/|\mathbf{G}|$ when d grows up to infinity, where n_χ is the degree of χ.*

Proof. The idea is to use the generalized Molien's formula given in theorem 3.73. The Hilbert series of $\mathbb{C}[X]_\chi$ can be written:

$$\mathsf{HS}_{\mathbb{C}[X]_\chi}(z) = \frac{n_\chi}{|\mathbf{G}|} \sum_{A \in \mathbf{G}} \frac{\overline{\chi(A)}}{\det(I_n - zA)}$$

Since we assumed that there are no uniform scalings in $\mathbf{G}$ except I_n, the previous meromorphic series has 1 as unique pole of order n, the other poles u are also n-roots of 1, since they satisfies $u^{|\mathbf{G}|} - 1 = 0$, but have smaller orders. We are interested in an asymptotic estimation of the coefficient in z^d in $\mathsf{HS}_{\mathbb{C}[X]_\chi}$. Following the ideas of [46, Theorem 4.9, p.256], the fraction expansion of $\mathsf{HS}_{\mathbb{C}[X]_\chi}$ can be written as

$$\mathsf{HS}_{\mathbb{C}[X]_\chi}(z) = \frac{n_\chi \overline{\chi(I_n)}}{|\mathbf{G}|(1-z)^n} + \sum_{p \in P} \sum_{r=0}^{n-1} \frac{c_{u,r}}{(u-z)^r}$$

d	Decomposition of $\mathbb{C}[X]_d$	Bases of $\mathbb{C}[X]_{d,\chi}$	
0	$\mathbf{1}$	$\mathbf{1}$	1
1	$\mathbf{1} \oplus \rho_2$	$\mathbf{1}$	$x_1 + x_2 + x_3$
		ρ_2	$x_1 - x_3$ $x_2 - x_3$
2	$2 \times \mathbf{1} \oplus 2 \times \rho_2$	$\mathbf{1}$	$x_1^2 + x_2^2 + x_3^2$ $x_1x_2 + x_1x_3 + x_2x_3$
		ρ_2	$x_1^2 - x_3^2$ $x_1x_2 - x_2x_3$ $x_2^2 - x_3^2$ $x_1x_3 - x_2x_3$
3	$3 \times \mathbf{1} \oplus \epsilon \oplus 3 \times \rho_2$	$\mathbf{1}$	$x_1^3 + x_2^3 + x_3^3$ $x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2$ $x_1x_2x_3$
		ϵ	$x_1^2x_2 - x_1x_2^2 - x_1^2x_3 + x_2^2x_3 + x_1x_3^2 - x_2x_3^2$
		ρ_2	$x_1^3 - x_3^3$ $x_1^2x_2 - x_1x_3^2$ $x_1x_2^2 - x_2x_3^2$ $x_2^3 - x_3^3$ $x_1^2x_3 - x_2x_3^2$ $x_2^2x_3 - x_1x_3^2$
4	$4 \times \mathbf{1} \oplus \epsilon \oplus 5 \times \rho_2$	$\mathbf{1}$	$x_1^4 + x_2^4 + x_3^4$ $x_1^3x_2 + x_1x_2^3 + x_1^3x_3 + x_2^3x_3 + x_1x_3^3 + x_2x_3^3$ $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$ $x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2$
		ϵ	$x_1^3x_2 - x_1x_2^3 - x_1^3x_3 + x_2^3x_3 + x_1x_3^3 - x_2x_3^3$
		ρ_2	$x_1^4 - x_3^4$ $x_1^3x_2 - x_1x_3^3$ $x_1^2x_2^2 - x_2^2x_3^2$ $x_1x_2^3 - x_2x_3^3$ $x_2^4 - x_3^4$ $x_1^3x_3 - x_2x_3^3$ $x_1^2x_2x_3 - x_1x_2x_3^2$ $x_1x_2^2x_3 - x_1x_2x_3^2$ $x_2^3x_3 - x_1x_3^3$ $x_1^2x_3^2 - x_2^2x_3^2$

Table 3.76 – Bases of isotypic components of $\mathbb{C}[x_1, x_2, x_3]_d$ under the action of $\mathfrak{S}_3$ for $d \leq 4$

where P is the set of poles of $\mathsf{HS}_{\mathbb{C}[X]_\chi}$ and $c_{u,r}, \gamma \in \mathbb{C}$. Now let u be a complex of modulus 1 and $r \geq 1$. Then

$$[z^d]\frac{1}{(u-z)^r} = [z^d]\frac{\overline{u}^r}{(1-z\overline{u})^r} = \overline{u}^{r+d}\binom{d+r-1}{r-1} \underset{d\to+\infty}{=} \frac{\overline{u}^{r+d}d^{r-1}}{(r-1)!} + o(d^{r-1})$$

Furthemore, $\chi(I_n) = n_\chi$, since the representation of I_n in the irreducible representation associated to χ is the identity matrix of size $n_\chi \times n_\chi$ (see proposition 3.58). Hence, the term of main order of $[z^d]\,\mathsf{HS}_{\mathbb{C}[X]_\chi}(z)$ is given by

$$[z^d]\frac{n_\chi^2}{|\mathbf{G}|(1-z)^n} = \frac{n_\chi^2\, d^{n-1}}{|\mathbf{G}|(n-1)!} + o(d^{n-1}).$$

Since the Hilbert series of the whole ring $\mathbb{C}[X]$ is simply $\mathsf{HS}_{\mathbb{C}[X]}(z) = 1/(1-z)^n$, it follows that

$$\Delta(\mathbb{C}[X]_{\chi,d}) = \frac{\dim(\mathbb{C}[X]_{\chi,d})}{\dim(\mathbb{C}[X]_d)} = \frac{[z^d]\,\mathsf{HS}_{\mathbb{C}[X]_{\chi,d}}(z)}{[z^d]\,\mathsf{HS}_{\mathbb{C}[X]}(z)} \underset{d\to+\infty}{\longrightarrow} \frac{n_\chi^2}{|\mathbf{G}|}$$

□

Example 3.79. *The representations* $\mathbf{1}$ *and* ϵ *of* $\mathfrak{S}_3$ *have degree 1, and* ρ_2 *degree 2. Since there are no uniform scalings in the representation of* $\mathfrak{S}_3$ *(given by* ρ_3*) acting on* $\mathbb{C}[X]$*, theorem 3.78 holds. Figure 3.80 presents the 50 first terms of* $\mathsf{HS}_{\mathbb{C}[X]_\chi}$ *for* $\chi \in \{\mathbf{1}, \epsilon, \rho_2\}$*. We see that*

$$\lim_{d\to+\infty}\frac{\dim_{\mathbb{C}}(\mathbb{C}[X]_{\mathbf{1},d})}{\dim_{\mathbb{C}}(\mathbb{C}[X]_d)} = \lim_{d\to+\infty}\frac{\dim_{\mathbb{C}}(\mathbb{C}[X]_{\epsilon,d})}{\dim_{\mathbb{C}}(\mathbb{C}[X]_d)} = \frac{1}{6} \simeq 0.167 \qquad \textit{and}$$

$$\lim_{d\to+\infty}\frac{\dim_{\mathbb{C}}(\mathbb{C}[X]_{\rho_2,d})}{\dim_{\mathbb{C}}(\mathbb{C}[X]_d)} = \frac{2^2}{6} \simeq 0.667,$$

according to theorem 3.78.

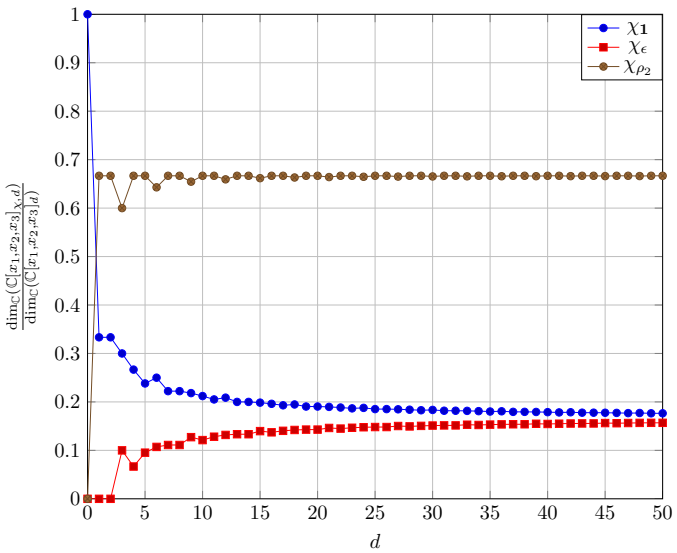


Figure 3.80 – Ratios between $\dim_{\mathbb{C}}(\mathbb{C}[x_1,x_2,x_3]_{\chi,d})$ and $\dim_{\mathbb{C}}(\mathbb{C}[x_1,x_2,x_3]_d)$ for $\mathfrak{S}_3$

Remark 3.81. *The previous theorem does not hold if uniform scalings other than I_n belong to $\mathbf{G}$: for example, if $n = 2$ and $\mathbf{G}$ is the group of order 4 generated by the diagonal matrices having diagonal coefficients in $\{\pm 1\}$, $\mathbb{C}[X]_{\mathbf{1}} = \mathbb{C}[x^2, y^2]$, and $\mathsf{HS}_{\mathbb{C}[X]_{\mathbf{1}}}(z) = (1-z^2)^{-2}$ has all its odd coefficients equal to zero. But for even d, $\dim(\mathbb{C}[X]_{\mathbf{1},d})$ is roughly half of $\dim(\mathbb{C}[X]_d)$, so in average we recover the factor $1/4 = 1/|\mathbf{G}|$. This idea leads to proposition 3.83.*

It is very interesting to see that the previous theorem allows us to recover a famous result of representation theory.

Remark 3.82. *Since $\mathbb{C}[X]_d = \oplus_{\chi \in \mathbf{X}(\mathbf{G})} \mathbb{C}[X]_{\chi,d}$, we can derive from the previous theorem that $\sum_{\chi \in \mathbf{X}(\mathbf{G})} n_\chi^2 = |\mathbf{G}|$, at least when there are no uniform scalings in $\mathbf{G}$ other than I_n. This result can be extended without hypothesis on $\mathbf{G}$, since it depends only on the structure of the underlying abstract group.*

We now prove that the density of $\mathbb{C}[X]_\chi$ in definition 3.77 is well-defined, and give its value.

Proposition 3.83. *With n_χ the degree of the character χ, the following relation holds.*

$$\Delta(\mathbb{C}[X]_\chi) = \lim_{D \to +\infty} \frac{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_{\chi,d})}{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_d)} = \frac{n_\chi^2}{|\mathbf{G}|}$$

Proof. From $\mathbf{G}$, we construct the group $\widetilde{\mathbf{G}} \subset \mathcal{GL}_{n+1}(\mathbb{C})$, the elements of which are the matrices

$$\widetilde{A} = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

for all $A \in \mathbf{G}$. Due to the coefficient 1 in the bottom right corner of each matrix of $\widetilde{\mathbf{G}}$, there are no uniform scalings in $\widetilde{\mathbf{G}}$ except I_{n+1}. Moreover, $\widetilde{\mathbf{G}}$ acts on the polynomial ring $\mathbb{C}[X, h] = \mathbb{C}[x_1, \ldots, x_n, h]$, where h is a new indeterminate. By applying theorem 3.78, we obtain that $\Delta(\mathbb{C}[X, h]_{\chi,D})$ has the limit $n_\chi^2/|\widetilde{\mathbf{G}}|$ when D grows up to infinity. For $m = X^\alpha = \prod x_i^{\alpha_i}$ a monomial in $x_1, \ldots, x_n$ and $\beta \geq 0$, it follows by definition of $\widetilde{\mathbf{G}}$ that $(mh^\beta)^{\widetilde{A}} = m^A h^\beta$ for all $A \in \mathbf{G}$. Thus, the actions of $\mathbf{G}$ and $\widetilde{\mathbf{G}}$ on $\mathbb{C}[X]$ and $\mathbb{C}[X, h]$ are compatible with the isomorphism between $\mathbf{G}$ and $\widetilde{\mathbf{G}}$. Hence, $\mathbb{C}[X, h]_{\chi,D} \simeq \oplus_{d=0}^{D} \mathbb{C}[X]_{\chi,d}$. Therefore,

$$\frac{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_{\chi,d})}{\sum_{d=0}^{D} \dim(\mathbb{C}[X]_d)} = \frac{\dim(\mathbb{C}[X, h]_{\chi,D})}{\dim(\mathbb{C}[X, h]_D)} = \Delta(\mathbb{C}[X, h]_{\chi,D}) \underset{D \to \infty}{\longrightarrow} \frac{n_\chi^2}{|\mathbf{G}|}$$

and the proposition is proved.

□

We now give applications to particular cases, that will be used later to explain the complexity of variants of the Matrix-F_5 algorithm 1.44.

Corollary 3.84. *Theorem 3.78 and proposition 3.83 apply in particular in the case where $\mathbf{G}$ is abelian. In this case, $\mathbf{X}(\mathbf{G}) = \widehat{\mathbf{G}} \simeq \mathbf{G}$ and all n_χ are equal to 1. Therefore, when no uniform scalings other than I_n lie in $\mathbf{G}$, the dimensions of $\mathbb{C}[X]_{\chi,d}$ tend to be equally distributed when d grows to infinity. This is also the case without hypothesis on $\mathbf{G}$ for the dimensions of $\oplus_{d=0}^{D} \mathbb{C}[X]_{\chi,d}$. In the same way, for any group $\mathbf{G}$, the trivial character $\mathbf{1}$ has degree 1. Therefore, the density $\Delta(\mathbb{C}[X]_{\mathbf{1},d}) = \Delta(\mathbb{C}[X]_d^{\mathbf{G}})$ has the limit $1/|\mathbf{G}|$ when d grows to infinity if there are no uniform scalings in $\mathbf{G}$, and $\Delta(\mathbb{C}[X]_{\mathbf{1}}) = \Delta(\mathbb{C}[X]^{\mathbf{G}}) = 1/|\mathbf{G}|$ without hypothesis on $\mathbf{G}$.*

All the results presented in this subsection have been stated with $\mathbb{K} = \mathbb{C}$. However, representations and characters can be defined on any field. In section 4.2, we will need the results on the estimates of dimensions of the isotypic components on any field, assuming that $\mathbf{G}$ is a group of *diagonal matrices*. For these groups, the linear maps of projections on an isotypic component (see theorem 3.65) have their eigenvectors given by monomials (this will be proved in section 4.2). The associated eigenvalues are either roots of 1 or zero. Therefore, considering a lifting of the group into $\mathcal{GL}_n(\mathbb{C})$ allows us to extend the generalization of Molien's formula 3.73 and the estimates of dimensions of isotypic components 3.78 and proposition 3.83 to the case of diagonal matrix groups.

For other groups, it is not easy to extend the results of linear representations on other fields than $\mathbb{C}$, see [91].

3.2 Monomial Algebras

In this section, we are interested in describing some properties of subalgebras generated by monomials, which is the algebraic context of chapter 5. We will allow here subalgebras $\mathcal{A}$ of the algebra of Laurent polynomials $\mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ instead of $\mathbb{K}[x_1, \ldots, x_n]$, but with restrictive conditions: the monomials lying in the subalgebra form a *semigroup* with no non-zero invertible elements. Therefore, the algebra is closer to $\mathbb{K}[x_1, \ldots, x_n]$ than to $\mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Affine semigroups. The basic underlying algebraic objects corresponding to monomials in classical polynomial rings are *affine semigroups*. We always consider them embedded in $\mathbb{Z}^n$.

We refer the reader to [78, 26, 49, 13] for a more detailed presentation of this background material. First, we describe the main notations that will be used throughout chapter 5.

Definition 3.85. *An* affine semigroup *S is a finitely-generated additive subsemigroup of $\mathbb{Z}^n$ for some $n \in \mathbb{N}$ containing $\mathbf{0} \in \mathbb{Z}^n$ and no nonzero invertible element: for all $\mathbf{s}, \mathbf{s}' \in S \setminus \{\mathbf{0}\}, \mathbf{s} + \mathbf{s}' \neq \mathbf{0}$.*

Depending on the articles on this topic, the condition "S contains no invertible element" is not always included in the definition of an affine semigroup. However, this is a necessary condition for the algorithms that we will see in chapter 5.

Definition 3.86. *Let $\mathrm{gp}(S)$ denote the smallest subgroup of $\mathbb{Z}^n$ containing S. Then S is called* normal *if $S = \{\mathbf{s} \in \mathrm{gp}(S) \mid \exists c \in \mathbb{N}, c \cdot \mathbf{s} \in S\}$.*

We always assume implicitly that $\mathrm{gp}(S) \subset \mathbb{Z}^n$ is a full rank lattice (this does not lose any generality since this case can be reached by embedding S in a lower dimensional $\mathbb{Z}^{n'}$).

An important feature of normal affine semigroups is that they can be represented by the intersection of $\mathbb{Z}^n$ with a pointed rational polyhedral cone (also called *strongly convex rational polyhedral cone* [81, Sec 1.1]).

Definition 3.87. *A* cone *$\mathscr{C} \subset \mathbb{R}^n$ is a convex subset of $\mathbb{R}^n$ stable by multiplication by $\mathbb{R}_+$, the set of non-negative real numbers. The* dimension $\dim(\mathscr{C})$ *of a cone $\mathscr{C}$ is the dimension of the linear subspace spanned by $\mathscr{C}$. A cone is called* pointed *if it does not contain any line. A pointed cone of dimension* 1 *is called a ray. A ray is called* rational *if it contains a point in $\mathbb{Z}^n$. A* rational polyhedral cone *is the convex hull of a finite number of rational rays. Pointed rational polyhedral cones will be abbreviated* PRPC.

We shall use PRPCs in Section 5.2 to define admissible monomial orderings in semigroup algebras (see definition 3.93.)

Proposition – Definition 3.88. *Any affine semigroup has a unique minimal set of generators, called the* Hilbert basis *of S and denoted by* $\mathrm{Hilb}(S)$.

Proof. [78, Prop. 7.15] Since S can be represented by the intersection of $\mathbb{Z}^n$ with a PRPC $\mathscr{C}$, we assume that $S = \mathscr{C} \cap \mathbb{Z}^n$. Then, S can be partially ordered by $\mathbf{a} \leq \mathbf{b}$ if $\mathbf{b} - \mathbf{a} \in S$, and we denote by $\mathrm{Hilb}(S)$ a subset of generators of S, that are minimal in $S\backslash\{\mathbf{0}\}$ with respect to this partial order. Since $\mathscr{C}$ is pointed, there exists $\mathbf{w} \in \mathbb{Z}^n$ such that $\mathbf{w}.\mathbf{a} > 0$ for all $\mathbf{a} \in S\backslash\{\mathbf{0}\}$. By induction on the quantity $\mathbf{w}.\mathbf{a}$, we show that every $\mathbf{a} \in S$ is a $\mathbb{N}$-linear combination of elements in $\mathrm{Hilb}(S)$. But these elements cannot be written in a nontrivial way as $\mathbb{N}$-linear combination of elements of S, therefore $\mathrm{Hilb}(S)$ is a unique minimal set of generators. □

Also, the term "Hilbert basis" is sometimes reserved for affine semigroups of the form $\mathscr{C} \cap \mathbb{Z}^n$ where $\mathscr{C}$ is a rational cone (see *e.g.* the discussion after [78, Prop. 7.15]). We now recall the definition of *simplicial affine semigroups*, which will play a crucial role in chapter 5, in order to design a variant of the FGLM algorithm 1.52 for solving systems of polynomials in monomial algebras.

Definition 3.89. *A PRPC $\mathscr{C}$ in $\mathbb{R}^n$ is said to be simplicial if it is the convex hull of n linearly independent rays.*

Remark 3.90. *If $n = 2$, all PRPCs are simplicial. This is not the case if $n \geq 3$: for instance the convex hull of the rays generated by $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,-1)$ is a PRPC which is not simplicial.*

Definition 3.91. *An affine semigroup $S \subset \mathbb{Z}^n$ is called simplicial if the convex hull of $\mathbb{R}_+ S$ is a simplicial PRPC.*

Example 3.92. *$\mathbb{N}^n \subset \mathbb{Z}^n$ is simplicial, while the affine semigroup generated by $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,-1)$ in $\mathbb{Z}^3$ is not.*

Semigroup algebras. To a semi-group, we can associate a monomial algebra, which is the subject of the following definition.

Definition 3.93. *Let $\mathbb{K}$ be a field, and S be a semi-group. We denote by $\mathbb{K}[S]$ the associated* semigroup algebra *of finite formal sums $\sum_{\mathbf{s}\in S} a_{\mathbf{s}} X^{\mathbf{s}}$ where $a_{\mathbf{s}} \in \mathbb{K}$. An element $X^{\mathbf{s}} \in \mathbb{K}[S]$ is called a* monomial.

Since S is contained in $\mathbb{Z}^n$, the semi-group algebra $\mathbb{K}[S]$ is a subalgebra of the algebra of *Laurent polynomials* $\mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Note that $\mathbb{K}[\mathbb{N}^n]$ is the classical polynomial ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. Semigroup algebras are integral domains [78, Thm. 7.4] of Krull dimension n and play an important role in toric geometry: they are precisely the coordinate rings of *affine toric varieties*. The normality of the semigroup S is an important property, which has the following consequence.

Theorem 3.94 (Hochster)**.** *If S is normal, then $\mathbb{K}[S]$ is a Cohen-Macaulay algebra.*

Proof. The proof is long and technical, see [56]. □

We now contruct from a finite set of points in $\mathbb{Z}^n$ two semigroups and the associated monomial algebras.

Notations 3.95. *From now, we use the letter $\mathcal{M}$ to denote a finite subset of $\mathbb{Z}^n$ such that $\mathbf{0} \in \mathcal{M}$ and such that the semigroup $S_{\mathcal{M}}$ generated by $\mathcal{M}$ contains no nonzero invertible element. To such a set $\mathcal{M}$, we associate another semi-group than $S_{\mathcal{M}}$, namely the affine semigroup generated by $\{(\alpha, 1) \mid \alpha \in \mathcal{M}\} \subset \mathbb{Z}^{n+1}$, denoted by $S^{(h)}_{\mathcal{M}}$. The semigroup algebra $\mathbb{K}[S^{(h)}_{\mathcal{M}}]$ is $\mathbb{N}$-graded : the degree of a monomial $X^{(s_1,\dots,s_n,d)}$ is $d \in \mathbb{N}$. The vector space of homogeneous elements of degree $d \in \mathbb{N}$ in $\mathbb{K}[S^{(h)}_{\mathcal{M}}]$, namely the linear combinations of monomials of degree d, is denoted by $\mathbb{K}[S^{(h)}_{\mathcal{M}}]_d$.*

With this grading, $\mathbb{K}[S^{(h)}_{\mathcal{M}}]$ is generated by its elements of degree 1: such a graded algebra is said to be *homogeneous*.

Another important family of objects are *projective toric varieties*. Their homogeneous coordinate rings are associated to a lattice polytope, which we shall assume to be normal in order to ensure that the coordinate ring is Cohen-Macaulay. As in the classical case, homogeneity is a central concept to analyze the complexity of Gröbner bases algorithms. All lattice polytopes will be assumed full dimensional.

Definition 3.96. *A* lattice polytope *$\mathscr{P} \subset \mathbb{R}^n$ is the convex hull of a finite number of points in $\mathbb{Z}^n$. Its* normalized volume, i.e. *$n!$ times its Euclidean volume, is denoted by* $\mathrm{vol}(\mathscr{P}) \in \mathbb{N}$.

Example 3.97.
— *We let $\Delta_n \subset \mathbb{R}^n$ denote the* standard simplex, *namely the convex hull of $\mathbf{0}$ and of the points $\mathbf{e}_i \in \mathbb{R}^n$ whose entries are zero except for the i-th coefficient which is equal to 1. The Euclidian volume of Δ_n is $\frac{1}{n!}$, therefore its normalized volume is 1.*
— *Let $\mathscr{P}$ be the convex hull of the three points $(0,0),(2,1)$ and $(1,2)$ in $\mathbb{R}^2$. This triangle has Euclidian volume (area) $\frac{3}{2}$ and therefore its normalized volume is 3.*

To a lattice polytope $\mathscr{P} \subset \mathbb{R}^n$ is associated the affine semigroup $S^{(h)}_{\mathscr{P}\cap\mathbb{Z}^n} \subset \mathbb{Z}^{n+1}$ generated by $\{(\alpha, 1) \mid \alpha \in \mathscr{P} \cap \mathbb{Z}^n\}$. The polytope $\mathscr{P}$ is called *normal* if $S^{(h)}_{\mathscr{P}\cap\mathbb{Z}^n}$ is a normal semigroup. The associated semigroup algebra is called a *polytopal algebra* and will be abbreviated $\mathbb{K}[\mathscr{P}]$.

If $\mathscr{P} \subset \mathbb{R}^n$ is a lattice polytope containing $\mathbf{0}$ as a vertex, then $\mathbb{K}[\mathscr{P}] = \mathbb{K}[S^{(h)}_{\mathscr{P}\cap\mathbb{Z}^n}]$ (notations 3.95).

Also, note that if $\mathscr{P}'$ is a translation of $\mathscr{P}$, then the homogeneous algebras $\mathbb{K}[\mathscr{P}]$ and $\mathbb{K}[\mathscr{P}']$ are isomorphic. Consequently, we shall assume without loss of generality in the sequel that one of the vertices of $\mathscr{P}$ is the origin, so that $\mathcal{M} = \mathscr{P} \cap \mathbb{Z}^n$ verifies the assumptions of notations 3.93. We also introduce a few more notations and definitions for lattice polytopes:

Notations 3.98. *Let $\mathscr{P}$, $\mathscr{P}_1$ and $\mathscr{P}_2$ be three lattice polytopes of $\mathbb{R}^n$.*
— *The number of lattice points in $\mathscr{P}$ (*i.e. *the cardinality of $\mathscr{P} \cap \mathbb{Z}^n$) is denoted by $\#\mathscr{P}$.*
— *The* Minkowski sum *of the lattice polytopes $\mathscr{P}_1, \mathscr{P}_2 \subset \mathbb{R}^n$ is the lattice polytope $\{p_1 + p_2 \mid p_1 \in \mathscr{P}_1, p_2 \in \mathscr{P}_2\}$.*
— *For all $\ell \in \mathbb{N}$ we write $\ell \cdot \mathscr{P}$ for the Minkowski sum $\mathscr{P} + \cdots + \mathscr{P}$ with ℓ summands.*
— *For $\mathscr{P}_1 \subset \mathbb{R}^i$,$\mathscr{P}_2 \subset \mathbb{R}^j$ we write $\mathscr{P}_1 \times \mathscr{P}_2 \subset \mathbb{R}^{i+j}$ for the lattice polytope whose points are $\{(p_1, p_2) \mid p_1 \in \mathscr{P}_1, p_2 \in \mathscr{P}_2\}$.*

Example 3.99.
— *With this definition, $\#\Delta_n = n+1$. For the polytope $\mathscr{P}$ defined in the previous example, namely the convex hull of $(0,0),(1,2)$ and $(2,1)$ we have $\#\mathscr{P} = 4$ since $\mathscr{P}$ contains the point $(1,1)$.*
— *The Minkowski sums $2\mathscr{P}$ and $3\mathscr{P}$ are drawn on figure 3.100.*
— *The standard simplex Δ_n can be seen as the product of n copies of Δ_1: $\Delta_1 \times \cdots \times \Delta_1$.*

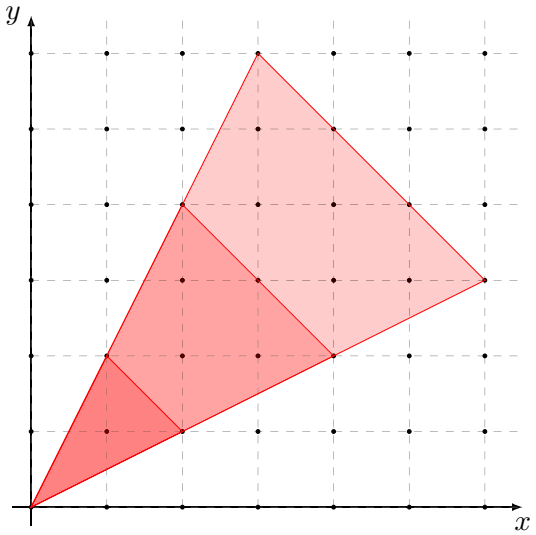


Figure 3.100 – $\mathscr{P}$, $2\mathscr{P}$ and $3\mathscr{P}$.

Ehrhart polynomial. Next, we recall several useful classical properties of polytopal algebras. The main object is the *Ehrhart polynomial* associated to a lattice polytope, and the associated power series.

Definition 3.101. *Let $\mathscr{P} \subset \mathbb{R}^n$ be a lattice polytope. For $d \in \mathbb{N}$, we let $\mathsf{HP}_{\mathscr{P}} \in \mathbb{Q}[d]$ denote the* Ehrhart polynomial *of $\mathscr{P}$,* i.e. *$\mathsf{HP}_{\mathscr{P}}(d) = \#(d \cdot \mathscr{P})$. Also, let $\mathsf{HS}_{\mathscr{P}}(z) \in \mathbb{Z}[[z]]$ denote the generating series*

$$\mathsf{HS}_{\mathscr{P}}(z) = \sum_{d \in \mathbb{N}} \mathsf{HP}_{\mathscr{P}}(d) z^d.$$

Example 3.102. *Consider the standard simplex Δ_n defined in example 3.97. Then*

$$\mathsf{HP}_{\Delta_n}(d) = \binom{n+d}{d} \qquad \textit{and} \qquad \mathsf{HS}_{\Delta_n} = \frac{1}{(1-z)^{n+1}}$$

Notice that the generating series $\mathsf{HS}_{\mathscr{P}}$ is equal to the generating series $\mathsf{HS}_{\mathbb{K}[\mathscr{P}]}(z) = \sum_{d=0}^{+\infty} \dim(\mathbb{K}[\mathscr{P}]_d) z^d$ (notations 3.95). The shape of this series is well known, since the following proposition holds.

Proposition 3.103. *Let $\mathscr{P}$ be a lattice polytope in $\mathbb{R}^n$. There exists a polynomial $Q \in \mathbb{Z}[z]$, of degree less than or equal to n, with non-negative coefficients such that*

$$\mathsf{HS}_{\mathscr{P}}(z) = \frac{Q(z)}{(1-z)^{n+1}}$$

Proof. The fact that the map $\mathsf{HP}_{\mathscr{P}} : d \mapsto \#(d \cdot \mathscr{P})$ is a polynomial of degree n is a classical result by Ehrhart [29], which dates back to 1962. It follows that the series $\mathsf{HS}_{\mathscr{P}}(z)$ has the desired shape $Q(z)/(1-z)^{n+1}$, with Q a polynomial of degree less than or equal to n. The fact that Q has non-negative integer coefficients is Stanley's non-negativity theorem [95, Thm. 2.1]. □

Example 3.104. *For the polytope $\mathscr{P} \subset \mathbb{R}^2$ defined in example 3.97, it is easy to see that $\#0 \cdot \mathscr{P} = 1$, $\#1 \cdot \mathscr{P} = 4$ and $\#2 \cdot \mathscr{P} = 10$. Therefore $\mathsf{HS}_{\mathscr{P}}(z) = \frac{1+z+z^2}{(1-z)^3}$. We can derive explictely a formula for the Hilbert polynomial: $\mathsf{HP}_{\mathscr{P}}(d) = \frac{3d^2+3d+2}{2}$. In particular, $\mathsf{HP}_{\mathscr{P}}(3) = 19$, according to figure 3.100.*

Integer interior points. We have seen how to describe the number of integer points lying in $d \cdot \mathscr{P}$, with $\mathscr{P}$ a lattice polytope and $d \geq 0$. An other interesting combinatorial number is related to *interior points*.

Definition 3.105. *Let $\mathscr{P}$ be a lattice polytope in $\mathbb{R}^n$. An integer interior point of $\mathscr{P}$ is a lattice point of $\mathbb{Z}^n$ lying in the interior of $\mathscr{P}$, defined by the classical topology of $\mathbb{R}^n$.*

Example 3.106. *For $d \in \{0, \ldots, n\}$, $d \cdot \Delta_n$ has no integer interior points, but $(n+1)\Delta_n$ has $(1, \ldots, 1)$ as unique integer interior point.*

We denote by $\mathsf{HP}_{\mathscr{P}^\circ}(d)$ the number of integer interior points in $d \cdot \mathscr{P}$. Since $\mathsf{HP}_{\mathscr{P}} : d \mapsto \#(d \cdot \mathscr{P})$ is a polynomial function, it can be extended to negative integers. MacDonald reciprocity law [76] is a beautiful formula, which relates $\mathsf{HP}_{\mathscr{P}}$ and $\mathsf{HP}_{\mathscr{P}^\circ}$.

Proposition 3.107 (Ehrhart-MacDonald reciprocity)**.** *[76] Let $\mathscr{P}$ be a lattice polytope in $\mathbb{R}^n$. Then, for all $d > 0$,*

$$\mathsf{HP}_{\mathscr{P}^\circ}(d) = (-1)^n \, \mathsf{HP}_{\mathscr{P}}(-d)$$

Example 3.108. — *We have seen that $\mathsf{HP}_{\Delta_n}(d) = \binom{d+n}{n}$, which can be also written*

$$\mathsf{HP}_{\Delta_n}(d) = \frac{(d+1)(d+2)\cdots(d+n)}{n!}$$

The Ehrhart-MacDonald reciprocity gives us the following writing for $\mathsf{HP}_{\Delta_n^\circ}$:

$$\mathsf{HP}_{\Delta_n^\circ}(d) = \frac{(d-1)(d-2)\cdots(d-n)}{n!} = \mathsf{HP}_{\Delta_n}(d-n-1)$$

which is not a surprise, since there are no integer interior points in $d \cdot \Delta_n$ for $0 < d \leq n$ and the integer interior points of $d \cdot \Delta_n$ form a simplex equal to $(1, \ldots, 1) + (d-n-1) \cdot \Delta_n$ if d is greater than or equal to $n+1$.

— *For the polytope $\mathscr{P} \subset \mathbb{R}^2$, it follows from $\mathsf{HP}_{\mathscr{P}}(z) = \frac{3d^2+3d+2}{2}$ that $\mathsf{HP}_{\mathscr{P}^\circ}(d) = \frac{3d^2-3d+2}{2}$, according to figure 3.100.*

Castelnuovo-Mumford regularity. The Castelnuovo-Mumford regularity of a graded module is an important measure of its "complexity": it is related to the degrees where its local cohomology modules vanish. We refer to [12, Ch. 15] for a detailed and general presentation. We define it here only in the case of a polytopal algebra:

Definition 3.109. *[12, 30, 13] Let $\mathbb{K}[Y] = \mathbb{K}[y_1, \ldots, y_r]$ and*

$$0 \longrightarrow E_s \longrightarrow \cdots \longrightarrow E_1 \longrightarrow \mathbb{K}[Y] \longrightarrow \mathbb{K}[\mathscr{P}] \longrightarrow 0$$

be a finite minimal free resolution of $\mathbb{K}[\mathscr{P}]$ as a graded $\mathbb{K}[Y]$-module, where E_i are graded finitely generated $\mathbb{K}[Y]$-modules. Let b_i be the maximum degree of the generators of E_i, for i in $\{1, \ldots, s\}$. Then, the Castelnuovo-Mumford regularity *of $\mathbb{K}[\mathscr{P}]$ is the number*

$$\operatorname{reg}(\mathbb{K}[\mathscr{P}]) = \max\{b_i - i \mid i \in \{1, \ldots, s\}\}$$

which does not depend on the chosen minimal finite free resolution.

The following classical proposition relates the regularity with a combinatorial property of the polytope $\mathscr{P}$ and with the degree of the numerator of $\mathsf{HS}_{\mathscr{P}}$:

Proposition 3.110. *[13, Sec. 5.4] Let $\mathscr{P}$ be a normal lattice polytope. The regularity $\mathrm{reg}(\mathbb{K}[\mathscr{P}])$ is equal to $n-d+1$, where d is the smallest integer such that $d\cdot\mathscr{P}$ contains an integer point in its interior.*

Example 3.111. *Since the smallest positive integer d such that $d\cdot\Delta_n$ contains an integer interior point is $n+1$, $\mathrm{reg}(\mathbb{K}[\Delta_n])=0$. The polytope $\mathscr{P}\subset\mathbb{R}^2$ defined by the convex hull of $(0,0),(2,1)$ and $(1,2)$ contains $(1,1)$ as integer interior point, therefore its regularity is $2-1+1=2$.*

Corollary 3.112. *With the same notations as in Proposition 3.103,* $\deg(Q)=\mathrm{reg}(\mathbb{K}[\mathscr{P}])$.

Proof. From proposition 3.103, we know that $\mathsf{HS}_{\mathscr{P}}(z)=\frac{Q(z)}{(1-z)^{n+1}}$ with $Q\in\mathbb{Z}[z]$ of degree less than or equal to n. The partial fraction expansion of $\mathsf{HS}_{\mathscr{P}}$ can be written

$$\begin{aligned}\mathsf{HS}_{\mathscr{P}}(z) &= \sum_{\ell=n+1-\deg(Q)}^{n+1}\frac{a_\ell}{(1-z)^\ell} && \text{with } a_{n+1-\deg(Q)}\neq 0\\ &= \sum_{\ell=n+1-\deg(Q)}^{n+1}\left[\frac{a_\ell}{(\ell-1)!}\sum_{i=0}^{+\infty}\prod_{j=1}^{\ell-1}(i+j)z^i\right]\end{aligned}$$

Then we obtain the equality $\mathsf{HP}_{\mathscr{P}}(d)=\sum_{\ell=n+1-\deg(Q)}^{n+1}\frac{a_\ell}{(\ell-1)!}\prod_{j=1}^{\ell-1}(d+j)$, and hence $d=n-\deg(Q)+1$ is the smallest positive integer such that $\mathsf{HP}_{\mathscr{P}}(-d)\neq 0$. It follows from the Ehrhart-MacDonald reciprocity (proposition 3.107) that $d=n-\deg(Q)+1$ is also the smallest positive integer such that $d\cdot\mathscr{P}$ contains an integer interior point. Proposition 3.110 concludes the proof. □

Example 3.113. *We have seen that $\mathsf{HS}_{\Delta_n}(z)=\frac{1}{(1-z)^{n+1}}$. The degree of 1 is zero, and is equal to the regularity of $\mathbb{K}[\Delta_n]$, according to the previous corollary. For the polytope $\mathscr{P}\subset\mathbb{R}^2$ seen previously, we have proved that $\mathsf{HS}_{\mathscr{P}}(z)=\frac{1+z+z^2}{(1-z)^3}$. Hence the degree of the numerator matches the regularity of $\mathscr{P}$.*

Part II

Contributions

Chapter 4

Solving systems with symmetries

This chapter is the main chapter of this thesis, and contains all the contributions involving polynomial systems with symmetries. It is divided into three sections, each of these corresponding to an article already published or that will be submitted separately.

Introduction

In this chapter, we are interested in solving problems with symmetry. The aim is to study such systems and their applications in the viewpoint of symbolic computations and more precisely Gröbner bases. The different questions that we want to answer can be summarized in:

— How can the algebraic structure given by the symmetry be used to obtain algorithmic improvements ?
— Given one possible symmetry, what is the complexity of solving a *generic system* having this symmetry ?
— Which systems can become solvable by taking their symmetry into account ?

What does symmetry mean ?

We focus on problems with symmetry given by the action of *a finite group*. Let $(f_1, \ldots, f_s)$ be polynomials in $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$, and $\mathbf{G} \subseteq \mathcal{GL}_n(\mathbb{K})$ be a finite matrix group. $\mathbf{G}$ acts on the affine space $\mathbb{K}^n$ and also on the vector space $(\mathbb{K}^n)^*$ of linear forms on $\mathbb{K}^n$, that can be identified with $\mathsf{Span}_{\mathbb{K}}(x_1, \ldots, x_n)$. For $A \in \mathbf{G}$, we denote by f^A the polynomial $f(A.x)$, where $x = {}^t(x_1, \ldots, x_n)$. Let $\mathcal{I}$ be the ideal $\langle f_1, \ldots, f_s \rangle$ and $\mathbb{V}_{\mathbb{K}}(\mathcal{I})$ be its associated variety (we refer to chapters 1 and 3 for precisions). The distinct cases of symmetries examined in this chapter are the following:

Stable Variety: V is said to be stable (or invariant) under the action of $\mathbf{G}$, which means that:

$$\forall x \in \mathbb{V}_{\mathbb{K}}(\mathcal{I}) \quad \forall A \in \mathbf{G} \qquad A.x \in \mathbb{V}_{\mathbb{K}}(\mathcal{I})$$

It is difficult to take the symmetry into account in this case, since there is no algebraic hypothesis on the action of $\mathbf{G}$ on $\mathcal{I}$. However, if $\mathbb{K}$ is algebraically closed, or if $\mathbb{V}_{\overline{\mathbb{K}}}(\mathcal{I})$, the variety of $\mathcal{I}$ in the algebraic closure of $\mathbb{K}$ is also $\mathbf{G}$-stable, we see with help of Hilbert's Nullstellensatz, that for all $f \in \mathcal{I}$ and for all $A \in \mathbf{G}$, f^A belongs to $\sqrt{\mathcal{I}}$, the radical of $\mathcal{I}$. Since $\mathbb{V}_{\mathbb{K}}(\mathcal{I}) = \mathbb{V}_{\mathbb{K}}(\sqrt{\mathcal{I}})$, this case can be reduced to the following one.

Stable Ideal: The ideal $\mathcal{I}$ is said to be *globally stable (or invariant) under the action of* $\mathbf{G}$ ($\mathbf{G}$-stable), if

$$\forall f \in \mathcal{I} \quad \forall A \in \mathbf{G} \qquad f^A \in \mathcal{I}$$

This case is the most important one, but there is no general strategy to solve a system generating a stable ideal. Note that, since $\mathbf{G}$ is a finite group, the set $\{f_i^A \mid 1 \leq i \leq s \text{ et } A \in \mathbf{G}\}$ is a finite set of generators of $\mathcal{I}$, which is stable under the action of $\mathbf{G}$. Hence, up to increase the number of generators, we can always assume that they form a $\mathbf{G}$-stable set.

Semi-stable equations. The ideal $\mathcal{I}$ is said to be generated by semi-invariant equations if

$$\forall i \in \{1, \ldots, s\} \quad \forall A \in \mathbf{G} \qquad f_i^A = \xi_i f_i$$

where $\xi_i \in \mathbb{K}$ for all i. Since the group $\mathbf{G}$ is finite, ξ_i is necessarily a root of 1. This is a subcase of the previous one.

Stable Equations: One interesting subproblem of the previous case is the following: $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ is generated by *individually* invariant equations under the action of $\mathbf{G}$, which means that:

$$\forall i \in \{1, \ldots, s\} \quad \forall A \in \mathbf{G} \qquad f_i^A = f_i$$

In this case, it is possible to work in the ring of invariant polynomials under the action of $\mathbf{G}$, denoted by $\mathbb{K}[X]^{\mathbf{G}} = \mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$. The structure of this ring goes back to work of Hilbert and has been intensively studied, see chapter 3.

We now detail the distinction between modular and non-modular cases. The action of $\mathbf{G}$ on $\mathcal{I}$ is said to be modular if the base field $\mathbb{K}$ has a positive characteristic which divides the order of the group $\mathbf{G}$, and non-modular otherwise. The invariant theory of finite groups is much better understood in the non-modular case. Therefore, when speaking about a problem with symmetries in the sequel, we will have to distinguish modular and non-modular cases.

Organization of the chapter

We present here briefly the three sections of the chapter.

An action of $\mathfrak{S}_n$ and application to the Vortex Problem. This section presents a strategy that takes advantage of the action of the symmetric group $\mathfrak{S}_N$, acting through a *block-diagonal representation* on several sets of N variables, in order to solve a polynomial system leading to a **stable ideal**. This action generalizes the classical action of the symmetric group $\mathfrak{S}_N$ on a set of N variables. This kind of problem is motivated by applications to physics/biology problems, and we apply our algorithms to the Vortex Problem in the plane: the goal is to solve in the complex plane the following equations:

$$\bar{z_i} = \sum_{j=1, j\neq i}^{n} \frac{1}{z_i - z_j} \qquad \forall i \in \{1, \ldots, n\}$$

where $\bar{z_i}$ denotes the complex conjugate of z_i. These equations are related to the *central configurations of vortices*. After reformulating the equations to obtain polynomials, we obtain an ideal in the ring $\mathbb{Q}[z_1, \ldots, z_n, Z_1, \ldots, Z_n]$, globally invariant under $\mathfrak{S}_N$ acting on both sets of variable $\{z_i\}, \{Z_i\}$. Since we want to obtain the variety in the Zariski-open subset $\cap_{i\neq j}\{z_i \neq z_j\}$ we can obtain *individually* invariant equations by applying several times *divided differences* to the equations. The system satisfies also a *rational parametrization assumption*, which allows us to reformulate the system, in order to obtain invariant equations involving only the first block of variables (z_i). In this case, the invariant ring $\mathbb{Q}[z_1, \ldots, z_n]^{\mathfrak{S}_n}$ is equal

to $\mathbb{Q}[e_1, \ldots, e_N]$ where e_i is the i-th symmetric function of the (z_j). Consequently, the next step is to rewrite the equations in terms of the (e_i), and solve the system. Finally, we have to remove some spurious solutions to recover all the central configurations.

Abelian groups and G-stable ideals. This section presents an approach to compute Gröbner bases of ideals *globally* invariant under the action of a matrix group $\mathbf{G}$ generated by diagonal matrices in the non-modular case. This approach can be used to solve systems invariant under every abelian group after a change of variables. The idea is that the action of the group $\mathbf{G}$ induces a grading on the ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. This grading allows us to obtain *semi-stable* equations instead of a stable ideal. Then, it can be used to split the Macaulay matrices arising during the computation of a Gröbner basis by use of linear algebra. The grading can be also used to split matrices arising in the FGLM algorithm. We suggest implementations in Magma/C and prove that this approach gives a gain of $|\mathbf{G}|^\omega$ (resp $|\mathbf{G}|^2$) while using our new *abelian* version of F_5 (resp FGLM) algorithm, instead of the classical versions.

SAGBI bases and invariant equations. In this section, we extend the results of Faugère and Rahmany in [41]. The aim is to propose new algorithms to solve systems of equations, which are individually invariant under the action of a group (**Stable Equations**). In [41], the authors proposed algorithms when $\mathbf{G}$ is a subgroup of the permutation group $\mathfrak{S}_n$. We suggest algorithms that can be applied with every group: all we have to know is a basis of $\mathbb{K}[X]_d^{\mathbf{G}}$, the component of homogeneous invariants of degree d. Moreover, we derive complexity bounds and give new approachs to remove spurious solutions that can appear during the computations.

4.1 Solving polynomial systems globally invariant under an action of the symmetric group. Application to the Vortex Problem

Introduction

This work is a common work with Jean-Charles Faugère and whas published in the proceedings of the ISSAC' 12 conference.

Problem Statement. In this section, we study the case of a *stable ideal* under the action of a finite group. The aim is to propose an efficient method to solve such problems assuming that the group is the whole symmetric group. To illustrate the algorithm and to demonstrate its efficiency, we apply the method to a well known physical problem called equilibria positions of vortices. Here, our problem generalizes the techniques used in the paper [40] dealing with the membrane inclusions curvature equations in biology, because it involves several groups of variables.

Vortex Problem. The problem of finding and classifying all relative equilibria of N-point vortices in the plane is of long-standing interest. In the plane, attacks on the problem date back to the 1800s with the works of von Helmholtz [54] and later in the works by Thomson [66] (the later Lord Kelvin). A complete bibliography of papers on the subject can be found in [77] or [2]. Several families of equilibria have been found [2] and other solutions have been found numerically, see [28]. More generally, the problem of equilibria on manifolds with different potentials has been studied by Albouy [1].

In the planar case, the problem is equivalent to solving the following algebraic system (in the following Z symbolizes the complex conjugate of z):

$$Z_i = \sum_{j=1, j\neq i}^{N} \frac{1}{z_i - z_j}.$$

Main results and organization of the section. In this section we describe a general algorithm and for each step we apply it to the equilibria of N-point vortices. The proposed algorithm is a three-step process:

1. We apply many times divided difference operators (see subsection 4.1.2) to the original system in order to obtain a new system of equations involving only invariant equations. For instance, the four-vortex problem is equivalent to

$$r_0 = s_1 = r_1 - 6 = r_2 = 2\,r_3 + 5\,s_2 = 0$$

   where $r_k = \sum_i Z_i\, z_i^k$ and $s_k = \sum_i z_i^k$ is the Newton sum.

2. As explained in subsection 4.1.3, the second step is to eliminate all the variables but the z_i. For that purpose, we require that the algebraic system fulfils the parameterization assumption (see definition 4.20). We derive a new system of equations involving only the symmetric functions of a subset of the variables. For instance, for the 4-vortex problem we obtain the symmetric system

$$e_3(e_2^2 + 12e_4)^2 = e_2(e_2^4 - 16e_2^2e_4 + 9e_2e_3^2 + 48e_4^2) = 0.$$

3. The last step consists simply in solving the symmetric equations using standard Gröbner bases techniques.

The organization of the section is as follows: we first present the vortex problem, and then successively explain the three points explained above. At the end of the section, we present timings that illustrate the efficiency of the approach on the vortex problem.

Applied to the vortex problem, our method has three advantages over previous methods:

1. In theory, it is possible to solve directly the original equations. However, when $N = 5$, it takes several days to compute the Gröbner basis and the number of solutions is 2060. By contrast, applying the new algorithm to the same problem gives rise to a system with 17 solutions that can be solved in less than 0.1 sec. The case $N = 7$ can be completely solved in about 20 minutes.
2. We are sure to find all the solutions, so we give a certificate for the previous numerical solutions. For $N \geq 5$, it is completely new.
3. Two distinct solutions could be so close, that 300 digits are needed to be sure that they are distinct, see [28] for example. With exact computations, the solutions appear to be distinct without further computations.

Since we are using only exact computations, our algorithm gives computational proofs of the solutions of the vortex problem.

4.1.1 Vortex Problem

4.1.1.1 Physical equations and first steps

We start with the equations of motion for the N-body problem:

$$\frac{\partial^2 \mathbf{r}_i(t)}{\partial t^2} = \sum_{j \neq i} m_j U'(s_{ij}(t))(\mathbf{r}_i(t) - \mathbf{r}_j(t)) \quad \text{for } i = 1, \ldots, N \tag{4.1}$$

where m_i and $\mathbf{r}_i$, are respectively the mass and the position vector (relative to the center of mass) for the i-th particle, $s_{ij} = |\mathbf{r}_i - \mathbf{r}_j|^2$ is the square of the distance between particles i and j and $U(s)$ is the potential function such that $U'(s) = s^a$ for some real value a. Without loss of generality, we can assume that the center of mass is at the origin. Usually the potential is one of the two well known potentials:

	a	*potential*
Newton	$-3/2$	$U(r) = r^{-\frac{1}{2}}$
Vortex	-1	$U(r) = \log(r)$

We are interested in solutions in the planar case. Moreover, we assume that all the masses (vortices) are equal (that is to say $m_i = 1$) and that the potential is the logarithmic one.

A central configuration is a configuration of bodies such that the acceleration vector for each body is a common scalar multiple of its position vector:

$$\frac{\partial^2 \mathbf{r}_i(t)}{\partial t^2} = \lambda(t)\mathbf{r}_i(t) \qquad \text{where } \lambda(t) \in \mathbb{R} \tag{4.2}$$

Central configurations are of interest for a variety of reasons: to every central configuration corresponds an *homothetic solution*, which is a solution that retains its shape for all time, while expanding, contracting and rotating around the center of mass.

We identify the real plane $\mathbb{R}^2$ with the complex plane $\mathbb{C}$. As we will see, in the planar case, it is easier to work with complex positions $z_i = x_i + \imath\, y_i = \mathbf{r}_i$. Hence $s_{i,j} = |\mathbf{r}_i - \mathbf{r}_j|^2 = (z_i - z_j)\,(\bar{z}_i - \bar{z}_j)$ where $\bar{z}$ is the complex conjugate of z. Combining equations (4.1) and (4.2) we obtain:

$$\lambda z_i = \sum_{j \neq i} \frac{(z_i - z_j)}{(z_i - z_j)\,(\bar{z}_i - \bar{z}_j)} = \sum_{j \neq i} \frac{1}{\bar{z}_i - \bar{z}_j} \tag{4.3}$$

Observe that the dependance on t has been removed, since the solutions of (4.3) depend only on λ. The value of λ is easy to recover from a solution $(z_1, \ldots, z_N)$, since the following property holds:

Proposition 4.1. *If $(z_1, \ldots, z_N)$ is a solution of equation (4.3), $2\lambda \sum_{i=1}^{N} |z_i|^2 = N\,(N-1)$.*

Proof. Let $i \in \{1, \ldots, N\}$. Then, by equation (4.3),

$$\lambda |z_i|^2 = \lambda z_i \bar{z}_i = \sum_{j \neq i} \frac{\bar{z}_i}{\bar{z}_i - \bar{z}_j} = \sum_{j \neq i} \left(1 + \frac{\bar{z}_j}{\bar{z}_i - \bar{z}_j}\right) = (N-1) - \sum_{j \neq i} \frac{\bar{z}_j}{\bar{z}_j - \bar{z}_i}$$

Hence, by summing over the index i, we obtain

$$\sum_{i=1}^{N} \lambda |z_i|^2 = N(N-1) - \sum_{i=1}^{N} \sum_{j \neq i} \frac{\bar{z}_j}{\bar{z}_j - \bar{z}_i} = N(N-1) - \sum_{i=1}^{N} \lambda |z_i|^2$$

and the conclusion follows. □

By summing over the index i, we see that $\sum z_i = 0$ (the center of mass is at the origin), so the first symmetric function of the z_i is equal to zero. Observe that $(z_1, \ldots, z_n)$ is solution of equation 4.3 if and only if $(\bar{z}_1, \ldots, \bar{z}_n)$ is. Hence, we have to solve the N following equations

$$\lambda \bar{z}_i = \sum_{j=1, j \neq i}^{N} \frac{1}{z_i - z_j} \tag{$E_{i,\lambda}$}$$

Moreover, since $\lambda > 0$ by proposition 4.1, we observe that $(E_{i,\lambda})$ can be rewritten:

$$\sqrt{\lambda} \bar{z}_i = \sum_{j=1, j \neq i}^{N} \frac{1}{\sqrt{\lambda} z_i - \sqrt{\lambda} z_j}$$

Hence, the uniform scaling by $\sqrt{\lambda}$ realizes a one-to-one mapping between the solutions of $(E_{i,1})$ and $(E_{i,\lambda})$. Therefore, we can assume that $\lambda = 1$ and recover the original solutions by multiplying the solutions of $(E_i) = (E_{i,1})$ by $\sqrt{\lambda}$. In summary, the central configuration problem is equivalent to solve the N equations:

$$\bar{z}_i = \sum_{j=1, j \neq i}^{N} \frac{1}{z_i - z_j} \tag{E_i}$$

4.1.1.2 Symmetry of the solutions

We now examine the symmetry of the solutions. Let $\mathbf{z} = (z_1, \ldots, z_N)$ be a solution of the equations (E_i).

— **Action of $\mathfrak{S}_N$.** The permutation group $\mathfrak{S}_N$ acts on the variables $\{z_1, \ldots, z_N\}$ with $\sigma(z_i) = z_{\sigma(i)}$. With this action, $E_i^\sigma = E_{\sigma(i)}$ for all $\sigma \in \mathfrak{S}_N$. Therefore, if $\mathbf{z}$ is a solution of the problem, any of the $N!$ N-tuples obtained by permutation of its coordinates is also a solution.

— **Action of $\mathcal{O}_2(\mathbb{R})$.** The isometry group of $\mathbb{R}^2$ can be identified to a transformation group on $\mathbb{C}$ generated by the rotations $z \mapsto az$ with a a complex of modulus one, and the symmetry $z \mapsto \bar{z}$. These transformations act on $\mathbb{C}^N$ by $\mathbf{z} \mapsto a\mathbf{z} = (az_1, \ldots, az_N)$ and $\mathbf{z} \mapsto \bar{\mathbf{z}} = (\bar{z_1}, \ldots, \bar{z_N})$. We have already seen that $\bar{\mathbf{z}}$ is also a solution of the equations (E_i). It is straighforward to verify that $a\mathbf{z}$ also is. Therefore, the set of solutions is invariant under these actions.

Consequently, the set of solutions is invariant under the action of $\mathfrak{S}_N \times \mathcal{O}_2(\mathbb{R})$. We will first focus on the action of $\mathfrak{S}_N$ to obtain invariant equations, and finally use the action of $\mathcal{O}_2(\mathbb{R})$ to speed up the Gröbner Basis computation (see subsection 4.1.4). Since any permutation of a solution of the vortex problem (E_i) is also a solution, it is natural to look for the symmetric functions in the solutions instead of the solutions themselves.

Definition 4.2. *Let Q be a univariate polynomial with complex coefficients of degree N, with no multiple roots. We say that Q is solution of the vortex problem if its roots $(z_1, \ldots, z_N$ are solutions of the equations (E_i).*

The following lemma is useful to express, in a very compact way, that such a polynomial Q is solution of the vortex problem.

Lemma 4.3. *A separable univariate monic polynomial Q in $\mathbb{C}[z]$ is solution of the vortex problem if and only if all roots z_i of Q satisfy $\bar{z}_i = \frac{1}{2}\frac{Q''(z_i)}{Q'(z_i)}$.*

Proof. Let $Q_i(z) = \frac{Q(z)}{z - z_i} = \prod_{j \neq i}(z - z_j)$, then $\frac{Q_i'(z)}{Q_i(z)} = \sum_{j \neq i} \frac{1}{z - z_j}$. Hence, according to the equations (E_i),

$$Q \text{ is solution of the vortex problem} \quad \Longleftrightarrow \quad \frac{Q_i'(z_i)}{Q_i(z_i)} = \bar{z}_i \text{ for all roots } z_i \text{ of } Q$$

But we can write $Q(z) = (z - z_i)Q_i(z)$, and with two derivations, we obtain $Q'(z) = Q_i(z) + (z - z_i)Q_i'(z)$ and $Q''(z) = 2Q_i'(z) + (z - z_i)Q_i''(z)$. Setting $z = z_i$, we get $Q_i(z_i) = Q'(z_i)$ and $Q''(z_i) = 2\,Q_i'(z_i)$. Hence, the lemma is proved. □

4.1.1.3 Particular solutions

Several particular solutions are known for this problem. We present only a few of them, see for example [77] for an overview. We have already said that the uniform scaling of factor $\sqrt{\lambda}$ changes solutions of $(E_{i,1})$ into solutions of $(E_{i,\lambda})$ It follows from lemma 4.3 that the roots of a separable monic polynomial Q satisfy equations $(E_{i,\lambda})$ if and only if $\frac{Q''(z_i)}{2Q'(z_i)} = \frac{\bar{z}_i}{\lambda}$ for all roots z_i of Q. Given such a polynomial, we just have to test if this relation holds for its roots and a given λ.

— **Regular polygon ($\mathbf{N \geq 2}$).** We want to prove that if $\{z_1, \ldots, z_N\}$ are the vertices of a regular N-gone, they are solutions of the vortex problem for some λ. Due to the

symmetries of the problem, we can assume that the center of the polygon is 0, and that the distance between the center and a vertex is 1. Due to the invariance by rotations, we can assume that the vertices are associated to the N-roots of 1. Hence, let $z_k = e^{\frac{2\imath k\pi}{N}}$ for $k \in \{1, \dots, N\}$ and $Q(z) = \prod_{k=1}^{N}(z - z_i) = x^N - 1$. Then $Q'(z) = Nz^{N-1}$ and $Q''(z) = N(N-1)z^{N-2}$, thus $\frac{Q''(z)}{2Q'(z)} = \frac{N-1}{2z}$. Consequently, with $\lambda = \frac{2}{N-1}$, $\frac{\bar{z_k}}{\lambda} = \frac{Q''(z_k)}{2Q'(z_k)}$ for all $k \in \{1, \dots, N\}$. Therefore:

$$z^N - 1 \text{ is solution of } (E_\lambda) \text{ with } \lambda = \frac{2}{N-1}$$

— **Regular centered polygon (N ≥ 3).** With the same analysis as in the previous point, we assume that $z_k = e^{\frac{2\imath k\pi}{N-1}}$ for $k \in \{1, \dots, N-1\}$ and $z_N = 0$, therefore $Q(z) = z^N - z$. It follows that $Q'(z) = Nz^{N-1} - 1$ and $Q''(z) = N(N-1)z^{N-2}$. Hence, $\frac{Q''(z)}{2Q'(z)} = \frac{N(N-1)z^{N-2}}{2(Nz^{N-1}-1)}$. Since $z_N = 0$ and $N \geq 3$, we have $\frac{Q''(z_N)}{2Q'(z_N)} = 0 = \bar{z_N}$, and for all $k \in \{1, \dots, N-1\}$, $\frac{Q''(z_k)}{2Q'(z_k)} = \frac{N(N-1)z_k^{N-2}}{2(N-1)} = \frac{N\bar{z_k}}{2}$.

$$z^N - z \text{ is solution of } (E_\lambda) \text{ with } \lambda = \frac{2}{N}$$

— **Aligned points.** We are interested in aligned points. Due to the symmetry by rotations of the problem, we can assume that these points lie on the real axis. Finding a solution of the vortex problem (with $\lambda = 1$) leads to finding a monic separable polynomial Q such that $\bar{z_i} = z_i = \frac{1}{2}\frac{Q''(z_i)}{Q'(z_i)}$ for all roots z_i of Q. Hence, polynomials $2NQ$ and $2zQ'(z) - Q''(z)$ both vanish on the roots of Q, have same degree N and same leading coefficient $2N$, so they are equal. The differential equation $2NQ - 2zQ' + Q''$ has only one polynomial solution for every N, which is the well know N-th *Hermite polynomial*, defined by $H_N(z) = (-1)^N \exp(x^2)\frac{d^N}{dz^N}\exp(-z^2)$.

4.1.1.4 Algebraic reformulation

For now, the equations (E_i) are rational equations, which mix variables z_i and their complex conjugates $\bar{z_i}$. Algebraically, it is not possible to separate $\imath$ and $-\imath$, and therefore z and $\bar{z}$. Thus, we introduce N new variables $Z_1, \dots, Z_N$, that represent $\bar{z_1}, \dots, \bar{z_N}$. The algebraic relations between these $2\,N$ variables are :

$$Z_i = \sum_{j \neq i} \frac{1}{z_i - z_j} \quad \text{and} \quad z_i = \sum_{j \neq i} \frac{1}{Z_i - Z_j} \qquad (E_i, \bar{E_i})$$

In order to obtain polynomials, we multiply the equation E_i by $D_i = \prod_{j \neq i}(z_i - z_j)$ to obtain the polynomial equation $U_i = 0$ where

$$U_i = Z_i \prod_{j \neq i}(z_i - z_j) - \sum_{j \neq i} \prod_{k \neq i,j} (z_i - z_k) \in \mathbb{Q}[z_1, \dots, z_N, Z_1, \dots, Z_N]$$

Observe that permuting z_i and Z_i for all i transforms the equation (E_i) in $(\bar{E_i})$, because of complex conjugation. Thus, for every relation in the ideal generated by the $2N$ equations $(E_i, \bar{E_i})$ in $\mathbb{Q}[z_1, \dots, z_N, Z_1, \dots, Z_n]$, there is another one obtained by permuting z_i and Z_i.

The ideal generated by the polynomials $U_i, \bar{U}_i$ is therefore *globally* invariant under the action of the conjugation τ, which acts on the system through the representation

$$M_\tau = \left(\begin{array}{c|c} & I_N \\ \hline I_N & \end{array}\right) \in \mathcal{GL}_{2N}(\mathbb{Q})$$

where I_N is the identity matrix of size $N \times N$. The ideal is also *globally* invariant under the action of the symmetric group $\mathfrak{S}_N$ through the representation given by

$$\sigma \longmapsto M_{\sigma,\sigma} = \left(\begin{array}{c|c} M_\sigma & \\ \hline & M_\sigma \end{array}\right) \in \mathcal{GL}_{2N}(\mathbb{Q})$$

where M_σ is the $N \times N$ matrix associated to $\sigma \in \mathfrak{S}_N$, as in proposition 3.13. We say that this action of $\mathfrak{S}_N$ is a *diagonal action*. Notice that the polynomials U_i, $\bar{U}_i$ are also weighted-homogeneous with weights 1 on variables z_i and -1 on Z_i.

The goal is to obtain equations depending only on the (e_i), the symmetric functions of the (z_i). To this end, it is useful to reintroduce the polynomial Q with indeterminate coefficients, which are new indeterminates $e_1, \ldots, e_N$. Hence, $Q(z) = \prod_{i=1}^{N}(z - z_i) = z^N - e_1 z^{N-1} + \cdots + (-1)^N e_N$. With help of the polynomial Q, the relations between variables e_i and z_i and lemma 4.3, the equation $U_i = 0$ can be reformulated $2Z_iQ'(z_i) - Q''(z_i) = 0$

In the next subsection we will see how to obtain equations of lower degree individually invariant under the action of $\mathfrak{S}_N$.

4.1.2 From invariant system to invariant equations

The algebraic equations obtained from the vortex problem are of a very special kind, which can be generalized as follows. Let $\mathbb{A}$ be an integral domain, $\mathcal{Z}$ be the set $\{z_1, \ldots, z_N\}$ and $\mathcal{V} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_\ell$ is another set of variables, decomposed in ℓ blocks of size N. For each $i \in \{1, \ldots, \ell\}$, we set $\mathcal{V}_i = \{x_{i,1}, \ldots, x_{i,N}\}$. We assume that $\mathfrak{S}_N$ acts on $\mathcal{Z} \cup \mathcal{V}$ through the diagonal representation of $\mathfrak{S}_N$, that is, $x^\sigma_{i,j} = x_{i,\sigma(j)}$ and $z^\sigma_j = z_{\sigma(j)}$ for all i, j and $\sigma \in \mathfrak{S}_N$. Let $(U_i)_{i\in\{1,\ldots,N\}}$ be a system of *globally* invariant polynomials under the action of $\mathfrak{S}_N$: for all $\sigma \in \mathfrak{S}_N$, $U^\sigma_i = U_{\sigma(i)}$. We also assume that U_i can be written $D_iP_i + R_i$, where $D_i = \prod_{j\neq i}(z_i - z_j)$, $P_i \in \mathbb{A}[\mathcal{Z} \cup \mathcal{V}]$ and $R_i \in \mathbb{A}[\mathcal{Z}]$, which also verify $P^\sigma_i = P_{\sigma(i)}$ and $R^\sigma_i = R_{\sigma(i)}$ for all $\sigma \in \mathfrak{S}_N$. The case of the vortex problem can be recovered by taking $\mathbb{A} = \mathbb{Q}$, $\ell = 1$, $\mathcal{V} = \{Z_1, \ldots, Z_N\}$, $P_i = Z_i$ and $R_i = -\sum_{j\neq i}\prod_{k\neq i,j}(z_i - z_k)$.

The aim of this subsection is to propose an algorithm that computes *individually* invariant equations under the action of $\mathfrak{S}_N$ from the system of globally invariant equations $\{U_i\}$. The main tool is *divided differences*. We first explain the simplest case, where there is only one block of variables.

4.1.2.1 Divided differences on one block

Here, we first assume that we only have one block of variables $\mathcal{Z} = \{z_1, \ldots, z_N\}$, $\mathcal{V} = \emptyset$ and N equations $U_i \in \mathbb{A}[z_1, \ldots, z_N]$ such that $\sigma(U_i) = U_{\sigma(i)}$ for all σ in $\mathfrak{S}_N$.

Definition 4.4. *We define recursively the divided differences of $U_1, \ldots, U_N$ by:*

— $[U_i] = U_i$ *for $i = 1, \ldots, N$.*

— $[U_{i_1}, \cdots, U_{i_k}] = \dfrac{[U_{i_1}, \cdots, U_{i_{k-1}}] - [U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}]}{z_{i_{k-1}} - z_{i_k}}$ *for any given distinct integers $i_1, \ldots, i_k$ in $\{1, \ldots, N\}$.*

Theorem 4.5. *The divided difference $[U_{i_1}, \cdots, U_{i_k}]$ is a polynomial in $\mathcal{Z}$ and depends only on the set $\{i_1, \ldots, i_k\}$, so for any subset $\mathcal{P} = \{i_1, \ldots, i_k\}$, we set $[U]_{\mathcal{P}} = [U_{i_1}, \ldots, U_{i_k}]$. Moreover, for any subset $\mathcal{P}$ of $\{1, \ldots, N\}$, and for any σ in $\mathfrak{S}_N$, $([U]_{\mathcal{P}})^{\sigma} = [U]_{\sigma(\mathcal{P})}$.*

Proof. We first prove by induction on $k \in \{1 \ldots, N\}$ that $[U_{i_1}, \ldots, U_{i_k}]$ is a polynomial in $\mathcal{Z}$.
- For $k = 1$, this is obvious.
- Let $k \in \{2, \ldots, N\}$ and assume that $[U_{i_1}, \ldots, U_{i_{k-1}}]$ is a polynomial for any $k-1$ distinct integers in $\{1, \ldots, N\}$. Let $i_1, \ldots, i_k$ be k distinct integers in $\{1, \ldots, N\}$. Since $z_{i_{k-1}} - z_{i_k}$ is monic as a univariate polynomial in $z_{i_{k-1}}$, we can perform the division of $\left[U_{i_1}, \cdots, U_{i_{k-1}}\right] - \left[U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}\right]$ by $z_{i_{k-1}} - z_{i_k}$. By mapping $z_{i_{k-1}}$ on z_{i_k}, we see that the remainder of the division is equal to 0, so $\left[U_{i_1}, \cdots, U_{i_{k-1}}, U_{i_k}\right]$ belongs to $\mathbb{A}[\mathcal{Z}]$.
- By induction, we conclude that $[U_{i_1}, \ldots, U_{i_k}]$ is a polynomial in $\mathbb{A}[\mathcal{Z}]$ for all distinct integers of $\{1, \ldots, N\}$.

To prove the second part of the statement, we just have to act with $\mathfrak{S}_N$ on the equality $[U_{i_1}, \cdots, U_{i_k}](z_{i_{k-1}} - z_{i_k}) = \left[U_{i_1}, \cdots, U_{i_{k-1}}\right] - \left[U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}\right]$ with any permutation σ and for all $k \geq 1$ and distinct integers $i_1, \ldots, i_k$. The proof follows by induction on N. □

When U_i can be written $F(z_i)$ for all $i \in \{1, \ldots, N\}$, where F is a univariate polynomial, it is usual to introduce a special notation.

Notations 4.6. *Let $F(z)$ be a univariate polynomial in $\mathbb{A}[z]$. We denote $F(z_1, \ldots, z_N)$ the divided difference $[F(z_1), \ldots, F(z_N)]$.*

The two following lemmas will be useful later.

Lemma 4.7. *For a univariate polynomial $F(z) \in \mathbb{A}[z]$, the following equality holds:*

$$F(z_1, \ldots, z_N) = \sum_{i=1}^{N} \frac{F(z_i)}{Q'(z_i)} \text{ where } Q(z) = \prod_{i=1}^{N} (z - z_i)$$

Proof. We prove this lemma by induction on N.
- For $N = 1, Q(z) = (z - z_1)$ so the assertion is obvious.
- Assume now that the equality holds for $N - 1 \geq 1$. Let $U(z) = \prod_{i=1}^{N-1}(z - z_i)$ and $V(z) = \left(\prod_{i=1}^{N-2}(z - z_i)\right) \times (z - z_N)$. Hence, $Q(z) = U(z)(z - z_N) = V(z)(z - z_{N-1})$, which implies that $Q'(z) = U(z) + U'(z)(z - z_N) = V(z) + V'(z)(z - z_{N-1})$. Therefore, $Q'(z_i) = U'(z_i)(z_i - z_N)$ for all $i \neq N$ and $Q'(z_i) = V'(z_i)(z_i - z_{N-1})$ for all $i \neq N - 1$. Consequently,

$$\begin{aligned}
F(z_1, \ldots, z_N) &= \frac{F(z_1, \ldots, z_{N-1}) - F(z_1, \ldots, z_{N-2}, z_N)}{z_{N-1} - z_N} \\
&= \frac{\sum_{i=2}^{N-1} \left(\frac{F(z_i)}{U'(z_i)} - \frac{F(z_i)}{V'(z_i)}\right)}{z_{N-1} - z_N} + \frac{\frac{F(z_{N-1})}{U'(z_{N-1})} - \frac{F(z_N)}{V'(z_N)}}{z_{N-1} - z_N} \qquad \text{(by induction)} \\
&= \frac{\sum_{i=2}^{N-1} \frac{F(z_i)(z_i - z_N - z_i + z_{N-1})}{Q'(z_i)}}{z_{N-1} - z_N} + \frac{F(z_{N-1})}{Q'(z_{N-1})} + \frac{F(z_N)}{Q'(z_N)} \\
F(z_1, \ldots, z_N) &= \sum_{k=1}^{N} \frac{F(z_k)}{Q'(z_k)}
\end{aligned}$$

— By induction, the lemma is proved for any $N \geq 1$.

□

Definition 4.8. *For $\mathcal{Z} = \{z_1, \ldots, z_N\}$, we define h_k the k-th complete symmetric function as the sum of all monomials of degree k on the variables in $\mathcal{Z}$. By extension, $h_k = 0$ when $k < 0$ and $h_0 = 1$.*

Lemma 4.9. *For any $k \geq 0$, if $F(z) = z^k$, then $F(z_1, \ldots, z_N) = h_{k-N+1}$.*

Proof. We prove this lemma again by induction on N.

— If $N = 1$, if $k \geq 0$, $F(z_1) = z_1^k$ is the complete symmetric function of degree k in one variable z_1.

— Let $N \geq 2$ and assume that the assertion is true for $N-1$. Then,

$$F(z_1, \ldots, z_N) = \frac{F(z_1, \ldots, z_{N-1}) - F(z_1, \ldots, z_{N-2}, z_N)}{z_{N-1} - z_N}$$

— If $k \leq N-3$, then by induction, both $F(z_1, \ldots, z_{N-1})$ and $F(z_1, \ldots, z_{N-2}, z_N)$ are equal to 0. Hence, $F(z_1, \ldots, z_N) = 0 = h_{k-N+1}$.

— If $k = N-2$, then by induction, both $F(z_1, \ldots, z_{N-1})$ and $F(z_1, \ldots, z_{N-2}, z_N)$ are equal to 1. Hence, $F(z_1, \ldots, z_N) = 0 = h_{k-N+1}$.

— If $k \geq N-1$, then by induction

$$F(z_1, \ldots, z_{N-1}) - F(z_1, \ldots, z_{N-2}, z_N) = \sum (z_{N-1}^{k-N+2-u} - z_N^{k-N+2-u}) \times m$$

where the sum is over all the monomials m in $z_1, \ldots, z_{N-2}$ of degree $u \in \{0, \ldots, k-N+2\}$. Writing $z_{N-1}^{k-N+2-u} - z_N^{k-N+2-u} = (z_{N-1} - z_N) \sum m'$, where the sum is over the monomials m' in z_{N-1}, z_N of degree $k-N+1-u$, we obtain exactly the complete symmetric function in $z_1, \ldots, z_N$ of degree $k-N+1$.

— By induction, the lemma is proved.

□

We explain here how to obtain invariant equations from divided differences in the case of only one block of variables.

Theorem 4.10. *Let V_i be $\sum_{\mathcal{P} \subset \{1,\ldots,N\}, |\mathcal{P}|=i} [U]_{\mathcal{P}}$ for all $i \in \{1, \ldots, N\}$. Then polynomials V_i are invariant under the action of $\mathfrak{S}_N$, and the varieties associated respectively to $\{V_i\}$ and $\{U_i\}$ are the same, except maybe for points with at least two equal components.*

Proof. Any σ in $\mathfrak{S}_N$ realizes a permutation of the subsets of $\{1, \ldots, N\}$ with same cardinality, and also a permutation of the $[U]_{\mathcal{P}}$ by theorem 4.5. Therefore, $V_i^\sigma = V_i$ for all i in $\{1, \ldots, N\}$. Assume that $\mathbf{a} = (a_1, \ldots, a_N)$ is a common zero of the polynomials U_i, without equal components. Then, we deduce easily that all the $[U]_{\mathcal{P}}(\mathbf{a})$ are equal to zero, and also the $V_i(\mathbf{a})$. Conversely, if $V_N(\mathbf{a}) = 0$ then all the $[U]_{\mathcal{P}}(\mathbf{a})$ with $\mathcal{P}$ of cardinality $N-1$ are equal, because V_N can be written as $\frac{[U]_{\mathcal{P}} - [U]_{\mathcal{Q}}}{z_k - z_\ell}$ where $\mathcal{P}$ and $\mathcal{Q}$ are two distinct subsets of cardinality $N-1$, $z_k = \mathcal{P} \backslash \mathcal{Q}$ and $z_\ell = \mathcal{Q} \backslash \mathcal{P}$. But their sum $V_{N-1}(\mathbf{a})$ is equal to zero, so they are equal to zero. We can repeat it for $i = N-2, N-3, \ldots, 1$ to deduce that $U_i(\mathbf{a}) = 0$ for all i. □

Using the Reynolds Operator (see definition 3.9), it is possible to compute only a few divided differences $[U]_{\mathcal{P}}$ in order to obtain the polynomials V_i: we just have to compute all

Algorithm 4.11: ComputeInvariantSystem algorithm

Input : Variables $\{z_1, \dots, z_N\}$ and the polynomials $U_i = D_i P_i + Q_i$
Output: Invariant Equations V_i
for $k = 2$ **to** N **do**
  $[U_1, \dots, U_k] :=$Quo$([U_1, \dots, U_{k-1}] - \tau_{k-1,k}([U_1, \dots, U_{k-1}]), z_{k-1} - z_k)$
return $\{\frac{1}{k!(N-k)!} \sum_{\sigma \in \mathfrak{S}_N} \sigma([U_1, \dots, U_k]), k = 1 \dots N\}$

divided differences $[U_1, U_2 \dots, U_k]$ for k in $\{1, \dots, N\}$, since $V_i = \binom{N}{i}\mathfrak{R}([U_1, \dots, U_i])$. We deduce from this property a simple algorithm 4.11 to compute the set $\{V_i\}$. In this algorithm, $\tau_{i,j}$ denotes the transposition permuting i and j.

Since $\mathbb{K}[z_1, \dots, z_N]^{\mathfrak{S}_N} = \mathbb{K}[e_1, \dots, e_N]$ (see theorem 3.33), we can rewrite the polynomials V_i in terms of the symmetric functions of the z_i. It is not possible to obtain such a nice writing while handling several blocks of variables (see the number of fundamental invariants needed for the diagonal action of $\mathfrak{S}_N$ in subsection 4.1.4). However, in the case of the vortex problem, we will see how to remove variables $Z_1, \dots, Z_N$ and perform this rewriting.

4.1.2.2 Generalization to several blocks and applications to the Vortex Problem

We come back to the general case where the polynomials U_i involve the set $\mathcal{Z} = \{z_1, \dots, z_N\}$ and another set of variables $\mathcal{V}$, and $\mathfrak{S}_N$ acts on $\mathcal{Z} \cup \mathcal{V}$. We recall the assumption that for each i, U_i can be written $D_i P_i + R_i$, where $D_i = \prod_{j \neq i}(z_i - z_j)$, R_i is a polynomial in $\mathcal{Z}$, and for all σ, $P_i^\sigma = P_{\sigma(i)}$ and $R_i^\sigma = R_{\sigma(i)}$. The previous case corresponds to the case $P_i = 0$, but when $P_i \neq 0$ we can still apply divided differences in the same way, and construct $[U_{i_1}, \dots, U_{i_k}]$ for given distinct integers, and obtain a similar theorem:

Theorem 4.12. *(i) $[U_{i_1}, \dots, U_{i_k}]$ is a polynomial in $\mathcal{Z}$ and $\mathcal{V}$ which depends only on the set $\{i_1, \dots, i_k\}$. Moreover for any σ and any $\mathcal{P}$, $\sigma([U]_\mathcal{P}) = [U]_{\sigma(\mathcal{P})}$.*
(ii) $V_i = \sum_{|\mathcal{P}|=i} [U]_\mathcal{P}$ is invariant under the action of $\mathfrak{S}_N$ and the varieties associated to respectively V_i and U_i are the same, except maybe for points with two equal $\mathcal{Z}$-components.

Proof. The proof is very similar to the proofs of theorems 4.5 and 4.10: the divided differences of (U_i) can be treated in two blocks, corresponding to (R_i) and $(D_i P_i)$. For the first block, the situation is the same, and for the second one, the presence of D_i ensures that the successive divisions by $z_{i_{k-1}} - z_{i_k}$ are possible. □

Corollary 4.13. *We can still use algorithm 4.11 to compute the V_i.*

We now apply this approach to the equations of the vortex problem. Recal that we obtained the following equations for all $i \in \{1, \dots, N\}$:

$$U_i = Z_i \prod_{j \neq i}(z_i - z_j) - \sum_{j \neq i} \prod_{k \neq i,j} (z_i - z_k)$$

which can be written as $U_i = D_i P_i + R_i$, with $P_i = Z_i$ and $R_i = -\sum_{j \neq i} \prod_{k \neq i,j}(z_i - z_k)$. These polynomials verify $P_i^\sigma = P_{\sigma(i)}$ and $R_i^\sigma = R_{\sigma(i)}$ for all i and all $\sigma \in \mathfrak{S}_N$.

Example 4.14. *For $N = 3$, it is easy to compute by hand the invariant polynomials V_1, V_2, V_3, and we obtain*

$$\begin{cases} V_1 = \sum_i Z_i z_i^2 - \sum_{j\neq i} Z_i z_i z_j + \sum_{\{i,j,k\}=\{1,2,3\}} Z_i z_j z_k \\ V_2 = 2\sum_i Z_i z_i - \sum_{i\neq j} Z_i z_j - 9 \\ V_3 = \sum_i Z_i \end{cases}$$

Using $V_3 = 0$ and $\bar{V}_3 = z_1 + z_2 + z_3 = 0$ in V_1 and V_2, we can rewrite the system as

$$\tilde{V}_1 = 4\sum_i Z_i z_i^2 \qquad \tilde{V}_2 = 3\sum_i Z_i z_i - 9 \qquad V_3 = 0$$

It turns out that the invariant equations of the vortex problem can be reformulated using a very small number of invariants, which leads to the following definition.

Definition 4.15. *From the variables $\mathcal{Z} = \{z_1, \dots, z_N\}$ and $\bar{\mathcal{Z}} = \{\bar{z}_1, \dots, \bar{z}_N\}$, we introduce the classical Newton sums:*

$$s_k = \sum_{i=1}^{N} z_i^k \qquad \text{and} \qquad S_k = \sum_{i=1}^{N} Z_i^k$$

and also new invariants, that we call twisted Newton sums*:*

$$r_k = \sum_{i=1}^{N} Z_i z_i^k \qquad \text{and} \qquad R_k = \sum_{i=1}^{N} Z_i^k z_i$$

Example 4.16. *For $N = 4$, after reformulation, we obtain the following equations:*

$$r_0 = s_1 = r_1 - 6 = r_2 = 2\,r_3 + 5\,s_2 = 0$$

and also the conjugate equations:

$$R_0 = S_1 = R_1 - 6 = R_2 = 2\,R_3 + 5\,S_2 = 0$$

Surprisingly, we can obtain a general and very simple expression of these equations for any N.

Theorem 4.17 (Invariant Equations)**.** *For any $N \geq 1$ and $k \geq 0$, the solutions of the vortex problem satisfy the following invariant equations:*

$$2\,r_k = \sum_{i=0}^{k-1} s_i\, s_{k-1-i} - k\, s_{k-1} \qquad \text{with } s_0 = N. \tag{4.4}$$

In order to prove the theorem 4.17 we first give a quite technical lemma.

Notations 4.18. *For $N \in \mathbb{N}^*$ and $j \in \mathbb{N}$, let e_j, h_j and s_j be respectively the symmetric function, the complete symmetric function, and the Newton sum of degree j in the variables $z_1, \dots, z_N$. We use the convention that $e_0 = h_0 = 1$, $s_0 = N$ and all these functions are equal*

to zero when $j < 0$. Moreover, $e_j = 0$ for $j > N$. We denote by E, H and S the generating series of $(e_j), (h_j)$ and (s_j), which can be written:

$$E(t) = \sum_{j=0}^{+\infty} e_j t^j = \prod_{i=1}^{N} (1 + t\, z_i)$$

$$H(t) = \sum_{j=0}^{+\infty} h_j t^j = \prod_{i=1}^{N} \frac{1}{1 - t\, z_i}$$

$$S(t) = \sum_{j=0}^{+\infty} s_j t^j = \sum_{i=1}^{N} \frac{1}{1 - t\, z_i}$$

Lemma 4.19. *With the previous notations, the following relation holds for all $k \geq 1$.*

$$\sum_{j=0}^{N} (-1)^j (N-j)(N-j-1)\, e_j\, h_{k-j-1} = \sum_{j=0}^{k-1} s_j\, s_{k-1-j} - k\, s_{k-1}$$

Proof. Let $\lambda_{k-1} = \sum_{j=0}^{N} (-1)^j (N-j)(N-j-1) e_j h_{k-j-1}$ and $\gamma_{k-1} = \sum_{j=0}^{k-1} s_j\, s_{k-1-j} - k\, s_{k-1}$ be the left and right terms of the equality we want to prove. Since $e_j = 0$ when $j > N$ and $h_{k-j-1} = 0$ when $j > k-1$, the sum in λ_{k-1} can be taken from 0 to $k-1$. We introduce

$$\Lambda(t) = \sum_{k=0}^{+\infty} \lambda_k t^k \qquad \text{and} \qquad \Gamma(t) = \sum_{k=0}^{+\infty} \gamma_k t^k$$

the associated generating series. We just have to prove that Λ and Γ are equal. We first rewrite Λ and Γ in terms of E, H and S.

$$\text{First,} \quad E(t) = \sum_{j=0}^{+\infty} e_j t^j \quad \text{then,} \quad E(-t) = \sum_{j=0}^{+\infty} (-1)^j e_j t^j.$$

$$\text{Moreover,} \quad E'(t) = \sum_{j=1}^{+\infty} j e_j t^{j-1} \quad \text{then,} \quad tE'(-t) = -\sum_{j=0}^{+\infty} (-1)^j j e_j t^j$$

$$\text{Finally,} \quad E''(t) = \sum_{j=2}^{+\infty} j(j-1) e_j t^{j-2} \quad \text{then,} \quad t^2 E''(-t) = \sum_{j=0}^{+\infty} (-1)^j j(j-1) e_j t^j.$$

Observe that $(N-j)(N-j-1) = N^2 - N - 2(N-1)j + j(j-1)$, hence

$$\Lambda(t) = (N^2 - N) E(-t) H(t) + 2(N-1) t E'(-t) H(t) + t^2 E''(-t) H(t)$$

It is easy to give an expression of Γ in terms of S and S':

$$\Gamma(t) = S^2(t) - S(t) - tS'(t)$$

We now rewrite Λ in terms of H and its derivatives: Clearly, $E(-t)H(t) = 1$. Furthermore, with two differentiations, we obtain $-E'(-t)H(t) + E(-t)H'(t) = 0$ and $E''(-t)H(t) - 2E'(-t)H'(t) + E(-t)H''(t) = 0$. Hence,

$$E'(-t)H(t) = \frac{H'(t)}{H(t)} \qquad \text{and} \qquad E''(-t)H(t) = -\frac{H''(t)}{H(t)} + 2\frac{H'^2(t)}{H^2(t)}$$

$$\text{Therefore,} \qquad \Lambda(t) = (N^2 - N) + 2(N-1)\frac{tH'(t)}{H(t)} + 2\frac{t^2H'^2(t)}{H^2(t)} - \frac{t^2H''(t)}{H(t)}.$$

$$\begin{aligned} \text{Moreover,} \quad H'(t) &= \sum_{i=1}^{N} \left(\prod_{j \neq i} \frac{1}{1-tz_i} \right) \frac{z_i}{(1-tz_i)^2} \\ H'(t) &= H(t) \sum_{i=1}^{N} \frac{z_i}{1-tz_i} \\ \text{Hence,} \qquad tH'(t) &= H(t) \sum_{i=1}^{N} \frac{tz_i - 1 + 1}{1-tz_i} \\ \text{Finally,} \qquad tH'(t) &= H(t)(-N + S(t)) \end{aligned}$$

It follows that Γ can also be rewritten with H and its derivatives. More precisely, we have

$$S(t) = N + t\frac{H'(t)}{H(t)}, S^2(t) = N^2 + 2Nt\frac{H'(t)}{H(t)} + t^2\frac{H'^2(t)}{H^2(t)}, S'(t) = \frac{H'(t)}{H(t)} + t\frac{H''(t)}{H(t)} - t\frac{H'^2(t)}{H^2(t)}$$

$$\text{Therefore,} \qquad \Gamma(t) = (N^2 - N) + 2(N-1)\frac{tH'(t)}{H(t)} + 2\frac{t^2H'^2(t)}{H^2(t)} - \frac{t^2H''(t)}{H(t)} = \Lambda(t).$$

and the lemma is proved. □

Proof of theorem 4.17. By lemma 4.3, we have already said that the equations of the vortex problem can be simply rewritten $2Q'(z_i)Z_i = Q''(z_i)$. Hence,

$$r_k = \sum_{i=1}^{N} z_i^k Z_i = \sum \frac{z_i^k Q''(z_i)}{2Q'(z_i)} = \sum \frac{F(z_i)}{Q'(z_i)} \qquad \text{where} \quad F(z) = \frac{z^k Q''(z)}{2}$$

Writing $Q(z) = z^N - e_1\, z^{N-1} + e_2\, z^{N-2} + \cdots + (-1)^N\, e_N = \sum_{j=0}^{N} (-1)^j e_j z^{N-j}$, we obtain

$$F(z) = \frac{1}{2} \sum_{j=0}^{N} (-1)^j (N-j)(N-j-1)\, e_j\, z^{N-j+k-2}.$$

By lemma 4.7, we know that $\sum \frac{F(z_i)}{Q'(z_i)} = F(z_1, \ldots, z_N)$. Using linearity and lemma 4.9, it follows that $2r_k = \sum_{j=0}^{N} (-1)^j e_j (N-j)(N-j-1)\, h_{k-j-1}$. Using lemma 4.19, we obtain the theorem 4.17. □

4.1.3 From two blocks to symmetric functions in one block

The aim of this subsection is to show how to obtain symmetric polynomials in only one block of variables from symmetric polynomials in two blocks, invariant under the diagonal action of $\mathfrak{S}_N$. This can be done easily under an additional assumption, which states that the system of equations admits a *rational parametrization*. Under this assumption, we give a general algorithm, which takes as input such a symmetric system in the variables $\{\mathcal{Z}, \bar{\mathcal{Z}}\}$ and returns directly polynomials in the symmetric functions $\{e_i\}$ of the first block. In particular, the algorihm can be applied to the previous invariant equations $\{V_i\}$ of the vortex problem. However, in this special case, the approach can be simplified and we propose a dedicated algorithm which returns equations in $\{e_i\}$ having a lower degree compared to the equations, that we can obtain with the general algorithm.

4.1.3.1 General case under the rational parameterization assumption

We return now to the general case of two blocks of variables where each U_i is an equation in $\mathbb{A}[\mathcal{Z}, \bar{\mathcal{Z}}]$ where $\mathcal{Z} = \{z_1, \ldots, z_N\}$ and $\bar{\mathcal{Z}} = \{Z_1, \ldots, Z_N\}$. In addition, we require that the algebraic system fulfils the following parameterization assumption:

Definition 4.20. *We say that the system $\{U_i = 0\}$ is under parameterization assumption if for all i, $Z_i = R(z_i)$ where $R(z) = \frac{N(z)}{M(z)} \in \mathbb{A}(z)$ with $\mathbb{A} = \mathbb{Q}(e_1, e_2, \ldots, e_N)$, so R is a univariate rational function whose coefficients depend on the symmetric functions of the z_i.*

The vortex problem satisfies this assumption, since from lemma 4.3, we have $Z_i = \frac{Q''(z_i)}{2Q'(z_i)}$, with $Q(z) = \prod(z - z_i)$.

We now describe an algorithm to obtain invariant equations under the action of $\mathfrak{S}_N$, in the first block of variables $\mathcal{Z}$. First, we apply the algorithm 4.11 to compute the invariant equations V_i. Denote again by $Q(z)$ the polynomial $\prod_i(z - z_i) = z^N - e_1 z^{N-1} + \cdots + (-1)^N e_N$. With notations of definition 4.20, there exist two polynomials B and C in $\mathbb{K}[e_1, \ldots, e_N][z]$ such that $B\,Q + C\,M = R_M$, where R_M is the resultant of Q and M with respect to the variable z. Since $Q(z_i) = 0$, it follows that:

$$R_M\, Z_i = R_M \frac{N(z_i)}{M(z_i)} = N(z_i)C(z_i).$$

More generally, the following relation holds for all $k \geq 0$:

$$R_M^k Z_i^k = (N^k \times C^k)(z_i) = (N^k \times C^k \mod Q)(z_i).$$

Notations 4.21. *In the following, the polynomial $NC \mod Q$ will be denoted $P_{\mathcal{Z}}$.*

For each $W \in \{V_i, \bar{V}_i\}$, we substitute $\frac{1}{R_M^k} P_{\mathcal{Z}}^k(z_i)$ to Z_i^k in each monomial of W. Up to a multiplication by a suitable power of R_M^k to obtain polynomials, we obtain equations involving only the variables $z_1, \ldots, z_N$. These polynomials are invariant under $\mathfrak{S}_N$, and can be reformulated as polynomials in the symmetric functions e_i.

These ideas lead to algorithm 4.22. In this algorithm, we denote by $\partial_{\mathcal{Z}} P$ the total degree of P as polynomial in the variables $Z_1, \ldots, Z_N$. For any polynomial P in $\mathbb{K}[z_1, \ldots, z_N]^{\mathfrak{S}_N}$, we denote by $\Sigma(P)$ the expression of P as polynomial in $\mathbb{K}[e_1, \ldots, e_N]$.

4.1.3.2 Application to the Vortex Problem. Dedicated algorithm.

For the vortex problem, we take $N = Q''/2$ and $M = Q'$, so the rational fraction R is equal to $\frac{Q''}{2Q'}$. Hence, the resultant $R_M = BQ + CQ'$ is equal to D, the resultant of $Q(z)$ with respect to the variable z. We still denote by $P_Z(z)$ the polynomial of $\mathbb{K}[e_2, \ldots, e_N][z]$ equal to $NC \mod Q = \frac{1}{2}Q''C \mod Q$. We can apply the previous algorithm to invariant polynomials to compute symmetric equations. From $V_k = 2r_k - \sum_{i=0}^{k-1} s_i s_{k-1-i} + k s_{k-1}$, we obtain always 0, but not from $\bar{V_k} = 2R_k - \sum_{i=0}^{k-1} S_i S_{k-1-i} + k S_{k-1}$. However, for the vortex problem, instead of using previous algorithm, there is a faster way to compute the equations, explained hereafter.

We introduce the two $\mathbb{K}[e_2 \ldots, e_N]$-modules morphisms :

$$\begin{array}{rccccc} \mathscr{S}: & \mathbb{K}[e_2, \ldots, e_N][z] & \to & \mathbb{K}[e_2, \ldots, e_N] & \text{and} & \mathscr{H}: \\ & z^k & \mapsto & s_k & & \end{array} \quad \begin{array}{ccccc} \mathbb{K}[e_2, \ldots, e_N][z] & \to & \mathbb{K}[e_2, \ldots, e_N] \\ z^k & \mapsto & h_{k-N+1} \end{array}$$

Algorithm 4.22: ComputeSymmetricFunctionsSystem algorithm

Input : The invariant equations $V_i, \bar{V}_i$ of variables $\mathcal{Z} = \{z_1, \ldots, z_N\}$ and $\bar{\mathcal{Z}} = \{Z_1, \ldots, Z_N\}$, the polynomial $Q = \prod(z - z_i)$, the polynomial $P_{\mathcal{Z}}$ and the resultant R_M.

Output: A system of $2N$ equations of variables e_i, the symmetric functions of the z_i

$m := \max\{\partial_{\mathcal{Z}} W \mid W \in \{V_i, \bar{V}_i\}\}$;

$L := [P_{\mathcal{Z}}^i \mod Q \mid i \in \{1, \ldots, m\}]$;

for W *in* $\{V_1, \ldots, V_n, \bar{V}_1, \ldots, \bar{V}_n\}$ **do**

  $d_W := \partial_{\mathcal{Z}}(W)$;

  for U *monomial of* W **do**

    $d_U := \partial_{\mathcal{Z}}(U)$;

    for $i := 1$ **to** N **do**

      $Z_i^k \leftarrow L[k](z_i)$ in U;

    $U \leftarrow R_M^{d_W - d_U} U$ in W;

return $\{\Sigma(W)\}$

Proposition 4.23. *For any polynomial P in $\mathbb{K}[e_2, \ldots, e_N][z]$, $\mathscr{S}(P)$ is equal to $\mathscr{S}(P \mod Q)$ and $\mathscr{H}(P) = \mathscr{H}(P \mod Q)$. Moreover*

$$\mathscr{S}(P) = \sum_{i=1}^{N} P(z_i) \quad \textit{and} \quad \mathscr{H}(P) = \sum_{i=1}^{N} \frac{P(z_i)}{Q'(z_i)}.$$

In particular, if $P = \sum_k^{N-1} a_k z^k$, then $\mathscr{H}(P) = a_{N-1}$.

Proof. Evaluating Q at a z_i leads to 0 since $Q = \prod(z - z_i)$. The second part of the proposition comes from the definion of $\mathscr{S}$ and $\mathscr{H}$ together with lemma 4.9. □

From theorem 4.17, we know that $2\,r_k = \left(\sum_{i=0}^{k-1} s_i\, s_{k-1-i}\right) - k\, s_{k-1}$, therefore the conjugate equation holds:

$$2\,R_k = \left(\sum_{i=0}^{k-1} S_i\, S_{k-1-i}\right) - k\, S_{k-1} \tag{4.5}$$

One way to obtain directly symmetric equations is to compute:

$$S_k = \sum_{i=1}^{N} Z_i^k = \frac{1}{D^k} \sum_{i=1}^{N} P_Z^k(z_i) = \frac{1}{D^k} \mathscr{S}(P_Z^k(z) \mod Q)$$

$$R_k = \sum_{i=1}^{N} z_i Z_i^k = \frac{1}{D^k} \sum_{i=1}^{N} z_i\, P_Z^k(z_i) = \frac{1}{D^k} \mathscr{S}(z\, P_Z^k(z) \mod Q)$$

Substituting these expressions in (4.5) we obtain the following proposition:

Proposition 4.24. *Given the Bézout relation $B(z)\,Q(z) + C(z)\,Q'(z) = D$, for any N and k, the solution of the vortex problem satisfies the following symmetric equations:*

$$\frac{2}{D} \mathscr{S}(z\, P_Z^k) = \sum_{i=0}^{k-1} \mathscr{S}(P_Z^i)\, \mathscr{S}(P_Z^{k-1-i}) - k\, \mathscr{S}(P_Z^{k-1})$$

where $\mathscr{S}(1) = N$ and $P_Z = \frac{1}{2} Q'' C$.

The drawback of the method is that high powers of the discriminant occur in the resultant equations. Instead of using the polynomial P_Z to obtain equations with the e_i's, we will use another polynomial. Using the following lemma it is possible to compute R_k and S_k with only half of the powers of the discriminant:

Lemma 4.25. *Given the Bézout relation $B(z)\,Q(z) + C(z)\,Q'(z) = D$, the following relation holds for all $k \in \{1, \ldots, n\}$:*

$$D\,\frac{Q''}{Q'^2}(z_k) = A(z_k)$$

where $A(z)$ is the polynomial $-(B(z) + C'(z))$.

Proof. By derivating the relation $BQ + CQ' = D$, we obtain $B'Q + (B' + C)Q' + CQ'' = 0$. Therefore, modulo Q, $CQ' = D$ and $(B' + C)Q' + CQ'' = 0$. Hence, $A = -(B' + C)$ verifies $A = \frac{CQ''}{Q'} = \frac{DQ''}{Q'^2}$ modulo Q. □

Consequently, with one power of A, there are two powers of Q' in the denominator, and only one power of D in the numerator. Hence, using $\mathscr{S}$ when k is even and $\mathscr{R}$ when k is odd, we obtain R_k and S_k in the following way:

Proposition 4.26. *The expressions of S_i and R_i in terms of the symmetric functions of the z_i's are given by the following formulas for all $k \geq 0$:*

$$\begin{array}{ll} D^k S_{2k} = \frac{1}{2^{2k}}\mathscr{S}(Q''^k A^k) & D^k R_{2k} = \frac{1}{2^{2k}}\mathscr{S}(z\,Q''^k A^k) \\ D^k S_{2k+1} = \frac{1}{2^{2k+1}}\mathscr{H}(Q''^{k+1} A^k) & D^k R_{2k+1} = \frac{1}{2^{2k+1}}\mathscr{H}(z\,Q''^{k+1} A^k) \end{array}$$

and all polynomials can be taken modulo Q.

Proof. With $Z_i = \frac{Q''(z_i)}{2Q'(z_i)}$, we have $D^k S_{2k} = \frac{1}{2^{2k}} \sum_{i=1}^{N} Q''(z_i)^k \left(D^k \frac{Q''(z_i)^k}{Q'(z_i)^k} \right) = \frac{1}{2^{2k}}\mathscr{S}(Q''^k A^k)$. The formulas in the other cases can be obtained in the same way. □

Substituting these expressions in (4.5) we obtain:

Theorem 4.27 (Symmetric Equations)**.** *Given the Bézout relation $B(z)\,Q(z) + C(z)\,Q'(z) = D$, and $A(z) - B(z) - C'(z)$, the solutions of the vortex problem satisfy the following symmetric equations, for any N and k:*

$$\begin{aligned} \frac{1}{2\,D}\,\mathbf{S}_{2k+1} &= \sum_{i=0}^{k-1} \mathbf{S}_{2i}\,\mathbf{H}_{2(k-i-1)} - 2k\,\mathbf{H}_{2k-2} \\ \mathbf{H}_{2k+1} &= \sum_{i=0}^{k} \mathbf{S}_{2i}\,\mathbf{S}_{2(k-i)} + D\sum_{i=0}^{k-1} \mathbf{H}_{2i}\,\mathbf{H}_{2(k-i-1)} - (2k+1)\,\mathbf{S}_{2k} \end{aligned}$$

where $\mathbf{S}_{2i+\delta} = \mathscr{S}(z^\delta\,Q''^i\,A^i)$, $\mathbf{H}_{2i+\delta} = \mathscr{H}(z^\delta\,Q''^{i+1}\,A^i)$ for $\delta = 0, 1$.

Proof. We substitute the expression of R_{2k}, R_{2k+1}, S_{2k}, S_{2k+1} given by proposition 4.26 into the equations:

$$\begin{aligned} 2\,R_{2k} &= 2\textstyle\sum_{i=0}^{k-1} S_{2\,i}\,S_{2\,k-1-2\,i} - 2k\,S_{2k-1} \\ 2\,R_{2k+1} &= \textstyle\sum_{i=0}^{k} S_{2i}\,S_{2k-2i} + \sum_{i=0}^{k-1} S_{2i+1}\,S_{2k-2i-1} - (2k+1)\,S_{2k} \end{aligned}$$

□

This theorem gives the very efficient algorithm 4.28 to compute a system involving only the e_i, which solutions include all symmetric functions of the vortex problem. To simplify the description of the algorithm we introduce the following notation $\alpha_{i,k}$ and β_k, which depend only on the parity of i and k:

$$\beta_k = \begin{cases} 0 \text{ if k is odd} \\ 1 \text{ if k is even} \end{cases} \qquad \alpha_{i,k} = \begin{cases} 0 \text{ if i is even and k odd} \\ 1 \text{ otherwise} \end{cases}$$

Algorithm 4.28: ComputeSymmetricFunctionsVorticesSystem algorithm

Input : N, the polynomials Q, D and $A = -B - C'$, where B and C appear in the Bézout relation $B\,Q + C\,Q' = D$, and the two functions $\mathscr{S}$ and $\mathscr{H}$
Output: Symmetric polynomials in the e_i's
$L_R := [\frac{N(N-1)}{2}]$; $L_S := [0]$; $P := 1$;
for $k = 2$ **to** $N-1$ **do**
  if *IsOdd(k)* **then**
    $L_S := L_S \cup [\mathscr{H}(\frac{1}{2}PQ'' \mod Q)]$;
    $L_R := L_R \cup [\mathscr{H}(\frac{z}{2}PQ'' \mod Q)]$;
  else
    $P := \frac{PAQ''}{4} \mod Q$;
    $L_S := L_S \cup [\mathscr{S}(P)]$;
    $L_R := L_R \cup [\mathscr{S}(z\,P \mod Q)]$;
return
$\{2L_R[k] - \sum_{i=1}^{k-2} D^{\alpha_{i,k}}\, L_S[i]\, L_S[k-1-i] - (2N-k)\, D^{\beta_k}\, L_S[k-1],\ k = 2 \ldots N-1\}$

Remark 4.29. *The equation $2R_1 = N(N-1)$ gives always $0 = 0$. We explain this fact in the next subsection.*

Example 4.30. *The case $N = 4$ can be handled by hand. In this case, $Q(z) = z^4 + e_2\,z^2 - e_3\,z + e_4$ and $A(z)$ is equal to the polynomial*

$$(-8\,{e_2}^3 + 32\,e_4\,e_2 - 36\,{e_3}^2)z^2 - 8\,e_3\,(12\,e_4 + {e_2}^2)z - 54\,{e_3}^2 e_2 + 80\,e_4\,{e_2}^2 - 192\,{e_4}^2 - 8\,{e_2}^4.$$

From theorem 4.27, the first equation is $R_2 = 0 = \mathscr{S}(z\,A(z)Q''(z))$. Hence we compute

$$\begin{aligned} P = zAQ'' \mod Q \;=\; & (640\,e_4\,{e_2}^2 - 16\,{e_2}^4 - 2304\,{e_4}^2 - 288\,{e_3}^2 e_2)z^3 \\ & - 16\,e_3\,(27\,{e_3}^2 - 84\,e_4\,e_2 + {e_2}^3)z^2 \\ & + (-204\,{e_3}^2{e_2}^2 + 256\,e_4\,{e_2}^3 - 768\,{e_4}^2 e_2 - 16{e_2}^5 - 720\,e_4\,{e_3}^2)z \\ & + 96 e_4 e_3 (12 e_4 + {e_2}^2). \end{aligned}$$

The next step is to replace z^3 by $s_3 = 3e_3$, z^2 by $s_2 = -2e_2$ and z by $s_1 = 0$ so that

$$0 = \mathscr{S}(z\,AQ'') = -16\,e_3\,(12\,e_4 + {e_2}^2)^2$$

In the same way, we compute the second equation $\mathscr{H}(\,z\,Q''^2 A) - (2\,N-3)\,\mathscr{S}(A\,Q'') = 0$. We obtain the system of two equations:

$$\begin{cases} e_3(e_2^2 + 12e_4)^2 &= 0 \\ e_2(e_2^4 - 16e_2^2e_4 + 9e_2e_3^2 + 48e_4^2) &= 0 \end{cases} \tag{4.6}$$

4.1.4 Solving the equations with the symmetric functions

The aim of this subsection is to solve explicitly the symmetric equations by exact methods. To this end, we will use Gröbner bases computation.

The case $N = 4$. Interestingly enough, we can solve the vortex problem by hand when $N = 4$. Hence, we give the complete resolution of the case $N = 4$ without Gröbner Basis computation. The symmetric equations are given by the equation (4.6) and, in addition, we assume that the discriminant

$$D = 16e_2^4e_4 - 4e_2^3e_3^2 - 128e_2^2e_4^2 + 144e_2e_3^2e_4 - 27e_3^4 + 256e_4^3$$

is non-zero, to ensure that the z_i's are distinct.

Lemma 4.31. *In equations* (4.6)*, if $e_2 \neq 0$, then $e_3 = 0$.*

Proof. We prove it by reduction to the absurd. If $e_2 \neq 0$ and $e_3 \neq 0$, the first equation states that $e_4 = -e_2^2/12$. Replacing e_4 by $-e_2^2/12$ in the second equation leads to $8e_2^3+27e_3^2 = 0$, but replacing it in the discriminant leads to$-(8e_2^3 + 27e_3^2)^2/27 \neq 0$, which is a contradiction. □

Then, if $e_2 \neq 0$, $e_3 = 0$, and the second equation becomes $(e_2^2 - 12e_4)(e_2^2 - 4e_4) = 0$, but D becomes $16e_4(e_2^2 - 4e_4)^2 \neq 0$, so $e_4 = \frac{1}{12}e_2^2$. If $e_2 = 0$ then $e_3 = 0$ or $e_4 = 0$. We can conclude that:

Proposition 4.32. *When $N = 4$, there are three solutions to the vortex problem :*

$$Q(z) = z^4 + e_2z^2 + \frac{1}{12}e_2^2 \qquad Q(x) = z^4 - e_3z \qquad Q(x) = z^4 + e_4$$

The indetermination on e_2, e_3 or e_4 will be explained and solved in the next subsection as shown in the figures 4.36,4.37 and 4.38.

Homogeneity of the equations. It turns out that the equations obtained in the previous subsection are homogeneous for a graded degree. This homogeneity will be useful to speed up the computation of the solutions.

Proposition 4.33. *The equation we obtained in the previous subsection are homogeneous for the degree $d = \sum_k k \times \partial_{e_k}$, where ∂_{e_k} is the degree in e_k. More precisely, the k-th equation has degree $d = N(N-1)\lfloor\frac{k}{2}\rfloor + 1 - k$.*

Proof. We started from $2R_k = \sum S_iS_{k-1-i} - kS_{k-1}$. With $Z_i = \sum_{k\neq i} \frac{1}{z_i - z_k}$, we see that this equation is homogeneous in the z_i of degree $1 - k$. The discriminant $D = \prod_{i\neq j}(z_i - z_j)$ is homogeneous of degree $2\binom{N}{2}$. So, the previous equation is homogeneous in the z_i with degree $2\lfloor\frac{k}{2}\rfloor\binom{N}{2} + 1 - k$. The symmetric function e_k is homogeneous in the z_i of degree k, that's why we took the degree d. □

Recall that we have lost the equation $2r_1 = 2R_1 = N(N-1)$, but there is no surprise : we have seen that the set of solutions (the z_i's) is invariant under multiplication by a complex of modulus one. This implies that the algebraic variety with variables $(e_2, \ldots, e_N)$ is invariant under the operation $(e_2, \ldots, e_N) \mapsto (\gamma^2e_2, \ldots, \gamma^Ne_N)$, with $|\gamma| = 1$. But an ideal associated to such a variety is homogeneous for the previous degree d : let P be a polynomial in this ideal, and write $P = \sum_u P_u$, with P_u the homogenous part of degree u for the degree d, then if $(e_2, \ldots, e_N)$ is a zero of P; we have $\sum_u \gamma^u P_u(e_2, \ldots, e_N) = 0$ for all γ of modulus 1. A non-zero univariate polynomial have only a finite number of roots, so this polynomial (in γ) is null and $P_u(e_2, \ldots, e_N) = 0$ for all u.

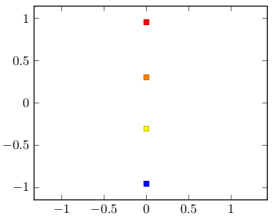
Strategy to compute the solutions Because of the homogeneity, we can assume that any of the symmetric functions e_i is equal to 1 or 0. If it is 0, we have again a homogeneous system, so we can suppose that another symmetric function e_j is equal to 1 or 0, and so on. We have to add a new equation to ensure that all the z_i are distinct : $h \times D = 1$. (We cannot solve the equations and remove the spurious solutions easily : for example, for $N = 5$, the system with $e_2 = 1$ without $h \times D = 1$ is 1-dimensional.)

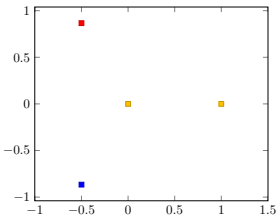
According to the benchmark, it seems that the fastest way to compute a Gröbner Basis is to separate the system into two parts, $e_2 = 1$ or $e_2 = 0$ and compute a Gröbner Basis with DRL order with $h > e_N > \cdots > e_3$, and then perform a change of ordering from DRL to the lexicographic order with FGLM (algorithm 1.52). For the component with $e_2 = 0$, we separate $e_3 = 1$ or $e_3 = 0$, and so on.

Then, we perform a Triangular Decomposition (see [72]) of each component.

Remark 4.34. *To compute a Gröbner Basis, we assume that $e_k = 1$ for some k. But with this assumption, the solutions $(z_1, \ldots, z_N)$ that we obtain are not solutions of the equations (E_i) $\bar{z}_i = \sum_{j \neq i} \frac{1}{z_i - z_j}$ but of $\lambda \bar{z}_i = \sum_{j \neq i} \frac{1}{z_i - z_j}$ for some $\lambda > 0$. Denote by $(az_1, \ldots, az_N)$ the solutions of (E_i), where a can be supposed to be a positive real. Then $2r_1 = 2R_1 = 2a^2 \sum_i |z_i|^2 = N(N-1)$, and $a = \sqrt{\frac{N(N-1)}{2\sum |z_i|^2}}$. The true value of e_k is $\sum a\, z_{i_1} \times \cdots \times a\, z_{i_k} = a^k$.*

Example 4.35. *With e_2, e_3 or e_4 equal to 1, the solutions $(z_1, \ldots, z_4)$ for $N = 4$ are drawn below :*





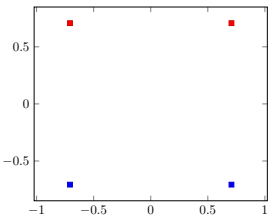


Figure 4.36 – $Q(z) = z^4 + z^2 + \frac{1}{12}$ Figure 4.37 – $Q(z) = z^4 - z$ Figure 4.38 – $Q(z) = z^4 + 1$

In the case of the four aligned points, $\sum_i |z_i|^2$ is equal to 2, so we have to perform a multiplication by $\sqrt{3}$ to obtain the solutions of (E_i). In the case of the centered equilateral triangle, $\sum_i |z_i|^2 = 3$, so $a = \sqrt{2}$ and in the case of the square, $\sum_i |z_i|^2 = 4$, so $a = \sqrt{\frac{3}{2}}$.

Removing spurious solutions. We can solve the system to obtain approximations of the e_i and then approximations of the z_i, but there are spurious solutions: we have to check that $P_Z(z_i) = D\,\bar{z}_i$ for each i to be sure that we have computed a true solution. Another way to perform it is to introduce two news variables x and z and add to the system the equations $P_Z(z) + D\,z = x$ and $z^N + e_2 z^{N-2} + \cdots + (-1)^N e_N$, with P_Z the polynomial computed previously, which maps z_i to DZ_i. The next step is to perform a Gröbner elimination with lexicographical order $z > e_N > \cdots > e_k > x$ to obtain a univariate polynomial $P_{\Re}$ in x. Then we isolate the real roots of this polynomial $P_{\Re}$ using certificated methods, see for example [83, 84].

Other symmetries. Assume that $(e_2, \ldots, e_N)$ is a solution with $e_2 = 1$. We have said that if $(e_2, \ldots, e_N)$ is a solution, then $(\lambda^2 e_2, \ldots, \lambda^N e_N)$ too, for all λ of modulus 1. If $\lambda = -1$ (geometrically, we do a symmetry of center O), e_2 stays at 1, but e_3 is changed into $-e_3$, so

we can keep only half of the possible e_3. The conjugation $(e_2, \ldots, e_N) \to (\bar{e_2}, \ldots, \bar{e_N})$ gives an other solution, so if e_3 is not real, we can suppose e_3 with imaginary part non negative. If e_3 is real and e_4 not, we can keep only the e_4 with imaginary part non negative, and so on.

4.1.5 Benchmarks

In this subsection, we indicate timings that we have obtained, in order to compute the equations involving only the symmetric functions (e_i) of $z_1, \ldots, z_N$. We also indicate how difficult it is to solve the problem with naive approach or using invariant theory.

Naive Approach. It is possible to solve directly the original system of $2N$ equations $(E_i, \bar{E}_i)$ in z_i and Z_i. Because of invariance by multiplication by a scalar of modulus 1, we can assume that z_1 is real, so we add the equation $z_1 = Z_1$. This trick gives an ideal of dimension 0, if we assume that $z_1 \neq 0$. We split the ideal into two parts : in the first one, we add the equation $z_1 \times \alpha = 1$, and in the second one, we add $z_1 = 0$, and we can add $z_2 = Z_2$. In each case, the ideal is zero dimensional, if we add the last equation $\prod_{i<j}(z_i - z_j)\beta = 1$, to ensure that all the z_i are distinct. We report in table 4.39 the following timings with Magma to compute the corresponding Gröbner basis (∞ means that we stopped the computation after five days):

	3	4	5
$\mathbb{Q}$	$0.02s$	$176.8s$	∞
$\mathbb{F}_{65521}$	$0.01s$	$0.2s$	∞

Table 4.39 – Direct approach: Gröbner bases of the non symmetric systems with Magma.

Invariant Theory. It is possible to introduce the ring of polynomials invariant under $\mathfrak{S}_N$ through the *diagonal representation*, see subsection 4.1.1. We report in table 4.40 the number of secondary invariants in the Hironaka decomposition or the number of fundamental invariants over $\mathbb{Q}$, and the timings to compute them in Magma. ∞ means that we stopped the computation after five days.

	3	4	5	6	7
Secondary Invariants	6	24	120	?	?
Timings	$0.0s$	$0.1s$	$225s$	∞	∞
Fundamental Invariants	9	14	20	27	?
Timings	$0.0s$	$0.1s$	$3.0s$	$400s$	∞

Table 4.40 – Invariant Ring : Hironaka Decomposition and Fundamental Invariants with Magma.

Generating and solving the symmetric system We have implemented the algorithm 4.22 in Maple and Magma to generate the symmetric system. We report in table 4.41 the timings to compute the systems depending only on the symmetric functions e_i using this algorithm with these software (Intel Xeon 2.93 GHz with 128GB Ram).

	4	5	6	7	8
Magma	0.0s	0.0s	0.06s	70.6s	7649.6s
Maple	0.0s	0.2s	0.9s	41.9s	2407.3s

Table 4.41 – Time to generate the symmetric systems with Maple or Magma.

On the same computer, the times to compute a Gröbner Basis using Magma of the symmetric system and perform a triangular decomposition of each component (mostly for the component with $e_2 = 1$) are presented in table 4.42.

	4	5	6	7
$\mathbb{Q}$	0.02s	0.10s	296.7s	?
$\mathbb{F}_{65521}$	0.53s	1.58s	3.9s	1680.8s

Table 4.42 – Gröbner bases of the symmetric systems with Magma.

When $N = 7$ we use FGb [63] to compute the corresponding Gröbner bases: it takes 144 secondes to compute the system over $\mathbb{F}_{65521}$ and about 20 minutes to compute a Gröbner basis and a triangular decomposition over $\mathbb{Q}$. The complete prime decomposition of the ideal corresponding to the case $N = 7$ is presented in figure 4.43. Using all the symmetries the problem admits 12 solutions. Among them, we recognize the particular cases in presented in the first subsection: the regular heptagone, the regular centered hexagone and the aligned points. Other classical solutions that have not been mentioned can be recognized: the pattern with all points aligned but two of them and the pattern with several triangles and a point in the middle, which is alone in the component $e_2 = 0$ and $e_3 \neq 0$. Notice that this solution is very close to another one in the component $e_2 = 1$ and $e_3 \neq 0$. Even up to symmetries, these two solutions are not the same, since the property $e_2 = 0$ is maintained by the group $\mathfrak{S}_N \times \mathcal{O}_2(\mathbb{R})$. Another argument is that the solution close to the regular centered triangles is expressed with algebraic numbers of degree 82. A web page was created to collect all the data: `http://www-salsa.lip6.fr/~jcf/vortices/`

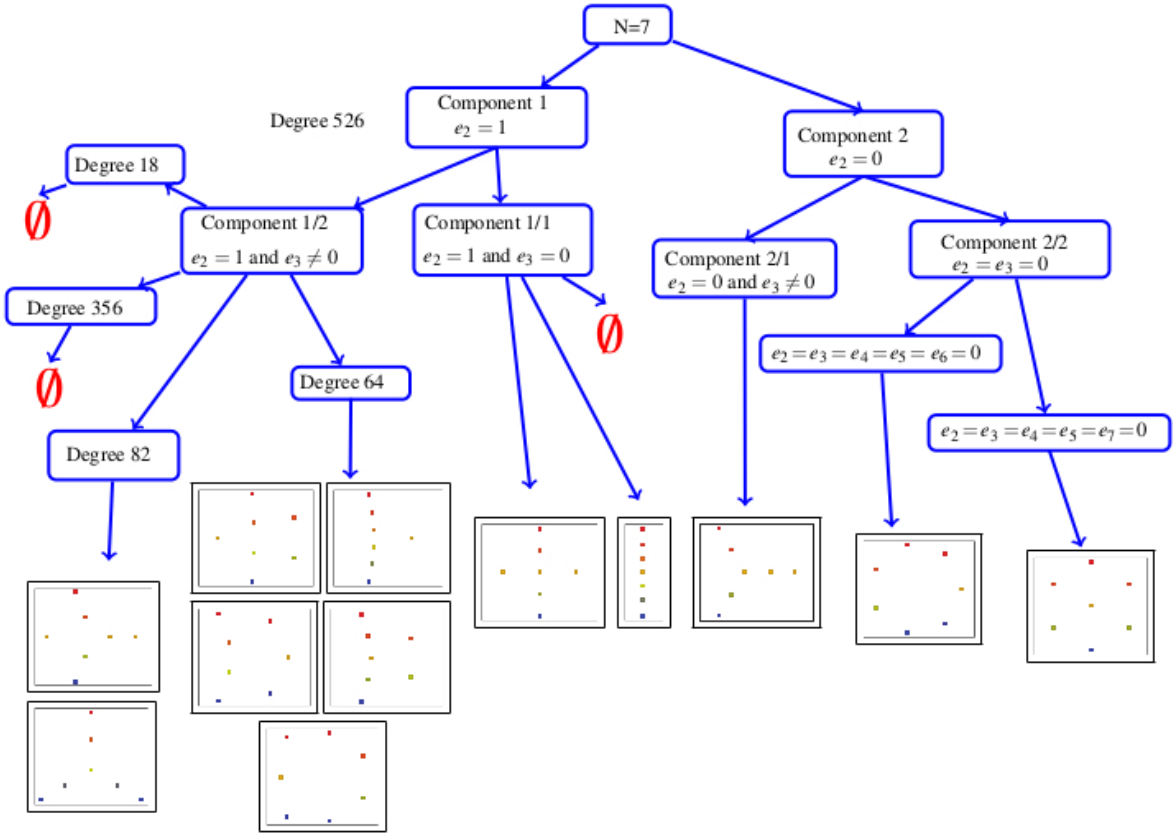


Figure 4.43 – The set of solutions for $N = 7$

4.2 Solving Systems Invariant under the Action of an Abelian Group in the Non-Modular Case

Introduction

This work is a common work with Jean-Charles Faugère and whas published in the proceedings of the ISSAC' 13 conference.

Problem Statement. The underlying algebraic problem studied in this section is to compute the variety $\mathbb{V}(\mathcal{I})$ associated to an ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ that is *globally stable* under the action a finite matrix group $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{K})$, as in the previous section. However, the group acting in the previous section was the whole symmetric group and in this section we focus on abelian groups. We will also assume that the action is *non-modular*: the characteristic of $\mathbb{K}$ does not divide $|\mathbf{G}|$.

Related Work. This problem is not new and has already been studied by some authors. The common idea is that, since the group $\mathbf{G}$ is commutative and the action non-modular, all matrices of $\mathbf{G}$ can be diagonalized with the same base-change matrix. Thus, up to some linear change of variables, we obtain an ideal $\mathcal{I}^{\mathcal{D}}$ invariant under a diagonal group $\mathbf{G}^{\mathcal{D}}$ isomorphic to $\mathbf{G}$. To our knowledge, the first author who proposed this idea in a Gröbner bases context was Gatermann in [51]. In this article, she shows why diagonalizing the group $\mathbf{G}$ and applying the linear change of variables on the input polynomials is interesting: some structure is maintained while computing a Gröbner basis of $\mathcal{I}^{\mathcal{D}}$ with Buchberger algorithm (see [51, Theorem 7]). She observed that the polynomials occuring during the execution of Buchberger algorithm remain sparse. More recently, Steidel [96] proposed to use such a diagonalization, compute a Gröbner basis of $\mathcal{I}^{\mathcal{D}}$, apply the reverse change of variables on this Gröbner basis and compute a Gröbner basis of $\mathcal{I}$ again. The idea of diagonalizing the group $\mathbf{G}$ and using the action of $\mathbf{G}^{\mathcal{D}}$ on $\mathbb{K}[X]$ has already been used in invariant theory, in order to find a decomposition $\mathbb{K}[X]^{\mathbf{G}} = \bigoplus_{i=1}^{t} \eta_i \mathbb{K}[\theta_1, \ldots, \theta_n]$ (see for example [100]) or more recently (after that this work was published) by Hubert and Labahn to find a decomposition $\mathbb{K}(x_1, \ldots, x_n)^{\mathbf{G}} = \mathbb{K}(\theta_1, \ldots, \theta_n)$ in [61]. However, to the best of our knowledge, the impact of the diagonalization on the complexity of Gröbner bases computations has not been investigated.

Main results. We present efficient algorithms together with complexity analysis to solve such polynomial systems which are *globally invariant* under the action of any *commutative* group $\mathbf{G}$. The algorithms are based on three main ideas: the first one is the diagonalization of $\mathbf{G}$ into $\mathbf{G}^{\mathcal{D}}$. Thus, up to some linear change of variables, we obtain an ideal $\mathcal{I}^{\mathcal{D}}$ invariant under a diagonal group $\mathbf{G}^{\mathcal{D}}$ isomorphic to $\mathbf{G}$.

The second idea is to introduce a grading on $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ given by the group $\mathbf{G}^{\mathcal{D}}$. This grading exists for every finite group H and is indexed on $X(H)$, the set of irreducible linear representations of the group H, and has been presented in chapter 3. In our case, since $\mathbf{G}^{\mathcal{D}}$ is diagonal, the set $X(\mathbf{G}^{\mathcal{D}})$ is isomorphic to $\mathbf{G}^{\mathcal{D}}$ and the isotypic components are generated by monomials. Therefore, we introduce the notion of $\mathbf{G}$-degree of a polynomial: assuming that $\mathbf{G}^{\mathcal{D}}$ is generated by diagonal matrices $\mathrm{Diag}(\beta_{i,1}, \ldots, \beta_{i,n})$ of order q_i with $q_1|q_2|\ldots|q_\ell = e$ and that β is a primitive e-root of 1, we say that a polynomial $f \in \mathbb{K}[X]$ is $\mathbf{G}$-homogeneous of $\mathbf{G}$-degree $(d_1, \ldots, d_\ell) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_\ell}$ if $f(\beta_{i,1}x_1, \cdots, \beta_{i,n}x_n) = \beta^{d_i \frac{e}{q_i}} f(x_1, \ldots, x_n)$ for all i.

Taking into account that the operation of taking the S-polynomial preserves this grading, the final idea is to observe that this can be used to speed up the Gröbner basis computation.

More precisely, Macaulay matrix can be decomposed into $|\mathbf{G}^{\mathcal{D}}|$ smaller *independent* matrices, being roughly the same size. In particular, this allows us to split the matrices arising in classical Gröbner basis algorithms based on linear algebra like Macaulay/Lazard algorithm (algorithm 1.40), F_4 [34] or F_5 (algorithm 1.44). Therefore, the complexity (in time and in memory) of computing Gröbner bases of such invariant ideals can be decreased in both theory and practice. In the same way, in the case of a zero-dimensional ideal $\mathcal{I}^{\mathcal{D}}$, the canonical basis of the ring $\mathbb{K}[X]/\mathcal{I}^{\mathcal{D}}$ can also be decomposed in monomials having same $\mathbf{G}$-degree and thus we are able to split the multiplication matrices arising in FGLM (algorithm 1.52).

In addition, this grading can be used to transform very easily a globally invariant problem into a problem for which all the equations are $\mathbf{G}$-homogeneous: we show that for each original equation f we can take the $\mathbf{G}$-homogeneous components of f.

We have implemented, in the computer algebra system Magma, "abelian" versions of the F_5 and FGLM algorithms that run several times faster, compared to the same implementation of these classical algorithms. For example, applying FGLM on the Cyclic-10 problem (a system with 34940 solutions), instead of computing 10 multiplication square matrices of size 34940×34840, our algorithm computes 900 quasi-square matrices of size at most 354.

In order to compare similar implementations, we have implemented an "abelian" version of F_4 [34] in FGb (C language): computing a Gröbner basis of the Cyclic-10 problem is about 410 times faster with the new approach. Moreover, a grevlex Gröbner basis for the Cyclic-11 problem (184756 solutions) can be computed in less than 8 hours. We also demonstrate that our approach has a significant impact in other fields: NTRU is a well known cryptosystem and the underlying problem can easily be modeled by quadratic equations which are left globally invariant by the action of a cyclic group. We observe a factor of 250 in favor of the new approach for small size problems and more importantly we can solve previously untractable problems. Surprisingly, during these experiments, the linear algebra parts (that is building the matrices and the gaussian elimination parts) can sometimes be so accelerated that the management of the list of critical pairs becomes the most time-consuming part whereas it is usually negligible.

More generally, the algorithms given in this paper can also be used for other kinds of structured polynomial systems like quasi-homogeneous or multi-homogeneous polynomials.

Perspectives. Several further developments can be made on the subject: the Abelian-F_5 and Abelian-FGLM algorithms have to be implemented in C, and it seems possible to obtain a parallelized version of the Abelian-FGLM algorithm. We have already identified new classes of invariant problems which can be solved in polynomial time; for other classes of problems the degree reached during the Gröbner basis computation is much lower than expected. It appears that this lower degree is more a consequence of the sparsity of the support of the polynomials (after change of variables) rather than a consequence of the invariance under the action of a group. The study of those sparse systems is a work in progress and part of this work will be presented in chapter 5.

Organization of the section. The organization of the section is as follows: in subsection 4.2.1, we recall classical notations and explain the relations between the ideals I and $\mathcal{I}^{\mathcal{D}}$, and the matrix groups $\mathbf{G}$ and $\mathbf{G}^{\mathcal{D}}$. In subsection 4.2.2, we explain the grading induced by the diagonal matrix group $\mathbf{G}^{\mathcal{D}}$, and introduce the notion of $\mathbf{G}$-degree of monomials and polynomials. The vector space generated by all monomials having same $\mathbf{G}$-degree is nothing else than an *isotypic component* ([94]) but since the formulation is simpler in the case of a diagonal group, we introduce the notion of $\mathbf{G}$-degree of monomials and $\mathbf{G}$-homogeneous polynomials.

Subsections 4.2.3 and 4.2.4 provide variants of the F_5 and FGLM algorithms. The complexity questions are answered in subsection 4.2.5, and benchmarks are made in subsection 4.2.6.

4.2.1 Linear change of variables

From now on we assume that $\mathbf{G}$ is a finite abelian subgroup of $\mathcal{GL}_n(\mathbb{K})$, with $\mathbb{K}$ a field of characteristic 0 or p such that p and $|\mathbf{G}|$ are coprime. We first prove that, within a linear change of variables, we can assume that the group $\mathbf{G}$ is a *diagonal group*, meaning that all matrices in $\mathbf{G}$ are diagonal matrices.

We start by recalling the following theorem, that describes the structure of finite abelian groups.

Theorem 4.44 (Classification of finite abelian groups)**.** *Any finite abelian group is uniquely isomorphic to a product $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1 | \dots | q_\ell$.*

Definition – Proposition 4.45. *Following the notations of the previous theorem, the integer $e = q_\ell$ is called the* exponent *of the group and is the lowest common multiple of the orders of the elements of the group.*

Recall that $\mathrm{char}(\mathbb{K})$ does not divide $|\mathbf{G}|$, therefore $\mathrm{char}(\mathbb{K})$ does not divide the exponent of $\mathbf{G}$ either. Hence, the polynomial $x^e - 1$ is separable on $\mathbb{K}$. It follows that, over $\bar{\mathbb{K}}$, $x^e - 1$ is separated.

Notations 4.46. *We will denote by e the exponent of $\mathbf{G}$ and by ξ a primitive e-root of 1 in bar$\mathbb{K}$. We will now consider the field $\mathbb{K}(\xi)$.*

The following theorem will allow us to assume that the matrix group $\mathbf{G}$ is diagonal, since it turns out that on $\mathbb{K}(\xi)$ the matrices of $\mathbf{G}$ can be diagonalized, with the same base-change matrix.

Theorem 4.47. *The matrix group $\mathbf{G}$ is diagonalizable over $\mathbb{K}(\xi)$, meaning that there exists a matrix P in $\mathcal{GL}_n(\mathbb{K}(\xi))$, such that the group $\mathbf{G}^{\mathcal{D}} = P^{-1}\mathbf{G}P = \{P^{-1}AP \mid A \in \mathbf{G}\}$ is a diagonal group.*

Although this theorem is very classical, we give the proof. To this end, we first give a lemma

Lemma 4.48. *Let $\mathbb{F}$ be a field and E be a $\mathbb{F}$-vector space of finite positive dimension. Let $(f_i)_{i\in I}$ be a commutative family of diagonalizable endomorphisms of E, which means that:*
- *for all $i, j \in I$, $f_i \circ f_j = f_j \circ f_i$.*
- *for each i, there exists a basis $\mathcal{B}_i$ of E such that the matrix of f_i in $\mathcal{B}_i$ is diagonal.*

Then, there exists a basis $\mathcal{B}$ of E such that the matrices of all f_i in $\mathcal{B}$ are diagonal.

Proof. This lemma is so classical, that it is hard to put a reference on it. The proof can be done by induction on $\dim_{\mathbb{F}}(E)$, the dimension of E:
- If $\dim_{\mathbb{F}}(E) = 1$, then every basis of E concurs.
- Assume now that the lemma has been proved for every dimension between 1 and $\dim_{\mathbb{F}}(E) - 1 \geq 1$. We distinguish to cases:
  - If all (f_i) are uniform scalings, then every basis of E concurs and there is nothing to prove.

— Otherwise, at least one of the endomorphism f_{i_0} is not a uniform scaling. Since f_{i_0} is diagonalizable, the vector space E admits a decomposition $E = \bigoplus_{\lambda \in \mathrm{Sp}(f_{i_0})} E_\lambda$ where $\mathrm{Sp}(f_{i_0})$ is the spectrum of f_{i_0}, which contains at least two elements of $\mathbb{F}$ since f_{i_0} is not a uniform scaling. Let $i \in I \backslash \{i_0\}$ and $v \in E_\lambda$. Then

$$\lambda f_i(v) = f_i(f_{i_0}(v)) = f_{i_0}(f_i(v)) \qquad \text{since } f_i \text{ and } f_{i_0} \text{ commute.}$$

Therefore, $f_i(v) \in E_\lambda$, which proves that every f_i stabilizes the eigenspaces (E_λ). Then, for each $\lambda \in \mathrm{Sp}(f_{i_0})$, $(f_{i_{|E_\lambda}})_{i \in I \backslash \{i_0\}}$ is a commutative family of diagonalizable endomorphisms of E_λ. By induction, there exist a basis $\mathcal{B}_\lambda$ of each eigenspace E_λ, such that the matrices of $(f_{i_{|E_\lambda}})_{i \in I \backslash \{i_0\}}$ in $\mathcal{B}_\lambda$ are diagonal. Hence $\mathcal{B} = \cup_\lambda \mathcal{B}_\lambda$ is a basis of E, such that the matrices of $(f_i)_{i \in I}$ in $\mathcal{B}$ are diagonal.

— By induction, the lemma is proved.

□

Proof of theorem 4.47. Every matrix $A \in \mathbf{G}$ satisfies the polynomial $X^e - 1$, which fully splits in $\mathbb{K}(\xi)$ and has simple roots since $\mathrm{char}(\mathbb{K}) \nmid |\mathbf{G}|$, so every matrix of $\mathbf{G}$ is diagonalizable. Therefore, by lemma 4.48, the endomorphisms associated to the matrices of $\mathbf{G}$ can be diagonalized in the same basis of $\mathbb{K}(\xi)^n$. This leads to the existence of a matrix $P \in \mathcal{GL}_n(\mathbb{K}(\xi))$ such that $P^{-1}AP$ is diagonal for every matrix $A \in \mathbf{G}$. Hence, $\mathbf{G}^{\mathcal{D}} = P^{-1}\mathbf{G}P = \{P^{-1}AP \mid A \in \mathbf{G}\}$ is a diagonal group. □

Example 4.49. *Throughout this section, we will consider often the representation in $\mathcal{GL}_n(\mathbb{K})$ of C_n, the subgroup of $\mathfrak{S}_n$ generated by the n-cycle $\sigma = (12 \dots n)$. With this representation, C_n is generated by the following matrix M_σ:*

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

With $\mathbb{K}$ a field of characteristic 0 or coprime with n and ξ a primitive n-root of 1 in $\bar{\mathbb{K}}$, the group C_n is diagonalizable with the base-change matrix $P = (\xi^{ij})_{i,j \in \{1,\dots,n\}}$. In particular, the matrix M_σ associated to the cycle $(1 \dots n)$ becomes the diagonal matrix $D_\sigma = P^{-1}M_\sigma P = \mathrm{Diag}(\xi, \dots, \xi^{n-1}, 1)$.

We now study this change of variables on ideals invariant under the action of $\mathbf{G}$.

Proposition 4.50. *Let $\mathcal{I} = \langle f_1, \dots, f_s \rangle_{\mathbb{K}[X]}$ be a $\mathbf{G}$-stable ideal in $\mathbb{K}[X]$, and let $\mathbf{G}^{\mathcal{D}}$ and P be the diagonal group and the base-change matrix obtained in theorem 4.47. Then $\mathcal{I}^{\mathcal{D}} = \langle f_1^P, \dots, f_s^P \rangle_{\mathbb{K}(\xi)[X]}$ is an ideal of $\mathbb{K}(\xi)[X]$ stable under $\mathbf{G}^{\mathcal{D}}$.*

Proof. Since $\mathbf{G}$ is a finite group, the orbit of $f \in \mathcal{I}$ under $\mathbf{G}$, which is $\{f^A \mid A \in \mathbf{G}\}$, is finite. Therefore, up to enlarging $\{f_1, \dots, f_s\}$, we can assume that for every i in $\{1, \dots, s\}$ and $A \in \mathbf{G}$, f_i^A is one of the $\{f_j\}$. Let B in $\mathbf{G}^{\mathcal{D}}$. Then, B can be written $B = P^{-1}AP$ with $A \in \mathbf{G}$. It follows that for every i in $\{1, \dots, s\}$,

$$(f_i^P)^B = (f_i^P)^{P^{-1}AP} = f_i^{PP^{-1}AP} = f_i^{AP} = f_j^P \qquad \text{with } f_j = f_i^A.$$

Since $\{f_1^P, \dots, f_s^P\}$ is a stable set of polynomials under the action of $\mathbf{G}^{\mathcal{D}}$, $\mathcal{I}^{\mathcal{D}}$ is a $\mathbf{G}$-stable ideal. □

Example 4.51. *To illustrate the definition, we will use the well known* Cyclic-n problem. *The ideal I of $\mathbb{K}[X]$ is generated by:*

$$\begin{cases} h_1 = x_1 + \cdots + x_n \\ h_2 = x_1x_2 + x_2x_3 + \cdots + x_nx_1 \\ \vdots \\ h_{n-1} = x_1x_2\ldots x_{n-1} + x_2\ldots x_nx_1 + \cdots + x_nx_1\ldots x_{n-2} \\ h_n = x_1x_2\ldots x_{n-1}x_n - 1 \end{cases}$$

The ideal I is obviously invariant under the cyclic group C_n, since each h_i satisfies $h_i^{M_\sigma} = h_i$, with M_σ defined in exemple 4.49. It is also stable under the scalar matrix ξI_n with ξ a primitive n-root of 1, since $h_i^{\xi I_n} = \xi^i h_i$. Hence, the system is globally invariant under the group $\mathbf{G}$ generated by M_σ and ξI_n. With P the matrix given in example 4.49, $\mathbf{G}^{\mathcal{D}} = P^{-1}\mathbf{G}P$, generated by D_σ and ξI_n, is a diagonal group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We denote by f_i the polynomials h_i^P, which generate $\mathcal{I}^{\mathcal{D}}$: for instance, when $n = 3$, the polynomials f_i are:

$$\begin{cases} f_1 = 3x_3 \\ f_2 = -3x_1x_2 + 3x_3^2 \\ f_3 = x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3 - 1 \end{cases}$$

Observe that for all n, the polynomial f_1 in the Cyclic-n problem is always equal to $n\,x_n$, since $P \times {}^t(1,\ldots,1) = {}^t(0,\ldots,0,n)$. Hence, for this problem, it is easy to remove one variable after diagonalization.

4.2.2 Grading induced by a diagonal matrix group

From now on, we assume that $\mathbf{G}$ is a diagonal matrix group on a field $\mathbb{K}$, isomorphic to $\prod_{i=1}^{\ell} \mathbb{Z}/q_i\mathbb{Z}$ with $q_1|\ldots|q_\ell = e$. It follows that $\mathbb{K}$ contains a primitive e-root of 1, which will be denoted by ξ.

Isotypic components given by monomials. We now show that a basis of each isotypic component of the representation $\mathbb{K}[X]_d$ of $\mathbf{G}$ consists in monomials. We define the $\mathbf{G}$-degree of a monomial m, which is a practical way to identify the isotypic component of m. This $\mathbf{G}$-degree induces a grading of $\mathbb{K}[X]$ given by the isomorphism $\mathbf{G} \simeq \widehat{\mathbf{G}} \simeq \prod \mathbb{Z}/q_i\mathbb{Z}$.

Since $\mathbf{G}$ is isomorphic to $\prod_{i=1}^{\ell} \mathbb{Z}/q_i\mathbb{Z}$, let ϕ be an explicit isomorphism

$$\begin{array}{rccc} \phi: & \mathbf{G} & \longrightarrow & \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z} \\ & D & \longmapsto & \phi(D) \end{array}$$

and let D_i be the preimage of $(0,\ldots,0,\underset{i}{1},0,\ldots,0)$, so D_i generates a subgroup of $\mathbf{G}$ of cardinality $|q_i|$.

Example 4.52. *With $\mathbf{G}$ the group arising in the previous example 4.51, we take ϕ such that $\phi(D_\sigma) = (1,0) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\phi(\xi I_n) = (0,1)$.*

Proposition 4.53. *For every monomial $m \in \mathcal{M}$ and for each i, there exists a unique $\mu_i \in \{0,\ldots,q_i-1\}$ such that $m^{D_i} = \xi^{\frac{e}{q_i}\mu_i} m$.*

Proof. Let $m = \prod_{j=1}^{n} x_j^{\alpha_j}$ and $D_i = Diag(\beta_1, \ldots, \beta_n)$. Since D_i has order q_i, the coefficients β_j are q_i-roots of 1, so can be denoted $\xi^{\ell_j \frac{e}{q_i}}$. Then

$$m^{D_i} = (\beta_1 x_1)^{\alpha_1} \times \cdots \times (\beta_n x_n)^{\alpha_n} = \left(\prod_{j=1}^{n} \beta_j^{\alpha_j} \right) m = \xi^{\frac{e}{q_i} \sum_{j=1}^{n} \ell_j \alpha_j} m$$

Then we can take $\mu_i = \sum \ell_j \alpha_j \bmod q_i$. Since ξ has order e, $\xi^{\frac{e}{q_i}}$ has order q_i and the unicity of μ_i is clear. □

Instead of considering μ_i in $\{0, \ldots, q_i - 1\}$, we take μ_i in $\mathbb{Z}/q_i\mathbb{Z}$, which makes sense since $\xi^{\frac{e}{q_i}}$ has order q_i.

Definition 4.54. *The k-tuple $(\mu_1, \ldots, \mu_\ell) \in \prod_{i=1}^{\ell} \mathbb{Z}/q_i\mathbb{Z}$ is said to be the* $\mathbf{G}$-degree *of m and is denoted $\mathsf{deg}_{\mathbf{G}}(m)$, although it depends on the choice of the matrices D_i (more exactly, the choice of ϕ). We denote by $\mathcal{D}(\mathbf{G}) = \prod \mathbb{Z}/q_i\mathbb{Z}$ the set of all $\mathbf{G}$-degrees.*

The relation between the $\mathbf{G}$-degrees and the characters of $\mathbf{G}$ can be explained easily. From theorem 3.70, we know that $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$. An explicit isomorphism is given by the following application:

$$\aleph : \begin{array}{ccc} \mathbf{G} & \longrightarrow & \widehat{\mathbf{G}} \\ D_i & \longmapsto & \chi_i \end{array} \qquad \text{where} \quad \chi_i : \begin{array}{ccc} \mathbf{G} & \longrightarrow & \mathbb{K}^* \\ D_j & \longmapsto & \begin{cases} \xi^{e/q_i} & \text{if } j = i \\ 1 & \text{otherwise.} \end{cases} \end{array}$$

Proposition 4.55. *With previous notations, any monomial m is of $\mathbf{G}$-degree $(\mu_1, \ldots, \mu_\ell)$ if and only if $m^D = \chi(D)m$ for all $D \in \mathbf{G}$, with $\chi = \prod_{i=1}^{\ell} \chi_i^{\mu_i}$.*

Proof. Let m be a monomial, and $D \in \mathbf{G}$. From the structure of $\mathbf{G}$, D can be uniquely written $\prod_{j=1}^{\ell} D_j^{\alpha_j}$, with $\alpha_j \in \mathbb{Z}/q_j\mathbb{Z}$. Then, with $\chi = \prod_{i=1}^{\ell} \chi_i^{\mu_i}$, we have

$$\chi(D) = \prod_{i=1}^{\ell} \chi \left(\prod_{j=1}^{\ell} D_j^{\alpha_j} \right) = \prod_{i=1}^{\ell} \left[\prod_{j=1}^{\ell} \chi_i(D_j)^{\alpha_j} \right]^{\mu_i} = \prod_{i=1}^{\ell} \xi^{\frac{e}{q_i} \alpha_i \mu_i}$$

Assume now that m is of $\mathbf{G}$-degree $(\mu_1, \ldots, \mu_\ell)$. Then for each i, $m^{D_i} = \xi^{\frac{e}{q_i} \mu_i}$, and $m^D = \chi(D)m$. The converse implication is obvious since we just have to set $D = D_i$ in the relation $m^D = \chi(D)m$. □

Remark 4.56. *It follows from proposition 3.83 that every $\mu \in \mathcal{D}(\mathbf{G})$ is the $\mathbf{G}$-degree of some monomials.*

To every monomial, we have associated a $\mathbf{G}$-degree. What is very interesting is that the set of monomials of a given $\mathbf{G}$-degree forms a basis of the isotypic component of the associated character, which follows from the following proposition:

Proposition 4.57. *For $D \in \mathbf{G}$, we denote by ρ_D the associated linear map on $\mathbb{K}[X]$. For all polynomial $f \in \mathbb{K}[X]$, we have $\rho_D(f) = f^D$. Then, for all monomial m in $\mathbb{K}[X]$, and $\chi = \prod_{i=1}^{\ell} \chi_i^{\mu_i}$, the following relation holds:*

$$p_\chi(m) = \begin{cases} m & \text{if } \mathsf{deg}_{\mathbf{G}}(m) = (\mu_1, \ldots, \mu_\ell) \\ 0 & \text{otherwise.} \end{cases}$$

where $p_\chi = \frac{1}{|\mathbf{G}|}\sum_{D\in\mathbf{G}} \chi(D)^{-1}\rho_D$ *is the projection on the isotypic component associated to* χ*, see theorem 3.65.*

Proof. Let χ_m be the character $\prod_{i=1}^{\ell}\chi_i^{\alpha_i}$, where $(\alpha_1,\dots,\alpha_\ell)$ is the $\mathbf{G}$-degree of m. Then $\rho_D(m) = \chi_m(D)m$ for all $D\in\mathbf{G}$, by proposition 4.55. It follows that

$$p_\chi(m) = \frac{1}{|\mathbf{G}|}\sum_{D\in\mathbf{G}} \chi^{-1}(D)\chi_m(D)m = m\left[\frac{1}{|\mathbf{G}|}\sum_{D\in\mathbf{G}}(\chi^{-1}\chi_m)(D)\right]$$

By theorem 3.59, $p_\chi(m) = m(\chi^{-1}\chi_m|\mathbf{1})$ is equal to m if and only if $\chi^{-1}\chi_m = \mathbf{1}$, and zero otherwise, which ends the proof. □

Proposition 4.58. *For all monomials* m, m' *in* $\mathbb{K}[X]$*, the* $\mathbf{G}$*-degrees of* m *and* m' *satisfy the relation* $\mathsf{deg}_{\mathbf{G}}(m) + \mathsf{deg}_{\mathbf{G}}(m') = \mathsf{deg}_{\mathbf{G}}(mm')$*.*

Proof. Let $i\in\{1,\dots,k\}$ and m, m' be two monomials. Let μ_i, μ_i' such that $m^{D_i} = \xi^{\frac{e}{q_i}\mu_i}m$ and $m'^{D_i} = \xi^{\frac{e}{q_i}\mu_i'}m'$. Then $(mm')^{D_i} = m^{D_i}m'^{D_i} = \xi^{\frac{e}{q_i}(\mu_i+\mu_i')}mm'$. Hence $\mathsf{deg}_{\mathbf{G}}(mm') = \mathsf{deg}_{\mathbf{G}}(m) + \mathsf{deg}_{\mathbf{G}}(m')$. □

Note that to compute $\mathsf{deg}_{\mathbf{G}}(m)$ with $m = \prod x_i^{\alpha_i}$, we just have to know $\mathsf{deg}_{\mathbf{G}}(x_i)$ since $\mathsf{deg}_{\mathbf{G}}(m) = \sum \alpha_i \mathsf{deg}_{\mathbf{G}}(x_i)$. This grading will be used to reduce the sizes of the matrices in the Diagonal-F_5 algorithm.

Remark 4.59. *If we denote by* $\mathcal{M}_{d,g}$ *the set of monomials of degree* d *and* $\mathbf{G}$*-degree* g*,* $\mathcal{M}_{d,g}\mathcal{M}_{d',g'} \subseteq \mathcal{M}_{d+d',g+g'}$ *for all* d, d', g, g'*. Therefore* $R = \bigoplus_{d\in\mathbb{N}, g\in\mathcal{D}(\mathbf{G})} Vect(\mathcal{M}_{d,g})$*.*

Example 4.60. *Let* $\mathbf{G}$ *be the matrix group generated by the diagonal matrix* $D_\sigma = Diag(\xi,\xi^2,1)$ *where* ξ *is a primitive third root of 1. Each* x_i *has* $\mathbf{G}$*-degree* i *mod* 3*, so* $m = \prod x_j^{\alpha_j}$ *has* $\mathbf{G}$*-degree* $\sum j\alpha_j$ *mod* 3*. Hence,* $x_1x_2x_3$ *(resp.* $x_1x_2^2$*) has* $\mathbf{G}$*-degree 0 (resp. 2).*

Example 4.61. *(cont. of example 4.51) The* $\mathbf{G}$*-degree of* x_i *is* $(i,1)$*.*

G-homogeneous polynomials. We now define a notion of $\mathbf{G}$-homogeneity, which follows directly from the grading induced by $\mathbf{G}$ on $\mathbb{K}[X]$. The cornerstone of the Abelian-F_5 algorithm (subsection 4.2.3) is that the S-polynomial of two $\mathbf{G}$-homogeneous polynomials is $\mathbf{G}$-homogeneous, which will be proved in theorem 4.64.

Definition 4.62. *A polynomial* f *in* $\mathbb{K}[X]$ *is said to be* $\mathbf{G}$-homogeneous *if all monomials of* f *share the same* $\mathbf{G}$*-degree* $(\mu_1,\dots,\mu_\ell)\in\mathcal{D}(\mathbf{G})$*. In this case, we set* $\mathsf{deg}_{\mathbf{G}}(f) = \mathsf{deg}_{\mathbf{G}}(\mathsf{LM}(f))$*.*

In other words, a polynomial is $\mathbf{G}$-homogeneous if it lies in an isotypic component $\mathbb{K}[X]_\chi$ of $\mathbb{K}[X]$, viewed as a representation of $\mathbf{G}$. Since a polynomial in $\mathbb{K}[X]$ can be written $\sum_{\mu\in\mathcal{D}(\mathbf{G})} f_\mu$, with f_μ a $\mathbf{G}$-homogeneous polynomial of $\mathbf{G}$-degree μ, we call f_μ the $\mathbf{G}$*-homogeneous component of* f *of* $\mathbf{G}$*-degree* μ*.*

Proposition 4.63. *If* f *is* $\mathbf{G}$*-homogeneous and* m *is a monomial, then* mf *is* $\mathbf{G}$*-homogeneous. Moreover,* $\mathsf{deg}_{\mathbf{G}}(mf) = \mathsf{deg}_{\mathbf{G}}(m) + \mathsf{deg}_{\mathbf{G}}(f)$*.*

Proof. For any monomial $\tilde{m}$ of f, $\mathsf{deg}_{\mathbf{G}}(\tilde{m}m) = \mathsf{deg}_{\mathbf{G}}(\tilde{m}) + \mathsf{deg}_{\mathbf{G}}(m) = \mathsf{deg}_{\mathbf{G}}(f) + \mathsf{deg}_{\mathbf{G}}(m)$, so all monomials of mf share the same $\mathbf{G}$-degree $\mathsf{deg}_{\mathbf{G}}(f) + \mathsf{deg}_{\mathbf{G}}(m) = \mathsf{deg}_{\mathbf{G}}(mf)$. □

It follows that the product of two **G**-homogeneous polynomials is also a **G**-homogeneous polynomial. Hence, $\mathbb{K}[X]$ is a *graded algebra*, in the sense of definition 2.12. Moreover, since each component is generated by monomials, it follows that the S-polynomial of two **G**-homogeneous polynomials is also **G**-homogeneous.

Theorem 4.64. *Let f, g be two* **G***-homogeneous polynomials of R_K. The S-polynomial of (f, g) (see definition 1.29) is* **G***-homogeneous of* **G***-degree $\mathsf{deg}_{\mathbf{G}}(\mathsf{LM}(f) \vee \mathsf{LM}(g))$, where $\mathsf{LM}(f) \vee \mathsf{LM}(g)$ denotes the lowest common multiple of $\mathsf{LM}(f)$ and $\mathsf{LM}(g)$.*

Proof. Since $\mathsf{LM}(f)$ and $\mathsf{LM}(g)$ divide $\mathsf{LM}(f) \vee \mathsf{LM}(g)$, both fractions

$$\frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(f)} \quad \text{and} \quad \frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(g)}$$

are monomials, therefore by previous proposition,

$$\frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(g)} \frac{\mathsf{LC}(f)}{\mathsf{LC}(g)} g \quad \text{and} \quad \frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(f)} f$$

are two **G**-homogeneous polynomials. Moreover, they share the same leading monomial, so they have same **G**-degree, which is the **G**-degree of $S(f, g)$. We actually proved that $\mathsf{deg}_{\mathbf{G}}(S(f, g)) = \mathsf{deg}_{\mathbf{G}}(\mathsf{LM}(f) \vee \mathsf{LM}(g))$. □

Example 4.65. *Following example 4.51, it appears that each f_i has* **G***-degree $(0, i) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ under* **G** *generated by D_σ and ξI_n.*

G-homogeneous ideals. We now consider ideals generated by **G**-homogeneous polynomials. Let $\mathcal{I}$ be a **G**-stable ideal generated by $f_1, \ldots, f_s$. A Gröbner basis computation preserves the **G**-degree, but the polynomials f_i are not necessarily **G**-homogeneous. Our aim here is to prove that the **G**-homogeneous components of the f_i are in $\mathcal{I}$, and so to compute a Gröbner basis of $\mathcal{I}$, we take the **G**-homogeneous components of generators of $\mathcal{I}$ as inputs. This operation has a negligible cost since at each degree d, the abelian-F_5 algorithm (presented in the next subsection) separates $\mathcal{M}_d$, the sets of monomials of degree d, into subsets $\mathcal{M}_{d,g}$ of same **G**-degree g.

Definition 4.66. *An ideal $\mathcal{J}$ of $\mathbb{K}[X]$ is said to be* **G**-homogeneous *if it is generated by* **G***-homogeneous polynomials.*

The previous definition follows the general definition of a homogeneous ideal in a graded algebra given in definition 2.13. An interesting result is that the notion of **G**-homogeneous and **G**-stable ideal are the same.

Theorem 4.67. *Let $\mathcal{J}$ be an ideal of $\mathbb{K}[X]$. Then, the following properties are equivalent.*

(1) $\mathcal{J}$ is **G***-homogeneous.*

(2) $\mathcal{J}$ is **G***-stable.*

(3) For all $f \in \mathcal{J}$, the **G***-homogeneous components of f also belong to $\mathcal{J}$.*

Proof. (1)$\Longrightarrow$(2). Let $f \in \mathcal{J}$. Then, $f = \sum_i h_i f_i$ with f_i a **G**-homogeneous polynomial. Hence, for all $D \in \mathbf{G}$, $f^D = \sum_i h_i^D f_i^D$. Since f_i is **G**-homogeneous, the polynomial f_i is equal to $\lambda_i f_i$ with λ_i a suitable root of 1. Hence, $\mathcal{J}$ is **G**-stable.

(2)$\Longrightarrow$(3). For all $\chi \in \widehat{\mathbf{G}}$, the projection on the isotypic component associated to χ is given by $p_\chi(f) = \frac{1}{|\mathbf{G}|}\sum_{D\in\mathbf{G}} \chi(D)^{-1} f^D$. If $f \in \mathcal{J}$ all f^D belong to $\mathcal{J}$ since $\mathcal{J}$ is $\mathbf{G}$-stable. It follows that all $\mathbf{G}$-homogeneous components of f belong to $\mathcal{J}$.
(3)$\Longrightarrow$(1). If $f_1, \ldots, f_s$ is a generating set of $\mathcal{J}$, it is clear that the $\mathbf{G}$-homogeneous components of $f_1, \ldots, f_s$ also generate $\mathcal{J}$, and they are $\mathbf{G}$-homogeneous. □

Example 4.68. *Let $\mathbf{G}$ be the diagonal group of order 2 generated by the matrix $Diag(-1, 1)$, acting on $R = k[x_1, x_2]$. Assume that $x_1^3x_2 + x_1^2x_2^2 - x_1 + 1 \in \mathcal{I}$, with $\mathcal{I}$ a $\mathbf{G}$-stable ideal. Then since $\mathsf{deg}_{\mathbf{G}}(x_i) = i$ mod 2, $\mathsf{deg}_{\mathbf{G}}(x_1^3x_2) = \mathsf{deg}_{\mathbf{G}}(x_1) = 1$ and $\mathsf{deg}_{\mathbf{G}}(1) = \mathsf{deg}_{\mathbf{G}}(x_1^2x_2^2) = 0$, so $x_1^3x_2 - x_1$ and $x_1^2x_2^2 + 1$ belong to $\mathcal{I}$.*

We end up this subsection with a quite obvious but useful property, which will be used in subsection 4.2.5.

Proposition 4.69. *Let $\mathbf{G}$ be a diagonal matrix group acting on $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$. Then the $\mathbf{G}$-degrees of the variables $x_1, \ldots, x_n$ span the group of $\mathbf{G}$-degrees $\mathcal{D}(\mathbf{G})$.*

Proof. If m is a monomial, m can be written $\prod x_i^{\alpha_i}$. Then $\mathsf{deg}_{\mathbf{G}}(m)$ belongs to the subgroup spanned by the $\mathbf{G}$-degrees of the variables. But from proposition 3.83, it follows that for each $\mathbf{G}$-degree, there exists a monomial having this $\mathbf{G}$-degree. □

4.2.3 Abelian Matrix-F_5 algorithm

We are now able to describe a variant of the Matrix-F_5 algorithm (algorithm 1.44), which takes advantage of the action of the diagonal group $\mathbf{G}$. Let $\mathcal{I}$ be a $\mathbf{G}$-stable ideal, with $\mathbf{G}$ a diagonal group isomorphic to $\mathcal{D}(\mathbf{G})$, the group of $\mathbf{G}$-degrees. Let $f_1, \ldots, f_s$ be $\mathbf{G}$-homogeneous polynomials generating $\mathcal{I}$ (according to theorem 4.67). Any computation of the reduced Gröbner basis of $\mathcal{I}$ would implicitly use the grading $\mathbb{K}[X] = \bigoplus_{g\in\mathcal{D}(\mathbf{G})} \mathbb{K}[X]_g$ since it computes S-polynomials. The key of the Abelian-F_5 algorithm is the following : the polynomials f_i are $\mathbf{G}$-homogeneous, and also the polynomials $m_\mu f_i$. Therefore, in one Macaulay matrix appearing in the classical Matrix-F_5 algorithm, the only non-zero coefficients of the row indexed by $m_\mu f_i$ are on columns indexed by monomials having same $\mathbf{G}$-degree. So, instead of building one Macaulay matrix $M_{d,i}$, we will construct $|\mathbf{G}|$ matrices $M_{d,i,g}$, for all $g \in \mathcal{D}(\mathbf{G})$. This idea leads to algorithm 4.70.

At each degree d, the algorithm builds $|\mathbf{G}|$ matrices $M_{d,i,g}$ and performs row reduction on them, in order to obtain $\widetilde{M}_{d,i,g}$. The columns of $M_{d,i,g}$ are indexed by all monomials of degree d and $\mathbf{G}$-degree g, sorted for an ordering (for example the grevlex ordering). The rows contain the writing of all products $m \times f_j$ with $j \leq i$ and m monomials of degree $d - d_i$ and $\mathbf{G}$-degree $g - g_i$, except those which have been removed by the F_5 criterion. This criterion (lemma 1.45) applies straightforwardly in this case, the only change is that the monomial m can only be found in $M_{d-d_i,i-1,g-g_i}$. Note that all the loops on $g \in \mathcal{D}(\mathbf{G})$ are independent, so at each degree d, it is possible to parallelize the computations of row-echelon forms on $|G|$ different processors to speed up the computations. Assuming that there are no uniform scalings in $\mathbf{G}$, we will see in the complexity subsection 4.2.5 that this allows a theoretical speed-up of $|\mathbf{G}|^\omega$ compared to the classial Matrix-F_5 algorithm, which appears also in practice, see subsection 4.2.6. In the affine case, this speed-up appears without restriction on $\mathbf{G}$.

4.2.4 Abelian-FGLM algorithm

In this subsection, we explain how to take advantage of the $\mathbf{G}$-grading to speed up the change of ordering, using a variant of the classical FGLM algorithm 1.52. We assume that

Algorithm 4.70: Abelian Matrix-F_5 algorithm

Input : The set $\mathcal{D}(\mathbf{G})$ of $\mathbf{G}$-degrees, homogeneous and $\mathbf{G}$-homogeneous polynomials $(f_1, \ldots, f_s)$ with degrees $d_1 \leq \ldots \leq d_s$ and $\mathbf{G}$-degrees $g_1, \ldots, g_s$, a maximal degree D

Output: Gröbner Bases of $(f_1, \ldots, f_i)$ for $i = 1, \ldots, s$ up to degree D

for $i = 1$ **to** s **do** $\mathcal{G}_i := \emptyset$;

for $d = d_1$ **to** D **do**

  for $g \in \mathcal{D}(\mathbf{G})$ **do**

    $\widetilde{M}_{d,0,g} := \emptyset$;

    for $i = 1$ **to** s **do**

      if $d < d_i$ **then**

        $M_{d,i,g} := \widetilde{M}_{d,i-1,g}$

      else

        $M_{d,i,g}$:= matrix obtained by adding new rows $m.f_i$ to $\widetilde{M}_{d,i-1,g}$, for all monomials m of degree $d - d_i$ and $\mathbf{G}$-degree $g - g_i$ that do not appear as leading monomial of a row of $\widetilde{M}_{d-d_i,i-1,g-g_i}$.

      Compute $\widetilde{M}_{d,i,g}$ by Gaussian elimination from $M_{d,i,g}$;

      Add to $\mathcal{G}_i$ all rows of $\widetilde{M}_{d,i,g}$ not top-reducible by $\mathcal{G}_i$;

return $\mathcal{G}_1, \ldots, \mathcal{G}_s$

the dimension of the $\mathbf{G}$-stable ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ is equal to zero, and that a Gröbner basis $\mathcal{G}_{\preceq_1}$ for an ordering $\preceq_1$ (for instance the DRL ordering) of $\mathcal{I}$ has already been computed, and we are interested in computing the Gröbner basis of $\mathcal{I}$ for an other ordering $\preceq_2$ (for example, the lexicographical ordering). The idea of the Abelian-FGLM algorithm is exactly the same as algorithm 1.52: we pick up monomials m in $\mathbb{K}[X]$ by increasing order for $\preceq_2$, and look for linear combinations in $\mathbb{K}[X]/\mathcal{I}$ between the Normal Forms $\mathsf{NF}(m, \mathcal{G}_{\preceq_1})$. But the additional structure given by the grading by $\mathbf{G}$ allows us to split the matrices used to compute the Normal forms and test the linear dependency. Contrary to the original article [44], we make the choice here to insist on the point of view of representation theory. In proposition 2.14, we have seen that given an ideal $\mathcal{I}$ in a graded algebra $\mathcal{A}$, both $\mathcal{I}$ and $\mathcal{A}/\mathcal{I}$ have a decomposition into homogeneous components. This proposition applies in our case, with the $\mathbf{G}$-grading.

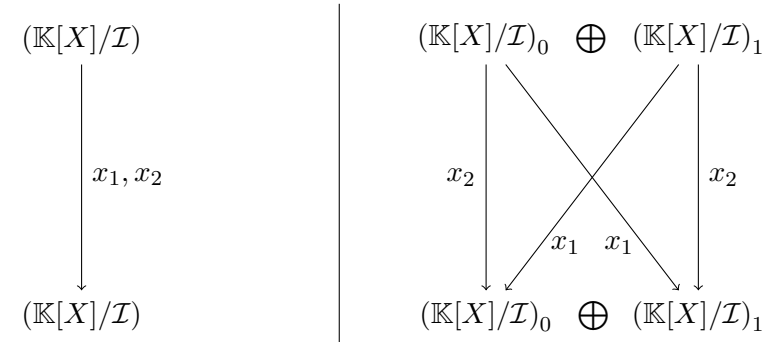
In the classical FGLM algorithm 1.52, the first step is to compute the matrices of the linear maps given by multiplication by the variables $x_1, \ldots, x_n$ in $\mathbb{K}[X]/\mathcal{I}$. But the decomposition

$$\mathbb{K}[X]/\mathcal{I} = \bigoplus_{g \in \mathcal{D}(\mathbf{G})} (\mathbb{K}[X]_g/\mathcal{I}_g)$$

and the fact that each variable x_i is $\mathbf{G}$-homogeneous allow us to decompose these linear maps into restricted maps

$$\mathbb{K}[X]_g/\mathcal{I}_g \xrightarrow{\times x_i} \mathbb{K}[X]_{g+\mathsf{deg}_{\mathbf{G}}(x_i)}/\mathcal{I}_{g+\mathsf{deg}_{\mathbf{G}}(x_i)}$$

Example 4.71. *Let $\mathbf{G}$ be the diagonal group of order 2 generated by the matrix $Diag(-1, 1)$, acting on $\mathbb{K}[x_1, x_2]$. The set of $\mathbf{G}$-degrees is equal to $\mathbb{Z}/2\mathbb{Z}$, and we have $\mathsf{deg}_{\mathbf{G}}(x_1) = 1$ and $\mathsf{deg}_{\mathbf{G}}(x_2) = 0$. If $\mathcal{I}$ is a $\mathbf{G}$-stable ideal, the linear maps of multiplication used in FGLM or Abelian-FGLM algorithms are the following:*



Multiplication with FGLM | *Multiplication with Abelian-FGLM*

As FGLM can be seen as a change of bases on the vector space of finite dimension $(\mathbb{K}[X]/\mathcal{I})$, Abelian-FGLM performs simultaneous change of bases on the isotypic components $(\mathbb{K}[X]/\mathcal{I})_g$ of the representation of $\mathbf{G}$ given by $\mathbb{K}[X]/\mathcal{I}$. For $g \in \mathcal{D}(\mathbf{G})$, we denote by $\mathcal{E}_g$ the set of $\mathbf{G}$-homogeneous monomials of degree g that are not reducible by $\mathcal{G}_{\preceq_1}$, and $\delta_g = |\mathcal{E}_g|$ will denote the dimension of $(\mathbb{K}[X]/\mathcal{I})_g$, as a $\mathbb{K}$-vector space. Therefore, $\delta = \dim(\mathbb{K}[X]/\mathcal{I}) = \sum_g \delta_g$.

The Abelian-FGLM algorithm needs the matrices of multiplication $M_{i,g}$ of multiplication by x_i from $(\mathbb{K}[X]/\mathcal{I})_g$ to $(\mathbb{K}[X]/\mathcal{I})_{g+\mathsf{deg}_{\mathbf{G}}(x_i)}$ in the bases $\mathcal{E}_g$ and $\mathcal{E}_{g+\mathsf{deg}_{\mathbf{G}}(x_i)}$. The algorithm 4.72 is used to compute these matrices. The proof of its correctness is exactly the same as the proof of algorithm 1.47 used to compute the multiplication matrices in the classical FGLM algorithm.

The Abelian-FGLM algorithm proceeds just like the classical FGLM algorithm: a new monomial to consider (except 1) is of the form $m = x_i m'$, with $m' \preceq_2 m$. Assume that $\mathsf{deg}_{\mathbf{G}}(m') = g'$, so we already know the expression of $\mathsf{NF}_{\preceq_1}(m', \mathcal{G}_{\preceq_1})$ in terms of $\mathcal{E}_{g'}$, which is a vector V'. It follows that $\mathsf{NF}_{\preceq_1}(m, \mathcal{G}_{\preceq_1})$ is computed by the product $V = M_{i,g'}V'$. Then we have to decide if m belongs to the new staircase in construction $\mathcal{S}$ or if it is the leading monomial of a polynomial of the Gröbner basis for $\preceq_2$. To this end, we use base-change matrices Q_g between $\mathcal{E}_g$ an $\mathcal{S}_g$, the subsets of the staircases having same $\mathbf{G}$-degree g. If s is the number of elements of the staircase $\mathcal{S}_g = \{u_1 \preceq_2 \cdots \preceq_2 u_s\}$ at the current point of the algorithm, and V_i the vectors corresponding to $\mathsf{NF}_{\preceq_1}(u_i, \mathcal{G}_{\preceq_1})$, then $Q_g V_i$ is equal to the i-th vector of the canonical basis. Since the matrix Q_g is invertible, if all the components but the s first ones of QV are zero, then we deduce a new element of the Gröbner basis $\mathcal{G}_{\preceq_2}$, otherwise m is a new element of $\mathcal{S}_g$ and we have to update Q_g, to map V on the $(i+1)$-th element of the canonical basis. The Update procedure used in algorithm 4.73 is exactly the Update procedure 1.54 used in the classical FGLM algorithm.

In the pseudocode of the Abelian-FGLM algorithm, $\hat{0}$ means the $\mathbf{G}$-degree $(0, \ldots, 0)$. We assume that the set of variables is ordered with $x_n \preceq_2 x_{n-1} \preceq_2 \cdots \preceq_2 x_1$. Note that with $\mathsf{deg}_{\mathbf{G}}(x_i) = \hat{0}$ for each i, we recover the standard FGLM algorithm. Abelian-FGLM has been implented in Magma, a web page has been created to collect the code and some examples [1].

4.2.5 Complexity questions

In this subsection, we discuss the arithmetic complexity of the algorithms presented before. This complexity will be counted in terms of operations in $\mathbb{K}$. We will assume that this field contains a e-primitive root of 1, with e the exponent of the group $\mathbf{G}$. We first make some considerations on the first steps, namely the diagonalization of the group and the change of variables on the polynomials induced by this diaonalization.

1. `http://www-polsys.lip6.fr/~jcf/Software/benchssym.html`

Algorithm 4.72: Abelian-Multi-Mat-building algorithm

Input : A reduced Gröbner basis $\mathcal{G}$ of a zero-dimensional $\mathbf{G}$-homogeneous ideal $\mathcal{I} \subsetneq \mathbb{K}[x_1, \ldots, x_n]$, the staircases $\mathcal{E}_g = \{1 = \epsilon_1^g \prec \epsilon_2^g \prec \cdots \prec \epsilon_{\delta_g}^g\}$ of monomials of $\mathbf{G}$-degree g, that are not (top-)reducible by $\mathcal{G}$.

Output: Multiplication matrices of the maps $f \mapsto x_i f$ in $\mathbb{K}[X]_g/\langle\mathcal{G}\rangle_g$

for $i := 1$ **to** n **and** g **in** $\mathcal{D}(\mathbf{G})$ **do**

  $M_{i,g}$:=Square matrix of size $\delta_g \times \delta_g$ filled with zeros; `// The rows of` $M_{i,g}$ `are indexed by` $[\epsilon_1^g \prec \epsilon_2 \prec \cdots \prec \epsilon_{\delta_g}^g]$ `and the columns by` $[x_i\epsilon_1^g \prec x_i\epsilon_2 \prec \cdots \prec x_i\epsilon_{\delta_g}^g]$

$L := [x_i\epsilon \mid 1 \leq i \leq n, \epsilon \in \cup\mathcal{E}_g]$, sorted by $\preceq$ and without duplicates;

for $u \in L$ **do**

  switch u **do**

    case u *in* $\cup\mathcal{E}_g$:

      $g := \mathsf{deg}_{\mathbf{G}}(u)$;

      $M_{i,g-\mathsf{deg}_{\mathbf{G}}(x_i)}[u/x_i, u] := 1$ for all i such that $x_i|u$; `//the column of` $M_{i,g-\mathsf{deg}_{\mathbf{G}}(x_i)}$ `indexed by` u `has only one non-zero entry corresponding to` u/x_i.

    case $u = \mathsf{LM}_{\preceq}(h)$ *for some* $h \in \mathcal{G}$:

      $g := \mathsf{deg}_{\mathbf{G}}(u)$; `//h is G-homogeneous of G-degree g.`

      h can be written $u + \sum_{i=1}^{\delta_g} \alpha_i\epsilon_i^g$;

      $M_{i,g-\mathsf{deg}_{\mathbf{G}}(x_i)}[., u] := {}^t(-\alpha_1, \ldots, -\alpha_{\delta_g})$ for all i such that $x_i|u$;

    otherwise

      $g := \mathsf{deg}_{\mathbf{G}}(u)$;

      Find j such that $x_j|u$ and $v = u/x_j \in L\backslash\mathcal{E}_{g-\mathsf{deg}_{\mathbf{G}}(x_j)}$;

      Find (ϵ, ℓ) such that $v = x_\ell\epsilon$ with $\epsilon \in \cup\mathcal{E}_{g'}$;

      $g' := \mathsf{deg}_{\mathbf{G}}(\epsilon)$; `//` $g' = g - \mathsf{deg}_{\mathbf{G}}(x_i) - \mathsf{deg}_{\mathbf{G}}(x_\ell)$

      $V := M_{\ell,g'}[., v]$; `//this column of` $M_{\ell,g'}$ `contains the expression of` $\mathsf{NF}_{\preceq}(v, \mathcal{G})$ `in the basis` $\mathcal{E}_{g'+\mathsf{deg}_{\mathbf{G}}(x_\ell)} = \mathcal{E}_{g-\mathsf{deg}_{\mathbf{G}}(x_j)}$.

      $W := M_{j,g-\mathsf{deg}_{\mathbf{G}}(x_j)}V$; `//`$W$ `is associated to` $\mathsf{NF}_{\preceq}(x_j v, \mathcal{G}) = \mathsf{NF}_{\preceq}(u, \mathcal{G})$ `in` $\mathcal{E}_g$

      $M_{i,g-\mathsf{deg}_{\mathbf{G}}(x_i)}[, u] := W$ for all i such that $x_i|u$;

return $\{M_{i,g} \mid i \in \{1, \ldots, n\}$ *and* $g \in \mathcal{D}(\mathbf{G})\}$

Algorithm 4.73: Abelian-FGLM algorithm

Input : Multiplication matrices $M_{i,g}$, the sub-staircases $\mathcal{E}_g$, an ordering $\preceq_2$
Output: The Gröbner basis of $\mathcal{I}$ for $\preceq_2$
$L := [(1, \hat{0}, n), (1, \hat{0}, n-1), \ldots, (1, \hat{0}, 1)]$; `//list of 3-uples` (j, g, i) `symbolizing the monomials` $S_g[j] \times x_i$`, ordered by increasing order`
$S_g := [\,]$ for $g \in \mathcal{D}(\mathbf{G}) \backslash \{\hat{0}\}$ and $S_{\hat{0}} = [1]$; `//subsets of the staircase` $\mathcal{S}$ `for the ordering` $\preceq_2$ `having same` **G**`-degree`
$V_g := [\,]$ for $g \in \mathcal{D}(\mathbf{G}) \backslash \{\hat{0}\}$ and $V_{\hat{0}} = [{}^t(1, 0, \ldots, 0)]$; `//`$V_g$ `contains the expressions of` $\mathsf{NF}_{\preceq_1}(S_g[j], \mathcal{G}_{\preceq_1})$ `in` $\mathcal{E}_g$`, each vector in` V_g `has` δ_g `components`
$G := [\,]$; `//The Gröbner basis for` $\preceq_2$
$Q_g := I_{\delta_g}$ for all $g \in \mathcal{D}(\mathbf{G})$;
while $L \neq [\,]$ **do**
  $m := L[1]$; and Remove m from L;
  $j := m[1]; g' := m[2]; i := m[3]; g := g' + \mathsf{deg}_{\mathbf{G}}(x_i)$;
  $v := M_{i,g'} V_{g'}[j]$; `//components of` $\mathsf{NF}_{\preceq_1}(x_i S_g[j], \mathcal{G}_{\preceq_1})$ `in` $\mathcal{E}_g$
  $s := \#S_g$; `//number of elements in` S_g
  $\lambda = {}^t(\lambda_1, \ldots, \lambda_{\delta_g}) := Q_g v$;
  if $\lambda_{s+1} = \cdots = \lambda_{\delta_g} = 0$ **then**
    $G := G \cup [m - \sum_{j=1}^{s} \lambda_j \cdot S_g[j]]$;
  else
    $S_g := S_g \cup [S_{g'}[j] \times x_i]$;
    $V_g := V_g \cup [v]$;
    $L := \mathrm{Sort}\left(L \cup [(s+1, g, i) \mid i = 1, \ldots, n], \preceq_2\right)$;
    Remove duplicates from L;
    Update(Q_g, λ, v); `//Now` $Q_g v = {}^t(0, \ldots, 0, \underset{s+1}{1}, 0, \ldots, 0)$
  Remove from L all multiples of $\mathsf{LM}_{\preceq_2}(G)$;
return G

Remark 4.74. *[96] When working in a finite field $\mathbb{F}_p$, a very interesting case is when ξ belongs to k, so $\mathbb{F}_p(\xi) = \mathbb{F}_p$. It is easy to see that*

$$\xi \in \mathbb{F}_p \iff X^e - 1 \text{ splits on } \mathbb{F}_p \iff \mathbb{Z}/e\mathbb{Z} \subseteq \mathbb{Z}/(p-1)\mathbb{Z} \iff p \equiv 1[e]$$

By Dirichlet's theorem, there are infinitely many such primes and the distribution of such primes is $1/\varphi(e)$, where φ is the Euler's totient function. To compute the Gröbner basis of an ideal over $\mathbb{Q}$, it is more efficient to compute modulo some such primes and use modular methods to recover the original Gröbner basis.

Now, we give without proof a bound on the cost of the two first linear steps:

Proposition 4.75. *The cost of the diagonalization of the matrix group G is bounded by $O((q_1 + \cdots + q_k)n^\omega)$, with ω the constant of linear algebra. With m polynomials f_i of degree less than or equal to d, the cost of computing the f_i^P is bounded by $O(\binom{n+d}{d} ndm \log d \log\log d)$.*

In practice, these costs are widely bounded by the cost of the Abelian-F_5 algorithm, therefore they are negligible.

Hilbert Series of the ideal before and after the diagonalization. Let $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ be a homogeneous ideal, let $\mathbf{G}$ be a matrix group such that $\mathcal{I}$ is $\mathbf{G}$-stable, and assume that $\mathbb{K}$ contains a primitive e-root of 1. Then, the base change matrix P introduced in subsection 4.2.1 induces a bijective mapping between the components $(\mathbb{K}[X]/\langle f_1, \ldots, f_s \rangle)_d$ and $\left(\mathbb{K}[X]/\langle f_1^P, \ldots, f_s^P \rangle\right)_d$. Therefore, both Hilbert series, degree of regularity and degree of the ideal are the same before and after diagonalization. From now, we assume that $\mathcal{I}$ is a $\mathbf{G}$-stable ideal with $\mathbf{G}$ a diagonal matrix group.

Complexity of the Abelian-F_5 algorithm. In order to bound the complexity of the Abelian-F_5 algorithm, we bound the complexity of an abelian version of the Lazard algorithm 1.40, consisting in building a row echelon form of Macaulay's matrices, that are the same as in Abelian-f_5 but without removing rows with the F_5-criterion. In the case of an ideal $\mathbf{F}$ invariant under a diagonal group $\mathbf{G}^{\mathcal{D}}$, we have seen that such a matrix can be splitted into $|\mathbf{G}^{\mathcal{D}}|$ parts, and previous analysis of the dimension of the vector space $\dim(\mathbb{K}[X]_{\chi,d})$ in proposition 3.83 proves that, under parallelization on the computations of row echelon form of the $|\mathbf{G}|$ submatrices, the following theorem holds:

Theorem 4.76. *Let $\mathbf{G}$ be a digonal group with no uniform scalings, and let $\mathbf{F} = (f_1, \ldots, f_s) \in \mathbb{K}[X]^s$ be a family of homogeneous polynomials generating a 0-dimensional $\mathbf{G}$-stable ideal $\mathcal{I}$. The complexity of computing a Gröbner basis for the DRL ordering of the ideal $\mathcal{I}$ is bounded by*

$$O\left(\frac{s}{|\mathbf{G}|^\omega}\binom{n + d_{reg}(\mathbf{F})}{d_{reg}(\mathbf{F})}^\omega\right)$$

operations in $\mathbb{K}$, with ω the constant of linear algebra.

Proof. Once the group $\mathbf{G}$ is fixed, we have seen in theorem 3.78 that the dimensions of the vector spaces $\mathbb{K}[X]_{d,g}$ tend to be equally distributed as d grows to inifinity. The matrix $M_{d,g}$ built by the abelian variant of the Lazard algorithm has $\dim(\mathbb{K}[X]_{d,g})$ columns and $\sum_{i=1}^s \dim(\mathbb{K}[X]_{d-d_i,g-g_i})$ rows if f_i is of degree d_i and $\mathbf{G}$-degree g_i for all i. Then, the proof ends by the same analysis as the complexity of the Lazard algorithm given in theorem 1.42. □

In the affine case, the complexity of the F_5-algorithm is unclear, due to the possible fall of degree. It seems that a bound similar to theorem 1.42 could be obtained (see for example [93, Theorem 1.73]), assuming that the homogeneous part of greatest degree of each polynomial f_i forms a regular sequence (and also, $s = n$). Therefore we could obtain a similar improvement as in theorem 4.77 with this kind of argument. However, we will see in chapter 5 that theorem 1.42 holds also for affine systems. Hence, the following theorem holds:

Theorem 4.77. *Let* $\mathbf{G}$ *be a digonal group and let* $\mathbf{F} = (f_1, \ldots, f_n) \in \mathbb{K}[X]^n$ *be a family of polynomials of degrees* $(d_1, \ldots, d_n)$ *generating a 0-dimensional* $\mathbf{G}$*-stable ideal* $\mathcal{I}$*. The complexity of computing a Gröbner basis for the DRL ordering of the ideal* $\mathcal{I}$ *is bounded by*

$$O\left(\frac{s}{|\mathbf{G}|^\omega}\binom{n + \mathrm{d}_{\mathrm{wit}}}{\mathrm{d}_{\mathrm{wit}}}^\omega\right)$$

operations in $\mathbb{K}$*, with* ω *the constant of linear algebra and* $\mathrm{d}_{\mathrm{wit}} \leq 1 + \sum_{i=1}^{n} d_i - 1$*.*

Complexity of the Abelian-FGLM algorithm. We are now interested in giving a complexity bound of the abelian-FGLM algorithm. Let $\mathcal{I}$ be a zero-dimensional ideal invariant under the diagonal group $\mathbf{G}$. We have to consider the two parts of the algorithm to give a complexity estimation : the construction of the multiplication's matrices $M_{i,g}$ and the loop in FGLM. We denote by δ the degree of the ideal $\mathcal{I}$. Unfortunately, the staircases are not necessarily evenly distributed over the set of $\mathbf{G}$-degrees:

Example 4.78. *Let* $\mathbf{G}$ *be the diagonal matrix group generated by the diagonal matrix* $D_\sigma = \mathsf{Diag}(\xi, \xi^2, \ldots, \xi^{n-1}, 1)$*, acting on* $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$*, with* ξ *a primitive* n*-root of 1. Then the zero-dimensional ideal* $\mathcal{I} = \langle x_1, \ldots, x_{n-1}, x_n^D \rangle$ *has an arbitrary high degree* D *but* $\mathcal{E} = \mathcal{E}_0 = \{1, x_n, \ldots, x_n^{D-1}\}$*, where* 0 *is the* $\mathbf{G}$*-degree of the variable* x_n*.*

However, this kind of "bad situation" happens only for very particular ideals. In practice, the sizes of the substaircases $\mathcal{E}_g$ are evenly distributed, and $|\mathcal{E}_g| \simeq |\mathcal{E}|/|\mathbf{G}|$, see subsection 4.2.6. Moreover, the size of these substaircases can be *exactly* the same; the following proposition gives a sufficient condition.

Proposition 4.79. *Let* $\mathcal{I}$ *be a* $\mathbf{G}$ *stable zero-dimensional ideal. If all the maps*

$$\mathbb{K}[X]/\mathcal{I} \xrightarrow{\times x_i} \mathbb{K}[X]/\mathcal{I}$$

are invertible, then all substaircases have same size.

Proof. It follows from the assumption that $|\mathcal{E}_g| = |\mathcal{E}_{g+\mathsf{deg}_{\mathbf{G}}(x_i)}|$ for all $g \in \mathcal{D}(\mathbf{G})$ and $i \in \{1, \ldots, n\}$. Since the group spanned by the $\mathbf{G}$-degrees $\mathsf{deg}_{\mathbf{G}}(x_i)$ is the whole group $\mathcal{D}(\mathbf{G})$ by proposition 4.69, the proposition is proved. □

In the case $|\mathcal{E}_g| \simeq |\mathcal{E}|/|\mathbf{G}|$, the following theorem holds.

Theorem 4.80. *Under the hypothesis that the monomials of* $\mathcal{E}$ *are evenly distributed over the staircases* $\mathcal{E}_g$ *(which is verified in practice), it is possible to obtain the reduced Gröbner basis* $\mathcal{G}_{\preceq_2}$ *from* $\mathcal{G}_{\preceq_1}$ *of* $\mathcal{I}$ *with* $O\left(\frac{n}{|\mathbf{G}|^2}\delta^3\right)$ *arithmetic operations in* $\mathbb{K}$*.*

Proof. The proof is essentially the same as the proof of theorems 1.51 and 1.57, which bound the complexity of computing the multiplication matrices and applying the usual FGLM algorithm [39]. In algorithm 4.72, the list L has size $O(n\delta)$ and only the"otherwise" case needs arithmetic operations. In this case, the linear algebra part can be done in at most $O\left((\delta/|\mathbf{G}|)^2\right)$, due to the fact than the matrices $M_{i,g}$ are assumed to be of size $(|\delta|/|\mathbf{G}|) \times (|\delta|/|\mathbf{G}|)$. Therefore, at most $O\left(\frac{n}{|\mathbf{G}|^2}\delta^3\right)$ are needed to compute the multiplication matrices in algorithm 4.72. In the same way, the while loop in algorithm 4.73 is entered at most $n\delta$ times, and linear algebra operations are also done in at most $O(\delta^2/|\mathbf{G}|^2)$ operations. Hence, the theorem holds. □

Polynomial complexity. Interesting enough, this approach allows us to identify some problems than can be solved in polynomial time. Assume that $g_1, \ldots, g_s$ are affine polynomials of $\mathbb{K}[X]$ of degree 2, which are individually invariant under the Cyclic-n group. Usually, computing a Gröbner basis of $I = \langle g_1, \ldots, g_s \rangle$ is exponential, but we will see that we can obtain a Gröbner basis of $\mathcal{I}$ in polynomial time in n and s. With $P = (\xi^{ij})$, and $f_i = g_i^P$, each f_i is invariant under $D_\sigma = \mathsf{Diag}(\xi, \xi^2, \ldots, \xi^{n-1}, 1)$ and f_i has $\mathbf{G}$-degree 0.

Lemma 4.81. *The support of each f_i is contained in*

$$\{1, x_n, x_n^2\} \cup \{x_i x_{n-i}, \mid 1 \leq i \leq \lfloor (n-1)/2 \rfloor\}$$

Proof. Each x_i has $\mathbf{G}$-degree i mod n, so $\mathsf{deg}_{\mathbf{G}}(x_i x_j) = i + j \bmod n$, and the only monomials of degree 2 having $\mathbf{G}$-degree 0 are $x_i x_{n-i}$. The only monomial of degree 1 and $\mathbf{G}$-degree 0 is x_n, and 1 is also of $\mathbf{G}$-degree 0. □

Theorem 4.82. *A Gröbner Basis for every monomial ordering of a system of s equations individually invariant under $D_\sigma = diag(\xi, \ldots, \xi^{n-1}, 1)$ can be computed in polynomial time in $n + s$.*

Proof. We set $y_i = x_i x_{n-i}$ for each $i \in \{0, \ldots, \lfloor (n-1)/2 \rfloor\}$ to linearize the equations, and perform a Gaussian elimination on the equations. The result is a Gröbner Basis since the leading monomials of any pair of the obtained polynomials are coprime. The matrix, that we have to reduce has s lines and $\lfloor (n+5)/2 \rfloor$ columns, and the complexity is polynomial in $n + s$. □

Remark 4.83. *Similar results can be obtained for other groups and systems. However, the polynomial timings are rather due to the sparsity of the system after diagonalization than to the action of the diagonal group. We study sparse systems in chapter 5, and this is also a work in progress with Jean-Charles Faugère and Pierre-Jean Spaenleheauer.*

Application to quasi-homogeneous systems. Let $(f_1, \ldots, f_s)$ be a set of polynomials in $\mathbb{K}[X]$, assumed to be quasi-homogeneous, with respect to the sequence of weights $(w_1, \ldots, w_n)$, with w_i being a positive integer for each i. We can assume that the integers w_i are relatively primes. For f a quasi-homogeneous polynomial with respect to this sequence of weights, denote by $\tilde{f}$ the polynomial $f(x_1^{w_1}, \ldots, x_s^{w_s})$ where $x_i^{w_i}$ has been substituted to x_i. Then, each $\tilde{f}_i$ is individually invariant under the action of the group $\mathbf{G}$ generated by the diagonal matrices $D_i = \mathrm{Diag}(1, \ldots, 1, \xi_j, 1, \ldots, 1)$ where ξ_j is a w_j-primitive root of 1. This group has size $\prod_{j=1}^n w_j$ and contains no uniform scalings except I_n since the weights are relatively prime.

d/n	2	3	4	5	10	15
2	0.33	0.00	0.20	0.00	0.091	0.00
3	0.00	0.14	0.00	0.09	0.00	0.01
4	0.20	0.00	0.10	0.09	0.02	0.01
5	0.00	0.09	0.00	0.02	0.00	0.00
10	0.09	0.00	0.02	0.00	0.00	0.00
15	0.00	0.09	0.00	0.00	0.00	0.00

Table 4.84 – Repartition of the monomials under $\mathbf{G}$

Hence, theorem 4.76 can be applied, and we conclude that a Gröbner basis of $\langle \tilde{\mathbf{F}} \rangle = \langle \tilde{f}_1, \ldots, \tilde{f}_s \rangle$ can be computed within

$$O\left(\frac{s}{(\prod_{i=1}^{n} w_i)^{\omega}} \binom{n + d_{reg}(\tilde{\mathbf{F}})}{d_{reg}(\tilde{\mathbf{F}})}^{\omega} \right)$$

if $\langle \tilde{f}_1, \ldots, \tilde{f}_s \rangle$ is a zero-dimensional ideal. This approach allows us to recover parts of the results of [37]. However, some improvements specific to quasi-homogeneous systems are done in this paper. First of all, if we pay attention to the S-polynomials built during the computation of a Gröbner basis of $\tilde{\mathbf{F}}$, we can see that only polynomials of $\mathbf{G}$-degree 0 occur. Hence, there is no need to build $\mathbf{G}$ Macaulay matrices at each step, only one is needed. Secondly, the authors of [37] give a precise bound on the degree of regularity of the sequence $\tilde{\mathbf{F}}$. Finally, it it possible to recover the Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ from the Gröbner basis of $\langle \tilde{f}_1, \ldots, \tilde{f}_s \rangle$. The FGLM algorithm can be applied with this Gröbner basis, and its complexity is precisely estimated.

4.2.6 Experiments

In this subsection, we report some experiments that show the improvements given by our approach on the computation of Gröbner bases of ideals invariant under an abelian matrix group. We first present the dimensions of $\mathbb{K}[X]_{d,g}$ and $(\mathbb{K}[X]/\mathcal{I})_g$ on some examples, and then give timings obtained with an implantation of the algorithm Abelian-F_4. A web page has been made for other software and benchmarks [2].

Distribution of $\dim(\mathbb{K}[X]_{d,g})$ and $\dim((\mathbb{K}[X]/\mathcal{I})_g)$. In this paragraph, we assume that $\mathbf{G}$ is the cyclic group generated by the matrix $D_\sigma = P^{-1} M_\sigma P = (\xi, \xi^2, \ldots, \xi^{n-1}, 1)$ presented in example 4.49. We first compare $\dim(\mathbb{K}[X]_{d,g})$ with $\dim(\mathbb{K}[X])_d/n$, since n is the order of the group $\mathbf{G}$. To this end we compute the relative standard deviation between these dimensions, for several n and d. The formula is given by

$$\sigma_{d,n} = \frac{\sqrt{\frac{1}{n} \sum_{g \in \mathbf{G}} \left(\dim(\mathbb{K}[X]_{d,g}) - \frac{\dim(\mathbb{K}[X]_d)}{n} \right)^2}}{\frac{\dim(\mathbb{K}[X]_d)}{n}}.$$

Table 4.84 presents some values of $\sigma_{d,n}$ in the case of this cyclic group. We see that the monomials are very quickly evenly distributed over $g \in \mathcal{D}(\mathbf{G})$.

2. `http://www-polsys.lip6.fr/~jcf/Software/benchssym.html`

n	$\lvert\mathcal{E}\rvert$	$\lvert\mathbf{G}\rvert$	$\lvert\mathcal{E}\rvert/\lvert\mathbf{G}\rvert$	$\max(\lvert\mathcal{E}_g\rvert)$	$\sigma_{\mathcal{E}}$
3	6	9	0.667	2	1
5	70	25	2.800	6	0.286
6	156	36	4.33	6	0.133
7	924	49	18.86	24	0.045
10	34940	100	349.40	354	0.0043
11	184756	121	1526.91	1536	0.00060

Table 4.85 – Cyclic-n: Repartition of the monomials into $\mathcal{E}_g$

In the same way, the stairs $\mathcal{E}_g$ that appear in the abelian-FGLM algorithm have roughly same size. Table 4.85 presents some zero-dimensional ideals together with the sizes of the groups and the sizes of the substaircases. The examined problem is the Cyclic-n problem, defined in example 4.51. We recall the resulting ideal is $\mathbf{G}$-stable with $\mathbf{G}$ a group of cardinal n^2. Notice that not all integers n between 3 and 11 lie in the table: the other values lead to an ideal of positive dimension. In the table, we present the size of the (global) staircase, the average size of a substaircase (equal to $|\mathcal{E}|/|\mathbf{G}|$) and the maximal size of a substaircase. This maximal substaircase is always given by the $\mathbf{G}$-degree of the monomial 1, corresponding to the trivial character. The final column is the relative standard deviation between $|\mathcal{E}_g|$ and $|\mathcal{E}|/|\mathbf{G}|$, the formula of which is given by

$$\sigma_{\mathcal{E}} = \frac{\sqrt{\frac{1}{|\mathbf{G}|}\sum_{g\in\mathbf{G}}\left(|\mathcal{E}_g| - \frac{|\mathcal{E}|}{|\mathbf{G}|}\right)^2}}{\frac{|\mathcal{E}|}{|\mathbf{G}|}}.$$

It follows that the relative standard deviation tends fast to 0 as n grows, meaning that all substaircases have roughly same size.

Abelian-F_4 implementation. A first implementation of the Abelian-F_4 algorithm has been made. This algorithm is a variant of the classical F_4-algorithm [34]. It constructs $|\mathbf{G}|$ matrices at each degree, using the usual strategy of F_4. Note that only the construction of the matrices and the operations of row-reduction on them have been parallelized, the handling of the list of critical pairs is still sequential. Surprisingly, the linear algebra can sometimes be so accelerated that this handling can become the most time-consuming part whereas it is usually negligible. Therefore we report in the following tables two timings or ratios in each column: the timings are related to $F_4^{A,n}$, which is the new abelian algorithm parallelized on n cores, applied on a $\mathbf{G}$-stable ideal $\mathcal{I}$, wich $\mathbf{G}$ a diagonal matrix group. The first one is the total timing and the second one is only the parallelized part (that is to say, building the matrices and the linear algebra parts). The other columns contain the ratios between F_4^A, F_4 or F_4^M and $F_4^{A,n}$. F_4 means the standard F_4 applied on the original ideal before diagonalization and F_4^A the standard F_4 applied on $\mathcal{I}$. F_4^M is the implementation of the F_4 algorithm in Magma, and there is only the ratio for the total timing. In each case except table 4.90, the group acting on the ideal before diagonalization is the cyclic group C_n generated by the matrix M_σ defined in example 4.49, and $\mathbf{G}$ is the group generated by the diagonal matrix $D_\sigma = \mathrm{Diag}(\xi, \xi^2, \ldots, 1) = P^{-1}M_\sigma P$. Note that we have to reach big-sized problems to have a significant impact. All computations have been made on a computer with 4 Intel(R) Xeon(R)

CPU E5-4620 0 @ 2.20GHz with 387 GB of RAM, on a field where $X^{|G|}-1$ fully splits (most of the time $\mathbb{F}_{65521}$), according to remark 4.74.

Equations of degree 3 and G-degree 0. In table 4.86, we consider n randomized affine equations of degree 3 individually stable under C_n, which give rise to equations of **G**-degree 0 in $\mathcal{I}$. Notice that in this case, the substaircases of each **G**-degree have exactly same size.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,n}$ tot
8	3.46s;2.48s	2.2;2.7	33.0;45.4	22
9	77.04s;64.21s	7.3;8.6	67.8;81.0	50
10	762s;672s	10.0;11.3	160.9;182.1	134
11	22162s;20425s	13.0;14.0	∞	∞

Table 4.86 – n cubic equations of **G**-degree 0

Equations of degree 2 with only two G-degrees. Table 4.87 presents n equations of degree 2, half of these equations in $\mathcal{I}$ are of **G**-degree 0, and half of **G**-degree 1. In this case, the computation on $\mathcal{I}$ becomes polynomial in n and the handling of the critical pairs is the most time-consuming part.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p
25	0.25s;0.06s	1.9;4.5	56.60;230.0
30	0.58s;0.11s	1.5;4.6	80.79;415.1
35	0.86s;0.11s	1.9;8.5	228.5;1755
40	1.55s;0.21s	2.0;8.5	300.6;2174
45	2.31s;0.30s	2.4;10.7	664.5;5043
50	3.96s;0.45s	2.6;13.3	753.8;6504
55	6.98s;0.66s	2.5;15.0	1207;12570
60	10.85s;0.96s	2.8;17.2	1294;14330

Table 4.87 – n quadratic equations of **G**-degree 0 or 1

Application to Cryptography. Table 4.88 presents equations coming from a cryptographic application : the cryptosystem NTRU [58]. The underlying basic problem is the following:

NTRU problem: Given $h = \sum_{i=0}^{n-1} h_i x^i \in \mathbb{F}_p[x]$, find f in $\mathbb{F}_p[x]$ of degree $n-1$ and coefficients in $\{0,1\}$ such that $g = fh \bmod x^n - 1$ has also its coefficients in $\{0,1\}$.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p
20	3.07s;0.78s	3.5;11.3	66.0;257.8
21	4.52s;1.21s	4.0;11.9	90.15;334.0
22	15.01s;2.28s	2.2;11.4	58.4,381.6
23	11.16s;1.87s	3.3;17.2	115.2;686.1
24	128s;14.3s	5.2;36.5	241.1;2149.
25	218s;31.0s	5.8;32.5	∞
26	365s;59.0s	6.6;32.6	∞
27	955s;113s	4.9;33.3	∞
28	1214s;192s	7.1;36.1	∞
29	3310s;323s	4.7;38.8	∞

Table 4.88 – NTRU equations

Denote $f = \sum_{i=0}^{n-1} f_i x^i$. Then, the f_i's are the unknowns, which satisfy the equations $f_i^2 - f_i = 0$, since we want f_i to be in $\{0, 1\}$. Let $g = \sum_{i=0}^{n-1} g_i x^i = fh$, then the g_i's are linear forms in the f_i's satisfying also $g_i^2 - g_i = 0$. More precisely, $g_i = \sum_{j=0}^{n-1} f_j h_{[(i-j) \bmod n]}$. The matrix M_σ acts on the variables f_i by $f_i^{M_\sigma} = f_{[(i+1) \bmod n]}$, therefore:

$$g_i^{M_\sigma} = \sum_{j=0}^{n-1} f_{[(j+1) \bmod n]} h_{[(i-j) \bmod n]} = \sum_{j=0}^{n-1} f_j h_{[(i-j+1) \bmod n]} = g_{[(i+1) \bmod n]}$$

It follows that the system consists of $2n$ quadratic equations in the polynomials (f_i) generating an ideal globally stable under the action of C_n. The speed-up between F_4 and $F_4^{A,n}$ is roughly 250 with 24 variables, and the use of $F_4^{A,n}$ has a significant impact since we can achieve bigger problems. In this case the handling of the critical pairs is also the most time-consuming part.

Cyclic-n problem. Table 4.89 presents timings on the Cyclic-n problem. We see that Cyclic-11 could be solved in less than 8 hours although it is untractable with F_4.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,n}$ tot
8	0.50s;0.40s	2.5;2.7	7.8;9.3	6.0
9	10.21s;7.71s	4.3;5.4	37.0;48.4	30.5
10	334s;290s	13.2;14.8	411.0;472.3	207
11	27539s;25454s	∞	∞	∞

Table 4.89 – The Cyclic-n problem

From the experimental side, applying the F_4 algorithm on the cyclic 9 problem we obtain, in degree 15, a matrix of size 72558×93917; applying the abelian-F_4 algorithm we obtain 9

independent matrices of roughly the same size: $8340 \times 10703, 8180 \times 10544$, 8122×10484, $7804 \times 10171, 7993 \times 10358, 8042 \times 10404, 7796 \times 10162$, 7967×10369 and 8314×10722.

Polynomials of degree 3 invariant under a product of cyclic groups. Table 4.90 is an example of ideals generated by random polynomials of degree 3 invariant under the group $C_{k_1} \times C_{k_2}$, each subgroup C_k acting on k variables. We see that the algorithm is more efficient when $k_1 = k_2$, which makes sense since the size of the group is $k_1 k_2$.

k_1, k_2	F_4^{A,k_1k_2} tot; // p.p	$F_4^{A}/F_4^{A,k_1k_2}$ tot;p.p	$F_4/F_4^{A,k_1k_2}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,k_1k_2}$ tot
4,4	2.0s;1.3s	2.4;3.2	61.8;94.6	37
6,2	2.9s;2.4s	2.2;2.5	76.4;91.4	44
5,5	70s;43s	11.8;16.2	∞	∞
6,4	92s;76s	17.7;19.8	∞	∞
8,2	107s;100s	12.1;12.3	∞	∞

Table 4.90 – $n = k_1 + k_2$ cubic equations invariant under $C_{k_1} \times C_{k_2}$

4.3 Solving Polynomial Systems of Invariant Equations with SAGBI bases

Introduction

This section presents a work in common with Jean-Charles Faugère and Guënael Renault which is still in progress.

Problem Statement. In this section, we assume that $\mathbf{G}$ is any finite subgroup of the general linear group $\mathcal{GL}_n(\mathbb{K})$, with no assumption on the characteristic of $\mathbb{K}$: the action of $\mathbf{G}$ on $\mathbb{K}[X]$ can be modular or non-modular. Let $\mathsf{F} = (f_1, \ldots, f_s)$ be a set of *individually* $\mathbf{G}$*-invariant* equations, that is to say each equation is $\mathbf{G}$-invariant: for all $i \in \{1, \ldots, s\}$ and $A \in \mathbf{G}$, ${f_i}^A = f_i$. Can we solve the system $\{f_1(X) = \cdots = f_s(X) = 0\}$ faster than with usual Gröbner bases algorithms ?

The main idea of the section is to compute in the subalgebra $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$ of $\mathbf{G}$-invariant polynomials. This allows to reformulate the polynomials (f_i) as linear combinations of elements in a basis of $\mathbb{K}[X]^{\mathbf{G}}$. This reformulation is a more compact way to manipulate the polynomials occuring in the computations, compared to the dense representation as linear combinations of monomials. Since the concept of Gröbner bases is not available in $\mathbb{K}[X]^{\mathbf{G}}$, we will use SAGBI bases instead, introduced in section 1.3. In this section, we have seen how the SAGBI-Matrix F_5 allows us to compute a SAGBI basis of an ideal generated by a finite set of polynomials in a subalgebra of $\mathbb{K}[X]$, up to some given degree. The knowledge of a SAGBI basis of the ideal generated by F in $\mathcal{A}$ at a sufficient degree will allow us to compute a finite *Gröbner basis* in some invariant ring, using a variant of the FGLM algorithm. The final step is to use this Gröbner basis to recover the solutions of the system.

Previous Work. We present an extension of the results given by Faugère and Rahmany in [41]. The main ideas of the present section can be found in this earlier version, but the authors restricted their discussion to the *non-modular case*, when the group $\mathbf{G}$ is a subgroup of the permutation group $\mathfrak{S}_n$ and no complexity analysis was provided.

Different approaches have already been proposed to solve such invariant problems. First of all, since we assume that all equations f_i generating the system are invariant under the action of the group $\mathbf{G}$ (${f_i}^A = f_i$ for all $A \in \mathbf{G}$), it is possible to use tools from invariant theory ([100, 27]) to rewrite the system: the algebra $\mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$ can be written $\mathbb{K}[h_1, \ldots, h_r]$ with $\{h_1, \ldots, h_r\}$ a suitable set of *fundamental invariants* of the group $\mathbf{G}$ (see definition 3.29). The idea is to reformulate the polynomials f_i in terms of h_j to obtain a new system to which we add the relations between the polynomials h_j. The drawback of this method is that, except for particular families of groups (for example reflection groups in the non-modular case) the number of requiring fundamental invariants can increase dramatically compared to n. For example, using this method to solve the Cyclic-5 problem leads to a system with 15 polynomials in 15 unknowns, which is in practice more time-consuming to solve than the original one (only 5 polynomials in 5 variables).

With the idea of working in the field of $\mathbf{G}$-invariant rational fractions $\mathbb{K}(x_1, \ldots, x_n)^{\mathbf{G}}$, Colin is able in [23] to reformulate the system into a rational system involving only $n + 1$ polynomials given by the *primary invariants* and only one other invariant. However, according to our experience, the resulting system can be more difficult to solve than the original one.

The idea of bringing together SAGBI basis of ideals and ring of invariants goes back to a work of Thiéry [104], where he used these objects to compute the secondary invariants of $\mathbb{K}[X]^{\mathbf{G}}$ for $\mathbf{G}$ a permutation group in any characteristic but assuming that $\mathbb{K}[X]^{\mathbf{G}}$ is

Cohen-Macaulay in the modular case. To this end, he proposed a variant of Buchberger's algorithm. The fact that with this algorithm, many unnecessary S-pairs remain undetected by the Buchberger-like criterions was another motivation of the paper [41].

We have already mentionned that the typical example of problem with symmetry is to solve $f_1 = \cdots = f_s = 0$ with $\mathsf{F} = \{f_1, \ldots, f_s\}$ a *globally* $\mathbf{G}$-invariant set of polynomials. Of course, if we have a method to solve efficiently those systems, we can apply it in the particular case of a system with $\mathbf{G}$-invariant polynomials. In the previous section, we proposed variants of F_5 and FGLM algorithms to compute a Gröbner basis of a zero-dimensional ideal generated by a globally $\mathbf{G}$-invariant set of polynomials, assuming that $\mathrm{char}(\mathbb{K}) \nmid |\mathbf{G}|$ and that $\mathbf{G}$ is abelian. It is possible to apply these results here with $\mathbf{G}'$, a maximal abelian subgroup of $\mathbf{G}$. Under some assumptions, this approach allows us to ensure a gain of $|\mathbf{G}'|^\omega$ in F_5 and $|\mathbf{G}'|^2$ in FGLM compared to a classical Gröbner basis computation, which remains unsatisfactory if $\mathbf{G}$ is much bigger than $\mathbf{G}'$: a lot of symmetry is not taken into account.

Main results. Let $\mathcal{A}$ be a graded subalgebra in $\mathbb{K}[X]$, and $f_1, \ldots, f_s$ be polynomials in $\mathcal{A}$ generating the ideal $\mathcal{I}^{\mathcal{A}}$ in $\mathcal{A}$ and $\mathcal{I}$ in $\mathbb{K}[X]$.

Our main contributions in this section are twofold: algorithms and complexity. First, we present an algorithm which computes a SAGBI basis of the ideals $\mathcal{I}^{\mathcal{A}}$ up to some given degree D. This algorithm SAGBI-F_5, is a variant of the F_5 algorithm [35], and requires a basis of $\mathcal{A}_d$ for $0 \leq d \leq D$, where $\mathcal{A}_d$ is the graded component of degree d of $\mathcal{A}$. Given these bases $\{(b_i^d)_{1 \leq i \leq n_d} \mid d = 0, \ldots, D\}$, we have also to know the expressions of $b_i^d \times b_{i'}^{d'}$ in terms of $(b_k^{d+d'})_{1 \leq k \leq n_{d+d'}}$. Let $h_1, \ldots, h_r$ be polynomials in $\mathcal{A}$. The aim of the second main algorithm is to compute a Gröbner basis of the ideal

$$\mathcal{J} = \mathcal{I} + \langle \{H_i - h_i(x_1, \ldots, x_n) \mid 1 \leq i \leq r\} \rangle \cap \mathbb{K}[H_1, \ldots, H_r]$$

where $H_1, \ldots, H_r$ are r new unknowns, assuming that $\mathcal{I}$ is zero-dimensional, with the help of the SAGBI-basis up to degree D. For example, if $\mathbf{G}$ is a subgroup of the symmetric group $\mathfrak{S}_n$ embedded in $\mathcal{GL}_n(\mathbb{K})$, it is possible to take the symmetric functions $\sigma_1, \ldots, \sigma_n$ as polynomials $h_1, \ldots, h_n$. This algorithm, called SAGBI-FGLM, is a variant of the FGLM algorithm [39]. In practice, SAGBI-FGLM algorithm computes *SAGBI-Normal Forms with respect to the SAGBI basis* of polynomials $\prod_{i=1}^n {h_i}^{\alpha_i}$ of degree less than D, corresponding to monomials in $\mathbb{K}[H_1, \ldots, H_r]$, taken by increasing order for a weighted DRL ordering (with $\mathsf{deg} H_i = \mathsf{deg} h_i$). Since we do not know the degree D that we have to reach until SAGBI-FGLM succeeds, we apply in practice successively *truncated versions* of both algorithms at each degree. Then, we compute the variety $\mathbb{V}(\mathcal{J})$ associated to $\mathcal{J}$, which is exactly the image of the variety $\mathbb{V}(\mathcal{I})$ through the map:

$$\begin{array}{rccc} \Phi : & \overline{\mathbb{K}}^n & \longrightarrow & \overline{\mathbb{K}}^r \\ & y = (y_1, \ldots, y_n) & \longmapsto & (h_1(y_1, \ldots, y_n), \ldots, h_r(y_1, \ldots, y_n)) \end{array}$$

where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. Roughly speaking, since $h_1, \ldots, h_r$ are invariant under the action of $\mathbf{G}$, a point in $\mathbb{V}(\mathcal{J})$ is the image of $|\mathbf{G}|$ points in $\mathbb{V}(\mathcal{I})$, therefore $\mathbb{V}(\mathcal{J})$ is much smaller than $\mathbb{V}(\mathcal{I})$. We finally recover the variety $\mathbb{V}(\mathcal{I})$ by computing $\Phi^{-1}(\mathbb{V}(\mathcal{J}))$, and removing the points that are not in $\mathbb{V}(\mathcal{I})$. In practice, since we stop the computation of a SAGBI basis as soon as SAGBI-FGLM algorithm gives a zero-dimensional ideal, we can have more spurious solutions to remove. The whole process can be summarized in the following diagram:

To remove spurious solutions, we propose several approaches. The first one can be applied only if $\mathbf{G}$ is a generalized permutation group, which is the main interesting case of this section

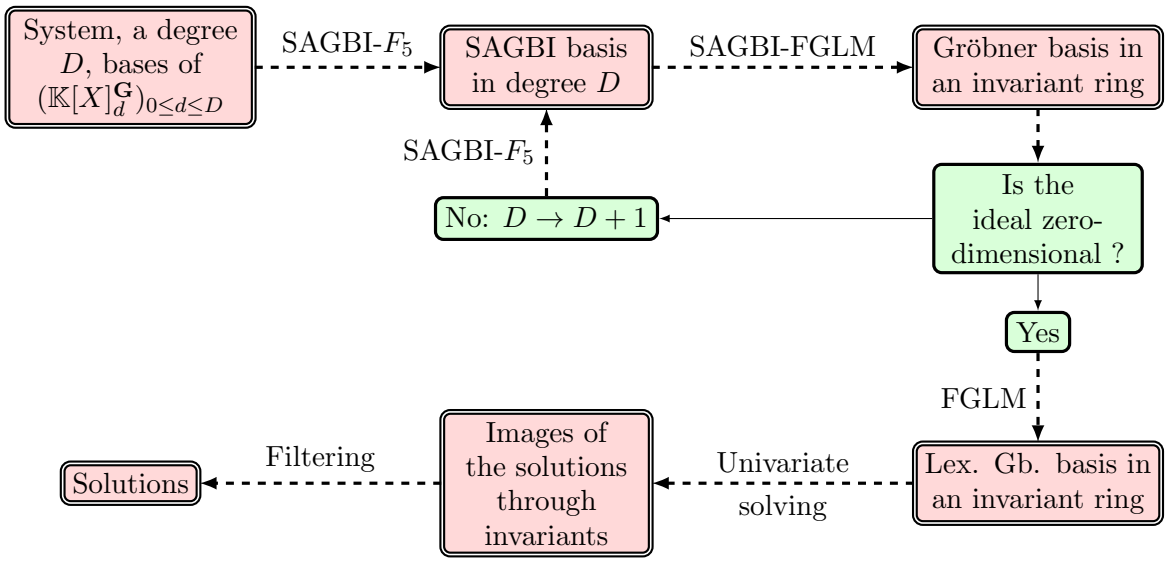


Figure 4.91 – Strategy for solving a system of invariant equations under the action of a finite group.

since computations of a basis $(b_i^d)_i$ of each component $\mathbb{K}[X]_d^{\mathbf{G}}$ and expressions of $b_i^d \times b_{i'}^{d'}$ in terms of $(b_j^{d+d'})_j$ can be done easily. The idea is to apply previous algorithms in order to know some powers (depending on $\mathbf{G}$) of the symmetric functions of the solutions. Then, one can introduce a univariate polynomial, the coefficients of which are such symmetric functions and compute its roots to recover the solutions. The two others are more general but need some precomputations. They have both in common that they are related to the problem of computing a lexicographical Gröbner basis of a zero-dimensional ideal $\langle E+T\rangle \subset \mathbb{K}[y_1,\dots,y_r]$, where E is a given set of polynomials and $T = \{T_1,\dots,T_r\}$ is a *triangular set*, that is the leading monomial of each T_i for lexicographical ordering with $y_1 > \cdots > y_r$ is a power of y_i. The second approach is close to the Lazard Lex-Triangular algorithm [73]. The final approach is univariate, which means that it needs an isomorphism of algebras

$$\begin{array}{rccc} \varphi: & \mathbb{K}[y_1,\dots,y_r]/\langle T\rangle & \to & \mathbb{K}[u]/Q(u) \\ & y_1,\dots,y_r & \mapsto & S_1(u),\dots,S_r(u) \\ & \Lambda & \mapsto & u \end{array}$$

where Λ is a suitable linear combination of $y_1,\dots,y_r$. This approach uses GCD's and a variant of the FGLM algorithm.

We present only one complexity result here, namely the complexity of computing a SAGBI basis of the ideal generated by the polynomials in F up to some given degree. This is easy to derive in this context, from the estimations given in chapter 3.

Theorem 4.92. *Let $f_1,\dots,f_s \in \mathbb{K}[X]^{\mathbf{G}}$ be homogeneous polynomials of degree $d_1,\dots,d_s$. If there are no uniform scaling in $\mathbf{G}$ except I_n, the complexity of computing a SAGBI-basis up to degree D of the ideal $\langle f_1,\dots,f_s\rangle \subset \mathbb{K}[x_1,\dots,x_n]^{\mathbf{G}}$ is bounded by $O\left(\frac{t}{|\mathbf{G}|^\omega}\binom{D+n}{D}^\omega\right)$ arithmetic operations in $\mathbb{K}$.*

Work has to be done, in order to precise other complexity results. As a proof of concept, we present here the table giving some sizes of the Gröbner bases and the Gröbner bases

in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$ obtained for the Cyclic-6 and Cyclic-7 problem (σ_i is the i-th symmetric function of the (x_j)). The group that acts on the system is the dihedral group D_n of size $2n$, for $n = 6, 7$.

$\mathcal{G}$	$\lvert\mathcal{G}\rvert$	Max length of a polynomial in $\mathcal{G}$	$\mathbb{V}(\langle\mathcal{G}\rangle)$
Lex-Gb of $\mathcal{I}^{D_6}$	17	27	156
$\mathfrak{S}_6$-inv Lex-Gb of $\mathcal{I}^{D_6}$	7	4	13
Lex-Gb of $\mathcal{I}^{D_7}$	35	132	924
$\mathfrak{S}_7$-inv Lex-Gb of $\mathcal{I}^{D_7}$	7	9	57

Table 4.93 – Sizes of the invariant Gröbner bases and the Gröbner bases

Organization of the section. The preliminaries needed to understand this section were presented in section 1.3 and chapter 3. In section 1.3, we have seen the concept of SAGBI bases and the Matrix SAGBI-F_5 algorithm 1.68 and in chapter 3, we gave some basic definitions of the invariant ring $\mathbb{K}[X]^{\mathbf{G}}$, and explain how to compute a basis of each homogeneous component $\mathbb{K}[X]_d^{\mathbf{G}}$ in different cases: modular and non-modular cases, and the special case of pseudo-reflexion groups. We also analysed the complexity of each computation. Moreover, we have given estimations of the dimensions of the components $\mathbb{K}[X]_d^{\mathbf{G}}$, which can be read from the Hilbert series of the invariant ring. We also reviewed properties on the structure of the algebra $\mathbb{K}[X]^{\mathbf{G}}$ and have defined the notion of Gröbner basis in invariant ring, which is the object we will compute after applying the FGLM algorithm.

Subsection 4.3.1 presents the Matrix SAGBI F_5 algorithm in the context of invariant rings, with an expanded example. The end of the subsection is devoted to the analysis of the complexity of algorithm SAGBI-F_5.

From the beginning of the subsection 4.3.2 to the end of the section, we assume that $\mathcal{I} = \langle f_1, \ldots, f_s\rangle$ is zero-dimensional. Thus, subsection 4.3.2 provides a FGLM like algorithm for converting a SAGBI-basis of an ideal $\mathcal{I}^{\mathcal{A}}$ in $\mathcal{A}$ into a Gröbner basis in some ring $\mathbb{K}[H_1, \ldots, H_r]$. Since each variable H_i corresponds to a given polynomial $h_i \in \mathcal{A}$, the result is a Gröbner basis of the ideal

$$\mathcal{J} = \mathcal{I} + \langle \{H_i - h_i(x_1, \ldots, x_n) \mid 1 \leq i \leq r\}\rangle \cap \mathbb{K}[H_1, \ldots, H_r]$$

Note that a SAGBI-basis is usually not finite, so we cannot compute a SAGBI basis of $\mathcal{I}^{\mathcal{A}}$ with SAGBI-F_5 and then use SAGBI-FGLM algorithm. Therefore, we have to apply step-by-step SAGBI-F_5 algorithm: a step corresponds to an increasing degree D and at each step we compute a SAGBI-basis of $\mathcal{I}^{\mathcal{A}}$ up to degree D, and then we apply SAGBI-FGLM. In practice, we stop as soon as we get a subset of polynomials in $\mathcal{J}$ generating a zero-dimensional ideal. The end of the subsection is also devoted to complexity analysis.

We explain in subsection 4.3.3 various methods to recover $\mathbb{V}(\mathcal{I})$ from the variety $\mathbb{V}(\mathcal{J})$, or at set containing $\mathbb{V}(\mathcal{J})$. The first one is restricted to the case $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$ and $\mathbf{G}$ a generalized permutation group. The two others are more general but need some precomputations. We present first a triangular approach, which can be viewed as a generalization of the Lex-Triangular algorithm, which converts a Gröbner basis for lexicographic ordering into a union of triangular sets. The final approach is based on a univariate representation of a triangular set, and leads to computation of GCDs and a variant of the FGLM algorithm.

The last subsection is devoted to experiments and benchmarks.

4.3.1 SAGBI-Gröbner bases in invariant rings

In [104], Thiéry gives a variant of the Buchberger's algorithm to compute SAGBI bases up to some given degree in invariant rings of permutation groups. Also, he provided a Buchberger-like criterion to skip the computation of unnecessary S-pairs. Although this criteria avoids many reductions to zero, still many useless pairs remain undetected. We have seen in chapter 1, a very general algorithm 1.68 that computes a SAGBI basis of an ideal $\mathcal{I}^{\mathcal{A}}$ in a subalgebra $\mathcal{A}$ up to some given degree. Our aim here is to apply this algorithm in the particular case where $\mathcal{A}$ is a ring of invariant $\mathbb{K}[X]^{\mathbf{G}} = \mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$. In order to analyze the efficiency of this algorithm in the case of invariants, all needed material has been presented in chapter 2, and the basic properties of invariant rings have been seen in chapter 3. Therefore, we present in this subsection only examples, which make the comprehension of the SAGBI tools in invariant rings easier, and perform a brief analysis of complexity, which follows the results given in the prerequisites.

Reminders. Depending on the group $\mathbf{G}$, we have seen in subsection 3.1.1 several algorithms, that compute a basis of each component $\mathcal{A}_d$, such that two polynomials of the basis have distinct leading monomials. Then, in every component $\mathcal{A}_d$, a basis $(b_i^d)_{1 \leq i \leq n_d}$ of $\mathcal{A}$ as a $\mathbb{K}$-vector space has been computed, with $\mathsf{LM}_{\preceq}(b_1^d) \succ \mathsf{LM}_{\preceq}(b_2^d) \succ \cdots \succ \mathsf{LM}_{\preceq}(b_{n_d}^d)$. For example, if $\mathbf{G}$ is a generalized permutation group in the non-modular case, the computation of such a basis is easy, since it is given by the set $\{\Re(m)\}$, with m describing all *initial monomials* of degree d, namely the leading monomials of elements of $\mathcal{A}_d$.

Example 4.94. *We consider the same situation as in example 3.19, where $\mathbf{G}$ is the representation in degree 3 of the alternate group $\mathfrak{A}_3$, acting on $\mathcal{A} = \mathbb{Q}[x, y, z]$, ordered with $\preceq$ the* graded lexicographical ordering. *Then, bases of $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_3$ are given by:*

$$x + y + z \qquad \begin{cases} x^2 + y^2 + z^2 \\ xy + yz + xz \end{cases} \qquad \begin{cases} x^3 + y^3 + z^3 \\ x^2y + xz^2 + y^2z \\ x^2z + xy^2 + yz^2 \\ xyz \end{cases}$$

Therefore, the initial monomials of degree less than or equal to 3 are $1, x, x^2, xy, x^3, x^2y, x^2z$ and xyz. Actually, initial monomials are of the form $m^*_{\alpha\beta\gamma} = x^\alpha y^\beta z^\gamma$ with $\alpha > \beta, \gamma$ or $\alpha = \beta \geq \gamma$. Notice that with the DRL ordering, x^2z would not have been an initial monomial, but xy^2 would.

Recall that reductions can be performed between elements of $\mathcal{A}$, see definition 1.60.

Example 4.95. *We continue the example 4.94. Let h be $x + y + z = 3\Re(x)$. Then $\Re(x^3y) = h\Re(x^2y) - \Re(x^2y^2) - \Re(x^2yz)$, so $3\Re(x^3y)$ reduces to $-\Re(x^2y^2) - \Re(x^2yz)$ modulo $\Re(x)$. The polynomial $\Re(x^2y^2)$ is not reducible by $\Re(x)$ but $\Re(x^2yz) = \Re(x)\Re(xyz)$ is. Therefore the SG-NormalForm of $\Re(x^3y)$ modulo h is $-\Re(x^2y^2)$.*

Recall that an element of an algebra $\mathcal{A}$ whose leading monomial is not a leading monomial of a polynomial in an ideal $\mathcal{I}^{\mathcal{A}}$ in $\mathcal{A}$ is called a standard element, with respect to the ideal. In the context of invariant ring, we will rather speak of *standard invariants*.

Example 4.96. *We continue the example 4.95. Let $\mathcal{I}^{\mathbf{G}}$ be the ideal generated by $h = 3\Re(x)$ in $\mathcal{A} = \mathbb{Q}[x, y, z]^{\mathbf{G}}$. An orbit sum $\Re(m^*_{\alpha\beta\gamma})$ is reducible by h if and only if $x^{\alpha-1}y^\beta z^\gamma$ is an initial monomial, which means that $\alpha - 1 > \beta, \gamma$ or $\alpha - 1 = \beta \geq \gamma$. Then, all the standard invariants*

are the orbit sums $\Re(m^*_{\alpha\beta\gamma})$ *with* $\alpha = \beta \geq \gamma$ *or* $\alpha - 1 = \gamma > \beta$. *In example 4.95, we have seen that* $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(\Re(x^3y), p) = -\Re(x^2y^2)$. *Actually,* $\Re(x^3y) = p(\Re(x^2y) - \Re(xyz)) - \Re(x^2y^2)$ *is the decomposition of* $\Re(x^3y)$ *into an element of* $\mathcal{I}^{\mathbf{G}}$ *and a linear combination of standard invariants.*

The SAGBI-F_5 algorithm (algorithm 1.68) is a generalization of the classical F_5 algorithm 1.44. In order to apply it in the algebra $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$, we first have to compute a basis of $\mathbb{K}[X]^{\mathbf{G}}$ as a $\mathbb{K}$-vector space.

Let $f_1, \ldots, f_s$ be homogeneous polynomials in $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$. The SAGBI-$F_5$ algorithm proceeds by building SAGBI-Macaulay's matrices (that we will call Invariant-Macaulay's matrices in this context) of $f_1, \ldots, f_i$ for each i between 1 and s and apply row reductions on them.

Example 4.97. *Assume that* $\mathbf{G}$ *is a generalized permutations subgroup, with* $\mathrm{char}(\mathbb{K}) \nmid |\mathbf{G}|$. *We have seen that a basis of* $\mathcal{A}_d = \mathbb{K}[X]^{\mathbf{G}}_d$ *can be chosen as* $\{\Re(m_1^d) \succ \cdots \succ \Re(m_{n_d}^d)\}$ *with* m_i^d *describing all initial monomials. In this case, the Invariant-Macaulay's matrix has the form:*

$$M_{d,i} = \begin{array}{c} \\ \Re(m_1^{d-d_1}).f_1 \\ \vdots \\ \Re(m_\mu^{d-d_j}).f_j \\ \vdots \\ \Re(m_{n_{d-d_i}}^{d-d_i}).f_i \end{array} \begin{array}{c} \begin{array}{cccc} \Re(m_1^d) & \Re(m_2^d) & \ldots & \Re(m_{n_d}^d) \end{array} \\ \begin{pmatrix} \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix} \end{array}$$

Example 4.98. *In this example, we continue the example 4.96, but now let* $\mathcal{I}^{\mathbf{G}}$ *be* $\langle f_1, f_2 \rangle$ *with* $f_1 = \Re(x)$ *and* $f_2 = \Re(x^2y) - \Re(xyz)$. *We want to write the Invariant-Macaulay's matrix* $M_{3,2}$. *Since there are four initial monomials at degree 3 (namely* x^3, x^2y, x^2z *and* xyz*),* $M_{3,2}$ *has four columns. Since* f_1 *has degree 1, we need the initial monomials of degree 2, which are* x^2 *and* xy. f_2 *has already degree 3, and 1 is the only initial monomial of degree 0. Then*

$$\begin{aligned} 9\Re(x^2)f_1 &= (x^2+y^2+z^2)(x+y+z) \\ &= x^3+y^3+z^3+x^2y+xz^2+y^2z+x^2z+xy^2+yz^2 \\ 9\Re(x^2)f_1 &= 3(\Re(x^3)+\Re(x^2y)+\Re(x^2z)) \end{aligned}$$

$$\begin{aligned} \textit{and}\quad 9\Re(xy)f_1 &= (xy+xz+yz)(x+y+z) \\ &= x^2y+xz^2+y^2z+x^2z+xy^2+yz^2+3xyz \\ 9\Re(xy)f_1 &= 3(\Re(x^2y)+\Re(x^2z)+\Re(xyz)) \end{aligned}$$

Hence, the Invariant-Macaulay's matrix $M_{3,2}$ *is*

$$M_{3,2} = \begin{array}{c} \\ \Re(x^2).f_1 \\ \Re(xy).f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccc} \Re(x^3) & \Re(x^2y) & \Re(x^2z) & \Re(xyz) \end{array} \\ \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & 0 & -1 \end{pmatrix} \end{array}$$

Recall that the SAGBI-F_5 algorithm constructs matrices incrementally degree by degree and equation by equation. At each degree d the algorithm constructs a SAGBI-Macaulay's matrix $M_{d,i}$ and performs row reductions on them, the valid operations being to add to some

row a linear combinations of rows situed above. The incremental step from $i-1$ to i introduces the rows corresponding to $b_j^{d-d_i} f_i$ for all polynomials of $(b_j^{d-d_i})$ in the basis of $\mathcal{A}_{d-d_j}$, that do not have same leading monomial as a row in $\tilde{M}_{d-d_i,i-1}$, where $d_i = \deg(f_i)$. This criterion is a variant of the F_5-criterion and was explained in proposition 1.69. The algorithm stops when the current degree is equal to a given bound D.

SAGBI-F_5 example. We now give a complete example of the execution of the Matrix-SAGBI F_5 algorithm, in the invariant context. In this example, we follow the example 4.98 by using the same group $\mathbf{G}$ (the alternating group A_3) acting on the variables $X = [x, y, z]$. The ring $\mathbb{Q}[X]$ is ordered with the graded lexicographic ordering $\preceq$, such that $x > y > z$. We recall that $\mathcal{I} = \langle f_1, f_2 \rangle$ with $f_1 = \Re(x)$ and $f_2 = \Re(x^2y) - \Re(xyz)$. In this example, we want to compute the SG-basis of $\mathcal{I}^{\mathbf{G}} = \langle f_1, f_2 \rangle_{\mathbb{Q}[X]^{\mathbf{G}}}$ up to degree 5.

We start with $\mathcal{S}_1 = \mathcal{S}_2 = \emptyset$. In order to compute the SG-bases, we proceed degree by degree. In degree 1, we only have one row indexed by $\Re(1) \times f_1$:

$$\widetilde{M}_{1,1} = M_{1,1} = \begin{array}{l} \\ \Re(1) f_1 \end{array} \begin{array}{c} \Re(x) \\ \left(\begin{array}{c} 1 \end{array} \right) \end{array}$$

Since f_1 is not SG-top-reducible by $\mathcal{S}_1$ (which is empty !), we add f_1 to $\mathcal{S}_1$ and obtain $\mathcal{S}_1 = \{f_1\}$. Since f_2 has degree 3, the matrix $M_{1,2} = \widetilde{M}_{1,2}$ is equal to $M_{1,1}$ and we add f_1 to $\mathcal{S}_2$. In degree 2, we have a single row indexed by $\Re(x)f_1$:

$$\widetilde{M}_{2,1} = M_{2,1} = \begin{array}{l} \\ \Re(x) f_1 \end{array} \begin{array}{c} \Re(x^2) \quad \Re(xy) \\ \left(\begin{array}{cc} \frac{1}{3} & \frac{2}{3} \end{array} \right) \end{array}$$

The polynomial $\Re(x)f_1$ can be reduced by f_1, so we do not add another polynomial to the SG-basis $\mathcal{S}_1$ in degree 2. We will actually never add new polynomials to $\mathcal{S}_1$ since all the rows of matrices $M_{d,1}$ will be of the form $\Re(m)f_1$ and will be SG-top-reducible by f_1. As in degree 1, $M_{2,2} = M_{2,1}$. In degree 3, we construct the matrix $M_{3,1}$ whose rows are coefficients of the following polynomials:

$$\begin{aligned} \Re(x^2)f_1 &= \tfrac{1}{3}\Re(x^3) + \tfrac{1}{3}\Re(x^2y) + \tfrac{1}{3}\Re(x^2z) \\ \Re(xy)f_1 &= \tfrac{1}{3}\Re(x^2y) + \tfrac{1}{3}\Re(x^2z) + \tfrac{1}{3}\Re(xyz) \end{aligned}$$

Hence,

$$M_{3,1} = \begin{array}{l} \\ \Re(x^2)f_1 \\ \Re(xy)f_1 \end{array} \begin{array}{c} \Re(x^3) \quad \Re(x^2y) \quad \Re(x^2z) \quad \Re(xyz) \\ \left(\begin{array}{cccc} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{array} \right) \end{array}$$

It is obvious that $\widetilde{M}_{3,1} = M_{3,1}$. We obtain $M_{3,2}$ by adding f_2 to $\widetilde{M}_{3,1}$:

$$M_{3,2} = \begin{array}{l} \\ \Re(x^2)f_1 \\ \Re(xy)f_1 \\ f_2 \end{array} \begin{array}{c} \Re(x^3) \quad \Re(x^2y) \quad \Re(x^2z) \quad \Re(xyz) \\ \left(\begin{array}{cccc} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & 0 & -1 \end{array} \right) \end{array}$$

Then, after Gaussian elimination, we obtain:

$$\widetilde{M}_{3,2} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & -1 & -2 \end{pmatrix}.$$

Now we have obtained one new polynomial $f_3 = \Re(x^2z) + 4\Re(xyz)$, which is not SG-top-reducible by f_1, since $xz \notin \mathsf{LM}_{\preceq}(\mathbb{K}[X]^{\mathbf{G}})$. Then, we add f_3 to $\mathcal{S}_2$ and obtain $\mathcal{S}_2 = \{f_1, f_3\}$. In degree 4 we construct the matrix $M_{4,1}$ as above and obtain :

$$\widetilde{M}_{4,1} = M_{4,1} = \begin{array}{c} \\ \Re(x^3)f_1 \\ \Re(x^2y)f_1 \\ \Re(x^2z)f_1 \\ \Re(xyz)f_1 \end{array} \begin{array}{c} \begin{array}{ccccc} \Re(x^4) & \Re(x^3y) & \Re(x^3z) & \Re(x^2y^2) & \Re(x^2yz) \end{array} \\ \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

The unique initial monomial of degree 1 is x, but x is the leading monomial of a row of $\widetilde{M}_{4-3,2-1}$ (corresponding to $\Re(1)f_1$), so by applying the SAGBI-$F5$ criterion (lemma 1.69), there is nothing to do anymore in degree 4. In degree 5, we construct the matrix $M_{5,1}$ whose rows are the coefficients of the following polynomials:

$$\begin{aligned}
\Re(x^4)f_1 &= \tfrac{1}{3}\Re(x^5) + \tfrac{1}{3}\Re(x^4y) + \tfrac{1}{3}\Re(x^4z) \\
\Re(x^3y)f_1 &= \tfrac{1}{3}\Re(x^4y) + \tfrac{1}{3}\Re(x^3y^2) + \tfrac{1}{3}\Re(x^3yz) \\
\Re(x^3z)f_1 &= \tfrac{1}{3}\Re(x^4z) + \tfrac{1}{3}\Re(x^3z^2) + \tfrac{1}{3}\Re(x^3yz) \\
\Re(x^2y^2)f_1 &= \tfrac{1}{3}\Re(x^3y^2) + \tfrac{1}{3}\Re(x^3z^2) + \tfrac{1}{3}\Re(x^2y^2z) \\
\Re(x^2yz)f_1 &= \tfrac{1}{3}\Re(x^3yz) + \tfrac{2}{3}\Re(x^2y^2z)
\end{aligned}$$

Therefore, $M_{5,1}$ is equal to the following matrix:

$$\begin{array}{c} \\ \Re(x^4)f_1 \\ \Re(x^3y)f_1 \\ \Re(x^3z)f_1 \\ \Re(x^2y^2)f_1 \\ \Re(x^2yz)f_1 \end{array} \begin{array}{c} \begin{array}{ccccccc} \Re(x^5) & \Re(x^4y) & \Re(x^4z) & \Re(x^3y^2) & \Re(x^3yz) & \Re(x^3z^2) & \Re(x^2y^2z) \end{array} \\ \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{2}{3} \end{pmatrix} \end{array}$$

Once again, it is easy to see that $M_{5,1} = \widetilde{M}_{5,1}$. There are two leading monomials in degree 2, which are x^2 and xy. By using the SAGBI-$F5$ criterion we do not add the row $\Re(x^2)f_2$ to $M_{5,2}$, because the single row of $M_{2,1}$ has x^2 as leading monomial. In other words $M_{5,2}$ is the following matrix

$$\begin{array}{c} \\ \Re(x^4)f_1 \\ \Re(x^3y)f_1 \\ \Re(x^3z)f_1 \\ \Re(x^2y^2)f_1 \\ \Re(x^2yz)f_1 \\ \Re(xy)f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} \Re(x^5) & \Re(x^4y) & \Re(x^4z) & \Re(x^3y^2) & \Re(x^3yz) & \Re(x^3z^2) & \Re(x^2y^2z) \end{array} \\ \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & 0 & \frac{-2}{3} \end{pmatrix} \end{array}$$

After Gaussian elimination, we finally get:

$$\widetilde{M}_{5,2} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{5}{3} \end{pmatrix}$$

and the matrix $\widetilde{M}_{5,2}$ gives us a new polynomial $f_4 = \Re(x^3z^2) + 5\Re(x^2y^2z)$, not reducible by any element of $\mathcal{S}_2$. Then, the Matrix-SAGBI F_5 algorithm stops and returns $\mathcal{S}_1, \mathcal{S}_2$ with $\mathcal{S}_1 = \{f_1\}$ and $\mathcal{S}_2 = \{f_1, f_3, f_4\}$.

The complexity analysis of the Matrix-SAGBI F_5 algorithm in the case $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$ has been done almost entirely in chapter 2 and 3. Before giving the end of this analysis, we come back to the behavior of this algorithm with respect to regular sequences.

Links between $\mathbb{K}[X]^{\mathbf{G}}$-regular and $\mathbb{K}[X]$ regular sequences. For $\mathcal{A} = \mathbb{K}[X]^{\mathbf{G}}$ with $\mathbf{G}$ a finite group, we can prove that regularity implies $\mathcal{A}$-regularity, at least in the non-modular case: the Reynolds Operator plays a crucial role in the proof of the following proposition.

Proposition 4.99. *Let $\mathbf{G} \subset \mathcal{GL}_n(\mathbb{K})$ be a finite group with $\mathrm{char}(\mathbb{K}) \nmid |\mathbf{G}|$. Let $\mathsf{F} = (f_1, \ldots, f_s) \in \mathbb{K}[X]^{\mathbf{G}}$ be a regular sequence (in $\mathbb{K}[X]$). Then F is $\mathbb{K}[X]^{\mathbf{G}}$-regular.*

Proof. Let $(g_1, \ldots, g_s)$ be a family of polynomials in $\mathbb{K}[X]^{\mathbf{G}}$, such that $\sum_{i=1}^{s} g_i f_i = 0$. Since F is regular, each g_i belongs to the ideal generated in $\mathbb{K}[X]$ by $\mathsf{F}\backslash f_i$, so we can write $g_i = \sum_{j \neq i} h_j f_j$. Applying the Reynolds Operator, we obtain $g_i = \Re(g_i) = \sum_{j \neq i} \Re(h_j) f_j$. Hence, g_i belongs to $\langle \mathsf{F}\backslash f_i \rangle_{\mathbb{K}[X]^{\mathbf{G}}}$. It follows that F is $\mathbb{K}[X]^{\mathbf{G}}$-regular. □

Complexity. We now analyze the complexity of algorithm 1.68 in order to compute SAGBI bases in invariant rings. We assume that the computation of products of the form $b_i^d \times b_{i'}^{d'}$ (see subsection 3.1.1) has been done as far as needed and is not counted here: in particular this cost is negligible when the algebra $\mathcal{A}$ is a ring of invariant $\mathbb{K}[X]^{\mathbf{G}}$ with $\mathbf{G}$ a subgroup of matrices of generalized permutations. The main complexity result is the following theorem, which is very similar to the theorem 4.76, which gives a complexity bound on the computation of a Gröbner basis up to degree D of an ideal invariant under the action of a diagonal matrix group.

Theorem 4.100. *Let $\mathbf{G}$ be a matrix group with no uniform scalings, and let $\mathsf{F} = (f_1, \ldots, f_s)$ be a family of invariant homogeneous polynomials in $\mathbb{K}[X]^{\mathbf{G}}$. Then the complexity of computing a SAGBI Gröbner basis up to degree D for the DRL ordering of the ideal $\langle \mathsf{F} \rangle_{\mathbb{K}[X]^{\mathbf{G}}}$ is bounded by*

$$O\left(\frac{s}{|\mathbf{G}|^{\omega}} \binom{D+n}{D}^{\omega} \right)$$

operations in $\mathbb{K}$, with ω a feasible exponent of linear algebra.

Proof. Once the group $\mathbf{G}$ is fixed, we have seen in theorem 3.78 that the quotient of dimensions $\dim(\mathbb{K}[X]_d^{\mathbf{G}}) / \dim(\mathbb{K}[X]_d)$ tends to $1/|\mathbf{G}|$ as d grows to inifinity. The matrix M_d built by a SAGBI variant of the Lazard algorithm has $\dim(\mathbb{K}[X]_d^{\mathbf{G}})$ columns and $\sum_{i=1}^{s} \dim(\mathbb{K}[X]_{d-d_i}^{\mathbf{G}})$

rows if f_i is of degree d_i. Then, the proof ends by the same analysis than the complexity of the Lazard algorithm given in theorem 1.42.

□

The cost of computing Gröbner bases in the affine case is not known as well as for homogeneous systems, due to falls of degrees that could appear during the computations, see [93]. The same fact holds during SAGBI bases computations in the affine case, so we do not give complexity results here. However, proposition 3.83 shows that heuristically the matrices occuring during a SAGBI basis computation in $\mathbb{K}[X]^{\mathbf{G}}$ up to some given degree have number of rows and columns divided by a factor $|\mathbf{G}|$, compared to a Gröbner basis computation up to the same degree. We refer to subsection 4.3.4 for experimental results.

4.3.2 SAGBI-FGLM algorithm and general algorithm to obtain an invariant Gröbner basis

The main goal of this subsection is to show how a SAGBI basis in $\mathbb{K}[X]^{\mathbf{G}}$ can be used to compute a Gröbner basis with respect to a fixed set of invariants of $\mathbf{G}$, for example a collection of invariants of a pseudo-reflexive group $\mathbf{H}$ containing $\mathbf{G}$. We will present a more general algorithm, able to convert a SAGBI basis of any ideal $\mathcal{I}^{\mathcal{A}} = \langle f_1, \ldots, f_s \rangle_{\mathcal{A}}$ in a subalgebra $\mathcal{A} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ into a Gröbner basis in some ring $\mathbb{K}[H] = \mathbb{K}[H_1, \ldots, H_r]$. Each H_i represents a polynomial h_i in $\mathcal{A}$ and we assume that the ideal $\mathcal{I}$ generated by $\mathsf{F} = (f_1, \ldots, f_s)$ in $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ is zero-dimensional. We fix an ordering $\preceq_H$ compatible with a weighted degree on the variables H_i, depending on the degree of the polynomials h_i in the variables $(x_1, \ldots, x_n)$, namely $\mathsf{deg}_H(H_i) = \mathsf{deg}(h_i)$. Therefore, the weighted degree of a monomial in these new variables is given by $\mathsf{deg}_H(\prod H_i^{\alpha_i}) = \sum \alpha_i \mathsf{deg}(h_i)$. More precisely, the object we are interested in computing is $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$, the Gröbner basis of $\mathcal{J} = \tilde{\mathcal{J}} \cap \mathbb{K}[H]$, where

$$\tilde{\mathcal{J}} = \mathcal{I} + \langle H_1 - h_1(x_1, \ldots, x_n), \ldots, H_r - h_r(x_1, \ldots, x_n) \rangle$$

We call this Gröbner basis the $\mathbb{K}[H]$-Gröbner basis of $\mathcal{I}$. Notice that this ideal $\mathcal{J}$ and this kind of Gröbner bases have already been introduced in subsection 3.1.3 in the case of a ring of invariants, more precisely in definition 3.45. Since $\mathcal{I}$ is assumed to be zero-dimensional, $\tilde{\mathcal{J}}$) and $\mathcal{J}$ are also zero-dimensional. We first present the SAGBI-FGLM algorithm and finally explain how to use both *truncated versions* of SAGBI-F_5 and SAGBI-FGLM algorithms to obtain a zero-dimensional ideal in the ring $\mathbb{K}[H]$.

SAGBI-FGLM algorithm The idea of the following SAGBI-FGLM algorithm is to perform the same kind of computations as in the original FGLM algorithm 1.52, but with the knowledge of a SAGBI basis of $\mathcal{I}^{\mathcal{A}}$ instead of the Gröbner basis of $\mathcal{I}$. For any monomial $m = \prod H_i^{\alpha_i}$, we can compute $\mathsf{NF}_{\preceq}^{\mathsf{SG}}(m_h, \mathcal{S})$, with $\mathcal{S}$ a SAGBI basis of $\mathcal{I}^{\mathcal{A}}$ and m_h the monomial m where $h_i(x_1, \ldots, x_n)$ has been substituted to H_i. Since a SAGBI basis is usually not finite, the computations have to be done with a SAGBI basis up to some degree D. Hence, we will obtain a $\mathbb{K}[H]$-Gröbner basis of $\mathcal{I}$ up to degree D. Therefore, if D is greather or equal than the maximal weighted degree of the polynomials in $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$, the SAGBI-FGLM algorithm computes it exactly. Hence, this algorithm picks up monomials m in $\mathbb{K}[H]$, of degree less than or equal to D, by increasing term order for $\preceq_H$ and looks for linear combinations

$$\mathsf{NF}_{\preceq}^{\mathsf{SG}}(m_h, \mathcal{S}) + \sum_{u \prec_H m} c_u \mathsf{NF}_{\preceq}^{\mathsf{SG}}(u_h, \mathcal{S}) = 0$$

with the convention that m_h (respectively u_h) is the result of substituting H_i by $h_i(x_1, \ldots, x_n)$ in m (respectively u). Since we have assumed that $\mathsf{deg}_H(m) \leq D$, the result of the Normal-Form computation is precisely $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(m_h, \mathcal{I}^{\mathcal{A}})$. If there is no such relation then m is a member of the staircase in construction. Termination is assured by the fact that the number of terms with total degree less than or equal to D is finite. The SAGBI-FGLM algorithm is presented as algorithm 4.101.

Algorithm 4.101: SAGBI-FGLM

Input : - a SG-basis $\mathcal{S}$ up to degree D of $\mathcal{I}^{\mathcal{A}}$ with respect to $\preceq$
- a second monomial ordering $\preceq_H$ on $\mathbb{K}[H_1, \ldots, H_r]$, compatible with deg_H.
- polynomials $(h_1, \ldots, h_r) \in \mathcal{A}$

Output: a $\mathbb{K}[H]$-Gröbner basis of $\mathcal{I}^{\mathcal{A}}$ up to degree D with respect to $\preceq_H$

$L := [1]$; `//list of monomials in` $\mathbb{K}[H_1, \ldots, H_r]$
$S := [\,]$; `//staircase for the ordering` $\preceq_H$
$V := [\,]$; `//`$V =$ `SG-NormalForm`(S)
$G_D^H := [\,]$; `//The` $\mathbb{K}[H]$`-Gröbner basis up to degree` D `in` $\mathbb{K}[H_1, \ldots, H_r]$
while $L \neq [\,]$ **do**
  $m := L[1]$; and Remove m from L;
  $m_h :=$ replace $H_1, H_2, \ldots, H_r$ by $h_1, h_2, \ldots, h_r$ in m;
  $v := \mathsf{NF}^{\mathsf{SG}}_{\preceq}(m_h, \mathcal{S})$;
  $s := \#S$;
  if $v \in \mathit{Span}_{\mathbb{K}}(V)$ **then**
    we can find $(\lambda_i) \in \mathbb{K}^s$ such that $v = \sum_{i=1}^{s} \lambda_i \cdot V_i$;
    $G_D^H := G_D^H \cup \left[m - \sum_{i=1}^{s} \lambda_i \cdot S_i \right]$;
  else
    $S := S \cup [m]$; $V := V \cup [v]$;
    $L := \mathrm{Sort}(L \cup [H_i\, m \mid i = 1, \ldots, r], \preceq_H)$;
  Remove from L elements of graded degree $> D$ or duplicates elements;

Theorem 4.102. *SAGBI-FGLM algorithm computes the reduced $\mathbb{K}[H]$-Gröbner basis up to degree D of $\mathcal{I}^{\mathcal{A}}$ with respect to $\preceq_H$.*

Proof. Let G_D^H be the output set $\{g_1, \ldots, g_\mu\}$ of polynomials indexed in the order of their placement into G_D^H. Let $m_i = \mathsf{LM}_{\preceq}(g_i)$, which is the value of m when g_i is added to G_D^H. Clearly, $m_1 \prec_H \ldots \prec_H m_\mu$ and $m_j \nmid m_k$ for $j < k$. For each i, all the monomials of g_i except m_i are in the staircaise S, hence g_i is in normal form modulo $G_D^H \backslash \{g_i\}$. Therefore, G_D^H is reduced. Clearly, $g_i(h_1, \ldots, h_r) \in \mathcal{I}^{\mathcal{A}}$ because the SG-Normal Form of $g_i(h_1, \ldots, h_r)$ is equal to 0. To see that G_D^H is a Gröbner Basis up to degree D of the ideal

$$\mathcal{J} = \mathcal{I} + \langle H_1 - h_1(x_1, \ldots, x_n), \ldots, H_r - h_r(x_1, \ldots, x_n) \rangle \cap \mathbb{K}[H]$$

assume by contradiction that there exists a polynomial $f \in \mathbb{K}[H]$ of graded degree less than or equal to D with $f(h_1, \ldots, h_r) \in \mathcal{I}^{\mathcal{A}}$, such that the normal form of f modulo G_D^H is non-zero. We can assume that f is reduced modulo G_D^H, and that f has the smallest leading monomial among the polynomials of $\mathcal{I}^{\mathcal{A}}$ which do not reduce to 0 modulo G_D^H. With these assumptions,

all monomials of f but the leading monomial are in the staircase S. When $m = \mathsf{LM}_{\preceq}(f)$ in the algorithm, the if-condition must detect the linear dependance between m_h and $\mathsf{Span}_{\mathbb{K}}V$ because $f(h_1, \ldots, h_r)$ belongs to $\mathcal{I}^{\mathcal{A}}$, which is a contradiction and the theorem is proved. □

Remark 4.103. *Since the $\mathbb{K}[H]$-Gröbner basis $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$ is finite, there exists a D_0 such that G_D^H is equal to $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$ for all $D \geq D_0$. Of course, we do not know in advance the degree D_0 that we have to reach in SAGBI-F_5 algorithm. We will explain in the sequel how to avoid this difficulty.*

Example 4.104. *Consider the cyclic matrix group $\mathbf{G}$ of order 4 generated by $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ over a field of odd characteristic. It is easy to check that $\mathbb{K}[x,y]^{\mathbf{G}} = \mathbb{K}[h_1, h_2, h_3]$ where $h_1 = x^2 + y^2, h_2 = x^2y^2$ and $h_3 = xy(x^2 - y^2)$ (see for instance [25, chapter 7]). Let us consider the following invariant system:*

$$\begin{cases} f_1 = x^4 + y^4 - 1 = 2\Re(x^4) - \Re(1) = 0 \\ f_2 = x^3y^3(x^6 - y^6) - 2 = 2\Re(x^9y^3) - 2\Re(1) = 0 \end{cases}$$

The SAGBI basis up to degree 12 (for the DRL ordering) of the ideal $\mathcal{I}^{\mathbf{G}}$ generated by f_1, f_2 in $\mathbb{K}[x,y]^{\mathbf{G}}$ is simply $\mathcal{S} = \{f_1, \tilde{f}_2\}$ where $\tilde{f}_2 = 2\Re(x^7y^5) + 2\Re(x^5y^3) - 2\Re(1)$ is the SAGBI-reduction of f_2 by f_1. We take $\{\Re(m) \mid m$ is an initial monomial in $\mathbb{K}[x,y]^{\mathbf{G}}\}$ as a basis of $\mathbb{K}[x,y]^{\mathbf{G}}$. The staircase E (a basis of the vector space of elements of $\mathbb{K}[x,y]^{\mathbf{G}}$ that are not (top-) reducible by $\mathcal{S}$) is given by

$$E = \left\{\Re(m) \mid m \in \{1, x^2, x^2y^2, x^3y, x^4y^2, x^5y, x^4y^4, x^5y^3, x^6y^4, x^7y^3, x^6y^6\}\right\}$$

The following array contains the current m_h, the SG-Normal Form v of m_h modulo $\mathcal{S}$, the staircase in construction for the ordering $\preceq_H$ and a boolean testing if v lies in the vector space generated by the SG-Normal Form of elements of E modulo $\mathcal{S}$.

m_h	v	S	$v \in V$?
1	$\Re(1)$	$\emptyset$	*false*
h_1	$2\Re(x^2)$	$[1]$	*false*
h_3	$2\Re(x^3y)$	$[1, H_1]$	*false*
h_2	$\Re(x^2y^2)$	$[1, H_1, H_3]$	*false*
h_1^2	$2\Re(x^2y^2) + \Re(1)$	$[1, H_1, H_3, H_2]$	*true*

Since $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(h_1^2, \mathcal{S}) = 2\mathsf{NF}^{\mathsf{SG}}_{\preceq}(h_2, \mathcal{S}) + \mathsf{NF}^{\mathsf{SG}}_{\preceq}(1, \mathcal{S})$, the polynomial $g_1 = H_1^2 - 2H_2 - 1$ belongs to the invariant Gröbner basis of $\langle f_1, f_2\rangle$ in $\mathbb{K}[h_1, h_2, h_3]$ up to degree 12. At this step, L is equal to $[H_1H_3, H_1H_2, H_3^2, H_3H_2, H_2^2]$. The next steps of the computation are :

h_1h_3	$2\Re(x^5y)$	$[1, H_1, H_3, H_2]$	*false*
h_1h_2	$2\Re(x^4y^2)$	$[1, H_1, H_3, H_2, H_1H_3]$	*false*
h_3^2	$-2\Re(x^4y^4) + \Re(x^2y^2)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2]$	*false*
h_2h_3	$2\Re(x^5y^3)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2, H_3^2]$	*false*
h_2^2	$\Re(x^4y^4)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2, H_3^2, H_2H_3]$	*true*

And the polynomial $g_2 = H_2^2 + H_3^2/2 - H_2/2$ is added to the invariant Gröbner basis. After removing from L multiples of H_2^2, L is equal to $[H_1H_3^2, H_1H_2H_3, H_3^3, H_2H_3^2]$. The computation follows in this way:

$h_1h_3^2$	$-4\Re(x^6y^4) + 2\Re(x^4y^2)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2, H_3^2, H_2H_3]$	*false*
$h_1h_2h_3$	$2\Re(x^7y^3)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2, H_3^2, H_2H_3, H_1H_3^2]$	*false*
h_3^3	$6\Re(x^5y^3) - 4\Re(1)$	$[1, H_1, H_3, H_2, H_1H_3, H_1H_2, H_3^2, H_2H_3, H_1H_3^2]$	*true*

And finally $g_3 = H_3^3 - 3H_2H_3 + 4$ is added to the basis. Since we do not add to L monomials of weighted degree greather than 12, the only element remaining in L is $H_2H_3^2$, which does not give a new element to the basis, so the algorithm stops and returns $\{g_1, g_2, g_3\}$.

Since the algorithm F5-invariant is the costliest step, it is interesting to stop as soon as the polynomials given by the FGLM invariant algorithm form a zero dimensional ideal in $\mathbb{K}[H]$, even if the $\mathbb{K}[H]$-Gröbner basis is not complete. We now explain this idea.

General Algorithm. We now propose a general strategy, in order to compute a lexicographical Gröbner Basis in a ring $\mathbb{K}[H]$ of a system of equations $\mathsf{F} = (f_1, \ldots, f_s) \in \mathcal{A}^s$ generating a zero-dimensional ideal $\mathcal{I} = \langle \mathsf{F} \rangle_{\mathbb{K}[X]}$ in the ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ containing the graded algebra $\mathcal{A}$. The idea is to combine truncated versions of both SAGBI-F_5 and SAGBI-FGLM algorithms: since we do not know in advance the degree D needed in SAGBI-F_5 to obtain a SAGBI basis $\mathcal{S}$ of $\mathcal{I}^{\mathcal{A}} = \langle \mathsf{F} \rangle_{\mathcal{A}}$, which gives a zero-dimensional $\mathbb{K}[H]$-Gröbner basis with the SAGBI-FGLM algorithm, we proceed incrementally degree by degree. This idea is reported in algoritm 4.105. Termination is assured by the fact that a finite Gröbner basis exists in $\mathbb{K}[H]$. Since the first D giving a zero-dimensional ideal in $\mathbb{K}[H]$ is possibly smaller than the maximal degree of a polynomial in $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$, it could happen that the obtain polynomials in $\mathbb{K}[H]$ do not form a Gröbner basis. Hence we have to add a Gröbner basis computation in $\mathbb{K}[H]$. Since we are interested in a Gröbner basis for a lexicographic ordering in $\mathbb{K}[H]$, algorithm 4.105 ends with a use of the classical FGLM algorithm 1.52.

Remark 4.106. *In practice, it is very easy to check that G_D^H generates a zero-dimensional ideal, we check that for all $i \in \{1, \ldots, r\}$ we can find $g \in \mathcal{G}_{\preceq_H}^H$ such that $LT(g) = H_i^{\alpha_i}$ for some $\alpha_i \in \mathbb{N}$. To compute $\mathcal{G}_{lex}^H$, we simply apply the standard FGLM-algorithm to $\mathcal{G}_{\preceq_H}^H$.*

Example 4.107. *Go back to the example 4.104. At degree 12, the FGLM-invariant algorithm gives a zero-dimensional Gröbner basis $\{g_1, g_2, g_3\}$, which is already a Gröbner basis for $\preceq_H$ since no pair of leading monomials have a common factor. The ideal generated is zero-dimensional since $\mathsf{LM}_{\preceq}(g_i) = H_i^{\alpha_i}$ for some $\alpha_i \in \mathbb{N}$, so we can apply the classical FGLM algorithm. We get the following lexicographical Gröbner Basis:*

$$\begin{cases} 6H_1^2 + H_3^5 + 3H_3^3 + 4H_3^2 - 12 \\ 12H_2 + H_3^5 + 3H_3^3 + 4H_3^2 - 6 \\ H_3^6 + 3H_3^4 + 8H_3^3 - 6H_3 + 16 \end{cases}$$

We can find the values of h_1, h_2, h_3 by finding the roots of univariate polynomials of degree at most 6. Since $h_1 = x^2 + y^2$ and $h_2 = x^2y^2$, we can find the values of x^2 and y^2 by finding the roots of $z^2 - h_1z + h_2 = 0$, and then find x and y by taking square roots. A direct approach of the system $f_1 = f_2 = 0$ gives us the following irreducible polynomial :

$$P = 6y^{48} - 24y^{44} + 69y^{40} - 125y^{36} + 156y^{32} - 138y^{28} + 70y^{24} + 12y^{20} - 39y^{16} + 15y^{12} + 16$$

Algorithm 4.105: General algorithm

Input : $\mathsf{F} = (f_1, \ldots, f_s) \in \mathcal{A}^s$ generating a zero-dimensional ideal in $\mathbb{K}[X]$, and $h_1, \ldots, h_r$ homogeneous polynomials in $\mathcal{A}$.
Output: A lexicographical $\mathbb{K}[H]$-Gröbner basis of $\langle \mathsf{F}_{\mathcal{A}} \rangle_{\mathbb{K}[X]}$ in $\mathbb{K}[H_1, \ldots, H_r]$.
$D := \min_i \deg(f_i)$;
Do
  $\mathcal{S}$:=Sagbi-Gröbner basis of $\langle \mathsf{F}_{\mathcal{A}} \rangle$ up to degree D; `//Apply SAGBI-`F_5 `algorithm 1.68, with` $\preceq = \preceq_{\mathtt{DRL}}$
  G_D^H :=Invariant Gröbner basis up to degree D in $\mathbb{K}[H]$; `//Apply SAGBI-FGLM algorithm 4.101, with` $\preceq_H$ `the weighted DRL ordering`
  $\mathcal{G}^H_{\preceq_H}$:= Compute a Gröbner basis of G_D^H in $\mathbb{K}[H]$;
  if $\langle G_D^H \rangle$ *is zero-dimensional in* $\mathbb{K}[H]$ **then**
    $\mathcal{G}^H_{\mathrm{Lex}}$:= Compute a lexicographical Gröbner basis of $\langle G_D^H \rangle$; `//Apply the FGLM algorithm 1.52`
    return $\mathcal{G}^H_{Lex}$
  else
    $D := D + 1$;
Loop;

Since powers of y in P are multiples of 4, we have to compute the roots of a polynomial of degree 12.

In practice, we do not use algorithm 4.101 with a set of *fundamental invariants* of $\mathbf{G}$ (see subsection 3.1.3), but rather with a set of primary invariants of $\mathbf{G}$.

Example 4.108. *In this example, we take* $\mathbb{K} = \mathbb{F}_{65521}$, $\mathbf{H} \simeq (\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathfrak{S}_5 \subset \mathcal{GL}_5(\mathbb{K})$, $\mathbf{G} \simeq (\mathbb{Z}/2\mathbb{Z})^4 \rtimes D_5 \subset \mathbf{H}$ *where the subgroup of* $\mathbf{H}$ *isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^4$ *is the group of diagonal matrices having an even number of* -1 *on the diagonal, with other diagonal-coefficients equal to* 1 *and the subgroup* D_5 *is the dihedral matrix group generated by*

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$\mathbf{H}$ is a reflexive group (a Coxeter group, actually), with invariants:

$$h_1 = e_1(\underline{x_i}^2), \quad h_2 = e_2(\underline{x_i}^2), \quad h_3 = e_3(\underline{x_i}^2), \quad h_4 = e_4(\underline{x_i}^2), \quad h_5 = e_5(\underline{x_i})$$

where $e_j(\underline{x_i}^2)$ is the j-th symmetric function in the variable $x_1^2, \ldots, x_5^2$ and $e_5(\underline{x_i})$ is simply $x_1x_2x_3x_4x_5$. Now consider the following set of $\mathbf{G}$-invariant polynomials :

$$\mathsf{F} = \begin{cases} f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - 1 = 5\Re(x_1^2) - \Re(1) \\ f_2 = x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 - 1 = 5\Re(x_1^4) - \Re(1) \\ f_3 = x_1^2x_2^2 + x_1^2x_5^2 + x_2^2x_3^2 + x_3^2x_4^2 + x_4^2x_5^2 - 1 = 5\Re(x_1^2x_2^2) - \Re(1) \\ f_4 = x_1x_2x_3x_4x_5 - 1 = \Re(x_1x_2x_3x_4x_5) - \Re(1) \\ f_5 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 - 1 = 5\Re(x_1^6) - \Re(1) \end{cases}$$

Using algorithm SAGBI-F_5 up to degree 24, we get a SG-basis of $\mathcal{I}^{\mathbf{G}}$ of size 73. Applying SAGBI-FGLM algorithm, we get the following very simple $\mathbb{K}[H]$-Gröbner basis:

$$\mathcal{G}^H_{\preceq_H} = [H_1-1, H_2, H_3, H_4^6-10488H_4^5+5251H_4^4-10492H_4^3-5271H_4^2+28927H_4+18242, H_5-1]$$

This $\mathbb{K}[H]$-Gröbner basis gives rise to an ideal whose associated variety has only 6 points. Notice that $|\mathbf{H}| = 3200$ and $|\mathbf{G}| = 160$, so these 6 points correspond to $6 \times |\mathbf{G}| = 960$ elements associated to the ideal generated by F in $\mathbb{K}[x_1, \ldots, x_n]$. The expressions of $(h_j)_{1\leq j\leq 5}$ in terms of $(x_i)_{1\leq i\leq 5}$ allow us to recover the possible $(x_i)_{1\leq i\leq 5}$ from a value of $(h_j)_{1\leq j\leq 5}$ very fast but these possible 5-tuples are $6 \times |\mathbf{H}| = 19200$. We explain in the following subsection how to remove these spurious solutions.

Remark 4.109. *Since we stop as soon as we obtain a zero-dimensional ideal in algorithm 4.105, it could happen that $\langle \mathcal{G}^H_D \rangle \subsetneq \langle G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H) \rangle$. This fact would lead to more spurious solutions, but in practice, on all examples we have computed, the Gröbner basis $\mathcal{G}^H_D$ is exactly $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$.*

Complexity. We now give an estimation of the complexity of the SAGBI-FGLM algorithm 4.101, assuming that we have computed a SAGBI basis at a degree D equal to the remaining degree to find a zero-dimensional ideal. The complexity evaluation involves several quantities, that we define now.

Notations 4.110. *Let $\mathcal{S}$ be the output of the algoritm 1.68. We denote by:*
- *E the* staircase *of $\mathcal{S}$, namely the elements of $\cup_{d=0}^{D}\{b_i^d \mid 1 \leq i \leq n_d\}$, that are not (top-)reducible by $\mathcal{S}$.*
- *δ_H the degree of the ideal, that we obtain in $\mathbb{K}[H]$, with algorithm 1.68.*

In practice, as in the classic FGLM algorithm 1.52, we compute the SG-NormalForm v and check the linear dependance between v and V by using linear algebra, but there is a slight difference with the FGLM algorithm, since we do not compute multiplication matrices to compute v. However, in order to check the linear dependance between v and V, we use a matrix of size $|E| \times |E|$ and an Update procedure exactly as in the classical FGLM algorithm. To compute $v = \mathsf{NF}^{\mathsf{SG}}_{\preceq}(m_h, \mathcal{S})$, we use the knowledge of the matrix $\widetilde{M_{d,s}}$ computed by the SAGBI-F_5 algorithm. This matrix has $\sum_{d=0}^{D} \dim(\mathcal{A}_d)$ columns, and smaller or equal number of rows. Since m_h has degree less than or equal to d, we can construct a row-vector giving the expression of m_h in terms of $\cup_{d=0}^{D}\{b_i^d \mid i = 1 \ldots n_d\}$ and compute $\mathsf{NF}^{\mathsf{SG}}_{\preceq}(m_h, \mathcal{S})$ by a Gaussian elimination in $O\left(\left(\sum_{d=0}^{D} \dim(\mathcal{A}_d)\right)^2\right)$ arithmetic operations. In order to compute the Gröbner basis in $\mathbb{K}[H]$, we have to perform this operation at most $O(r \cdot \delta_H)$ times (the size of the staircase and the boundary of the ideal in $\mathbb{K}[H]$) therefore the total cost of computing the SAGBI Normal forms is bounded by $O\left(r \cdot \delta_H \left(\sum_{d=0}^{D} \dim(\mathcal{A}_d)\right)^2\right)$. Since the cost of testing the membership of m_h and updating the "base change matrix" is identical in the classical FGLM algorithm, we conclude that

Theorem 4.111. *With previous notations, the cost of computing the Gröbner basis in $\mathbb{K}[H]$ at degree D with the SAGBI-FGLM algorithm 4.101 is bounded by*

$$O\left(r\delta_H \left(\sum_{d=0}^{D} \dim(\mathcal{A}_d)\right)^2 + r|E|^3\right)$$

arithmetic operations in $\mathbb{K}$.

Heuristically, in the case of a ring of invariant, δ_H is very small, and $|E| \simeq \mathsf{deg}(I)/|\mathbf{G}|$. Work has to be done to prove it properly, but this cost is in practice very small, compared to the cost of the SAGBI-F_5 algorithm.

4.3.3 Removing spurious solutions

In the previous subsections, we have explained how to compute a $\mathbb{K}[H]$-Gröbner basis of the zero-dimensional ideal $\mathcal{I}$, which can be supposed to be $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$, according to remark 4.109. If it is not the case, we would have more spurious solutions to remove, but the following algorithms would work as well. The aim of this subsection is to remove the spurious solutions and compute the variety $\mathbb{V}(\mathcal{I})$, using the knowledge of polynomials in $G_{\mathbb{K}[H]}(\mathcal{I}, \preceq_H)$. To this end, we propose three approaches. The two first ones deal with an ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ generated by polynomials invariant under a group $\mathbf{G}$ which is a subgroup of a reflexive group $\mathbf{H}$. More exactly, in the first one, we assume that $\mathbf{H}$ is a direct product of groups of the form $G(\mu, \pi, n)$ (in the classification of Shephard and Todd [92]), since their invariants have a simple form and allow an easy reconstrution of the solutions (x_i) by numerical approach. The second and the last ones can be applied in the general case of an ideal in some graded algebra, but need some precomputation. We finally compare the complexity of these approaches.

4.3.3.1 First approach: exhaustive search and numerical approximation

In this subsubsection, we assume that $\mathbf{H}$ is a product of reflexive subgroups of the form $G(\mu_i, \pi_i, n_i)$ defined hereafter.

Definition – Proposition 4.112. *[92] Let $\mu, \pi, n \geq 1$ with $\pi | \mu$, and let ξ be a μ-primitive root of 1 in $\mathbb{K}$. The matrix group $G(\mu, \pi, n)$ is the subgroup of $\mathcal{GL}_n(\mathbb{K})$ of matrices with only one non-zero coefficient per row and column and each coefficient is a μ-root of 1. These non-zero coefficients are of the form $\xi^{\alpha_1}, \ldots, \xi^{\alpha_n}$, and we assume in addition that $\sum \alpha_i \equiv 0 [\pi]$. This is a subgroup of cardinal $\mu^n n!/\pi$ of the already seen group of generalized permutations.*

It is easy to prove that this kind of group is generated by reflections. In the non-modular case, according to theorem 3.36, this is a sufficient condition for the ring of invariants to be a polynomial ring. This is actually true in the modular case, moreover a set of invariants is very easy to exhibit:

Proposition 4.113. *With e_j the j-th symmetric function in n variables, the polynomials defined by:*

$$h_j = e_j(x_1^\mu, \ldots, x_n^\mu) \quad \textit{for} \quad 1 \leq j \leq n-1 \qquad \textit{and} \qquad h_n = e_n(x_1, \ldots, x_n)^{\mu/\pi}$$

are such that $\mathbb{K}[x_1, \ldots, x_n]^{G(\mu,\pi,n)} = \mathbb{K}[h_1, \ldots, h_n]$.

Now assume that $\mathbf{H} = \prod_{i=1}^{\ell} G(\mu_i, \pi_i, n_i)$ with $n_1 + \cdots + n_\ell = n$. The groups $G(\mu_i, \pi_i, n_i)$ act on distinct sets of variables $\{x_{i,1}, \ldots, x_{i,n_i}\}$, thus $\mathbf{H}$ is a reflexive group: $\mathbb{K}[X]^{\mathbf{H}} = \mathbb{K}[x_{i,j}]^{\mathbf{H}}$ can be written $\mathbb{K}[h_{1,1}, \ldots, h_{1,n_1}, h_{2,1}, \ldots, h_{\ell,n_\ell}]$, with $\{h_{i,1}, \ldots, h_{i,n_i}\}$ the invariants given in proposition 4.113 for $G(\mu_i, \pi_i, n_i)$ acting on $\{x_{i,1}, \ldots, x_{i,n_i}\}$. Let $\mathbf{G}$ be a subgroup of $\mathbf{H}$ and $f_1, \ldots, f_s$ be polynomials invariant under $\mathbf{G}$, generating an ideal $\mathcal{I}$ in $\mathbb{K}[x_{i,j}]$. With the general algorithm presented in the previous subsection, we obtain the lexicographical invariant

Gröbner basis $\mathcal{G}_{\mathbb{K}[h_{i,j}]^{\mathbf{H}}}(\mathcal{I})$ of the ideal $\mathcal{J}_{\mathbf{H}}$ in $\mathbb{K}[X]^{\mathbf{H}}$. We denote by $\mathbb{V}(\mathcal{J}_{\mathbf{H}})$ the corresponding variety in $\overline{\mathbb{K}}$. For $(b_{i,j}) \in \overline{\mathbb{K}}^n$ a point in $\mathbb{V}(\mathcal{J}_{\mathbf{H}})$, we can construct at most

$$\frac{\mu_1^{n_1} n_1!}{\pi_1} \times \cdots \times \frac{\mu_\ell^{n_\ell} n_\ell!}{\pi_\ell}$$

points $(a_{i,j})$ of $\overline{\mathbb{K}}^n$ such that the invariants $h_{i,j}$ take the value $(b_{i,j})$ on these points $(a_{i,j})$. Let $\mathbf{a} = (a_{i,j})$ be one of them, then this set $\{(a_{i,j})\}$ can be written $\mathbf{H}.\mathbf{a}$. All elements of the orbit $\mathbf{H}.\mathbf{a}$ are not necessary elements of $\mathbb{V}(\mathcal{I})$, because $f_1, \ldots, f_s$ are not assumed to be invariant under $\mathbf{H}$. The algorithm 4.114 removes spurious solutions: the idea is to check for all $\mathbf{a} \in \mathbb{V}(\mathcal{J}_{\mathbf{H}})$ and A in $\mathbf{H}$ if $A.\mathbf{a}$ belongs to $\mathbb{V}(\mathcal{I})$. Since $\mathbb{V}(\mathcal{I})$ is invariant under $\mathbf{G}$, the value of $A.\mathbf{a}$ is the same while A describes a coset in $\mathbf{H}/\mathbf{G}$. Hence, we can identify a coset with one of its element and check only if $A.\mathbf{a} \in \mathbb{V}(\mathcal{I})$ for each $A \in \mathbf{H}/\mathbf{G}$.

Algorithm 4.114: Removing spurious solutions by exhaustive search

Input : $F = [f_1, \ldots, f_s]$, $\mathbf{G}$, $\mathbf{H}$ and the variety $\mathbb{V}(\mathcal{J}_{\mathbf{H}}) \subset \overline{\mathbb{K}}^n$
Output: The variety $\mathbb{V}(\mathcal{I})$
$V := \{\}$;
for $\mathbf{b} = (b_{i,j})_{1 \le i \le \ell, 1 \le j \le n_i} \in \mathbb{V}(\mathcal{J}_{\mathbf{H}})$ **do**
  for $i = 1$ **to** ℓ **do**
    $g_i(x) := x^{n_i} - b_{i,1} x^{n_i - 1} + \cdots + (-1)^{n_i} b_{i,n_i}^{\pi_i}$;
    Compute the multiset $\{c_{i,j} \mid j \in \{1, \ldots, n_i\}\}$ of roots of g_i;
    Extract μ_i-roots of each $c_{i,j}$, denoted by $a_{i,j}$;
    Compute ξ_i, a primitive μ_i-root of 1;
    while $(\prod_j a_{i,j})^{\mu_i/\pi_i} \neq b_{i,n_i}$ **do**
      $a_{i,1} := \xi_i a_{i,1}$;
  $\mathbf{a} := (a_{i,j})_{1 \le i \le \ell, 1 \le j \le n_i}$;
  for $A \in \mathbf{H}/\mathbf{G}$ **do**
    if $f_1(A.\mathbf{a}) = \cdots = f_s(A.\mathbf{a}) = 0$ **then** $V := V \cup \{A.\mathbf{a}\}$;
return V;

Theorem 4.115. *Algorithm 4.114 outputs the variety* $\mathbb{V}(\mathcal{I})$.

Proof. Since $\mathbb{V}(\mathcal{I})$ is $\mathbf{G}$-invariant, it is clear with the last **if** condition that the output is contained in $\mathbb{V}(\mathcal{I})$. Let $\mathbf{v} = (v_{i,j})_{1 \le i \le \ell, 1 \le j \le n_i}$ be in $\mathbb{V}(\mathcal{I})$, then $(b_{i,j}) = (h_{i,j}(\mathbf{v}))$ belongs to $\mathbb{V}(\mathcal{J}_{\mathbf{H}})$. Let $\mathbf{c} = (c_{i,j})$ and $\mathbf{a} = (a_{i,j})$ be as in the algorithm. Clearly, for each i, $h_{i,j}(\mathbf{a}) = b_{i,j}$ for $1 \le j \le n_i - 1$ and this equality is maintained during the **while** loop. Moreover, $h_{i,n_i}(\mathbf{a})^{\pi_i} = b_{i,n_i}^{\pi_i}$ so $h_{i,n_i}(\mathbf{a})$ and b_{i,n_i} are equal, up to multiplication by a π_i-root of 1. Since ξ_i is a μ_i-primitive root of 1, at each step in the **while** loop $h_{i,n_i}(\mathbf{a})$ is multiplied by the same π_i-primitive root of 1, so the loop ends with $h_{i,n_i}(\mathbf{a}) = b_{i,n_i}$. Since the values of $h_{i,j}$ on $\mathbf{a}$ and $\mathbf{v}$ are the same, they are in the same orbit under the action of $\mathbf{H}$, so $\mathbf{v}$ will be in some set $A.\mathbf{a}$, which ends the proof. □

Example 4.116. *We consider the Cyclic-5 problem on* $\mathbb{Q}$*, see for instance example 4.51 for the definition. Using the SAGBI* F_5 *algorithm, we compute a SG-basis of the ideal* $\mathcal{I}^{D_5}$ *up to degree* 8*; then, thanks to the algorithm SAGBI-FGLM, we first obtain an invariant Gröbner*

basis up to degree 8, with respect to the weighted DRL ordering on the symmetric functions, given by:

$$G_{\mathbb{K}[\sigma_1,\ldots,\sigma_5]^{\mathfrak{S}_5}}(\mathcal{I},\prec) \supseteq \left[{\sigma_2}^3 + 5\,{\sigma_3}^2, {\sigma_2}^2\sigma_3 - 25\,\sigma_2, \sigma_2\,{\sigma_3}^3 + 5\,{\sigma_2}^2, \sigma_1, \sigma_4, \sigma_5 - 1\right]$$

If we compute a Gröbner basis of the previous set, we obtain the complete invariant Gröbner basis for the weighted DRL ordering (to obtain it directly, we would have to go to degree 9 in the SAGBI F_5 algorithm)

$$G_{\mathbb{K}[\sigma_1,\ldots,\sigma_5]^{\mathfrak{S}_5}}(\mathcal{I},\prec) = \left[{\sigma_2}^3 + 5\,{\sigma_3}^2, {\sigma_2}^2\sigma_3 - 25\,\sigma_2, \sigma_2\,{\sigma_3}^2 - 25\,\sigma_3, {\sigma_3}^3 + 5\,{\sigma_2}^2, \sigma_1, \sigma_4, \sigma_5 - 1\right]$$

and then by applying again the classical FGLM algorithm we obtain the lexicographical Gröbner basis:

$$\mathcal{G} := \left[\ \sigma_5 - 1, \sigma_4, \sigma_3^6 + 3125\,\sigma_3, 125\sigma_2 + \sigma_3^4, \sigma_1\ \right]$$

The ideal generated by this Gröbner Basis is radical, and we obtain easily a prime decomposition given by the three following Gröbner bases :

$$\mathcal{G}_1 = [\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 - 1] \qquad \mathcal{G}_2 = [\sigma_1, \sigma_2 + 5, \sigma_3 + 5, \sigma_4, \sigma_5 - 1]$$

and $\mathcal{G}_3 = \left[\sigma_1, 25\sigma_2 + \sigma_3^3 - 5\sigma_3^2 + 25\sigma_3 - 125, \sigma_3^4 - 5\sigma_3^3 + 25\sigma_3^2 - 125\sigma_3 + 625, \sigma_4, \sigma_5 - 1\right]$

Let $\mathbb{U}_5$ be the set of the fifth-root of 1 in $\mathbb{C}$, we are now able to compute $\mathbb{V}_{\mathbb{C}}(\mathcal{G})$ using this prime decomposition. This variety has cardinal 6 and can be expressed by radicals:

$$\mathbb{V}_{\mathbb{C}}(\mathcal{G}) = \{(0,0,0,0,1)\} \cup \{(0, -5\omega^2, -5\omega^3, 0, 1) \mid \omega \in \mathbb{U}_5\}$$

Then we compute the cosets of $\mathfrak{S}_5/D_5$, which are the cosets of these elements :

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

We now apply algorithm 4.114.

Case 1. *$b = (0,0,0,0,1)$. Then $g = x^5 - 1$. The roots of g are the fifth roots of 1 and we can take $a = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$, with $\alpha = e^{\frac{2i\pi}{5}}$. We obtain the two subsets of $\mathbb{V}_{\mathbb{C}}(\mathcal{I})$: $D_5.a$ and $D_5.(1\ \ 2\ \ 4\ \ 3).a$.*

Case 2. *For each $\omega \in \mathbb{U}_5$, we have : $b = (0, -5\omega, -5\omega^2, 0, 1)$, then $g = x^5 - 5wx^3 + 5w^2x^2 - 1$, whose roots are the components of $a = (\omega, \omega, \omega, \frac{-3-\sqrt{5}}{2}\omega, \frac{-3+\sqrt{5}}{2}\omega)$. Because of multiplicities of the roots of g, we obtain several elements of $\mathfrak{S}_5/D_5$ which give rise to the same orbit. Only one is solution : $D_5.a$.*

To summerize, the variety $\mathbb{V}_{\mathbb{C}}(\mathcal{I})$ has cardinal 70 and is given by

$$\bigcup_{\omega\in\mathbb{U}_5} D_5.(\omega, \omega, \omega, \frac{-3-\sqrt{5}}{2}\omega, \frac{-3+\sqrt{5}}{2}\omega) \quad \bigcup \quad \bigcup_{\omega\in\{e^{\frac{2i\pi}{5}}, e^{\frac{4i\pi}{5}}\}} D_5.(1, \omega, \omega^2, \omega^3, \omega^4)$$

Remark 4.117. *Of course, for general problems we have to take numerical approximations of the roots of points in $\mathbb{V}(\mathcal{J}_{\mathbf{H}})$ and roots of g_i, since the solutions are not given by radicals in the general case.*

In the next subsubsection, we will introduce a new object for removing the spurious solutions, by working only in the base field.

4.3.3.2 Triangular sets, divided differences and triangular approach

In this subsubsection, we introduce the notion of triangular sets of polynomials, which will be useful to describe the two other methods used to remove spurious solutions. The well known divided differences of a univariate polynomial (already defined in subsection 4.1.2) form such a triangular set and are related to the symmetric group $\mathfrak{S}_n$. We will see that we can obtain a triangular set from every group or even in a graded algebra. From now on and until the end of the subsubsection, $\preceq$ will denote the lexicographical ordering.

Definition 4.118. *Let $\mathbb{K}[Y] = \mathbb{K}[y_1, \ldots, y_r]$ be a polynomial ring, ordered by lexicographical ordering such that $y_1 \succ \cdots \succ y_r$. We say that a set of r polynomials $T = \{P_1, \ldots, P_r\} \in \mathbb{K}[Y]$ forms a triangular set if $\mathsf{LM}_{\preceq}(P_i)$ is a power of y_i for all $i \in \{1, \ldots, r\}$. Moreover, we assume that T is reduced, which means that $\mathsf{NF}_{\preceq}(P_i, [P_{i+1}, \ldots, P_r]) = P_i$ for all i.*

Proposition 4.119. *With the previous definition, it is obvious that a triangular set of polynomials is a reduced Gröbner basis of a zero-dimensional ideal for lexicographic ordering. Moreover, the degree of such an ideal is $\prod_{i=1}^{r} \mathsf{deg}(P_i)$.*

We recall here the definition of the divided differences for a univariate polynomial.

Definition – Proposition 4.120. *For a univariate polynomial $c(x)$ of degree n in $\mathbb{K}[x]$, we define n polynomials $c_1, \ldots, c_n$ of $\mathbb{K}(x_1, \ldots, x_n)[x]$ by $c_n(x) = c(x)$ and $c_i(x) = \frac{c_{i+1}(x) - c_{i+1}(x_{i+1})}{x - x_{i+1}}$ for all i in $\{1, \ldots, n-1\}$. Since $c_i \in \mathbb{K}[x_{i+1} \ldots x_n][x]$ and $\mathsf{deg}_x(c_i) = i$, the n polynomials $c_1(x_1), \ldots, c_n(x_n)$ belong to $\mathbb{K}[x_1, \ldots, x_n]$ and are called the* divided differences of the polynomial c.

Observe that the computation of divided differences can be down with a monic polynomial with variables $\sigma_1, \ldots, \sigma_n$ as coefficients, instead of elements of $\mathbb{K}$:

Example 4.121. *Let $c(x) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 \in \mathbb{K}[\sigma_1, \sigma_2, \sigma_3][x]$. The divided differences of c are very easy to compute and are:*

$$c_1 = x_1 + x_2 + x_3 - \sigma_1 \qquad c_2 = x_2^2 + x_2 x_3 - x_2 \sigma_1 + x_3^2 - x_3 \sigma_1 + \sigma_2 \qquad c_3 = x_3^3 - \sigma_1 x_3^2 + \sigma_2 x_3 - \sigma_3$$

We can now reformulate our problem of removing spurious solutions with the divided differences. Assume that $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ is a zero-dimensional ideal generated by polynomials $f_i \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbf{G}}$, with $\mathbf{G}$ a subgroup of $\mathfrak{S}_n$. We have seen in the previous subsection how to obtain, a $\mathfrak{S}_n$-invariant Gröbner basis of $\mathcal{I}$ in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$, for lexicographic ordering with $\sigma_1 \succ \cdots \succ \sigma_n$. Since this Gröbner basis generates also a zero-dimensional ideal, it contains a polynomial with leading monomial a power of σ_i for all i. Extracting this set of polynomials and adding the divided differences of the polynomial $c(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ (and performing some reductions), we obtain a triangular set T in $\mathbb{K}[x_1, \ldots, x_n, \sigma_1, \ldots, \sigma_n]$. Let E be the set of polynomials $\{f_1, \ldots, f_s\}$ (reduced with respect to T), together with the polynomials in the invariant Gröbner basis not in the triangular set.

Example 4.122. *Consider the ideal $\mathcal{I}$ generated by the following polynomials in $\mathbb{Q}[x_1, x_2, x_3]$:*

$$f_1 = x_1 + x_2 + x_3 \qquad f_2 = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \qquad f_3 = x_1 x_2 x_3 - 1$$

The polynomials f_1, f_2 and f_3 are invariant under the action of the alternate group $\mathfrak{A}_3$. We find easily the $\mathfrak{S}_3$-invariant Gröbner basis of the system, which is $[\sigma_1, \sigma_2^3 + 9, \sigma_3 - 1]$, and

is already a triangular set in $\mathbb{Q}[\sigma_1, \sigma_2, \sigma_3]$. *Adding to this set the divided differences computed in example 4.121, and after performing some reductions, we obtain:*

$$T = \{x_1 + x_2 + x_3, x_2^2 + x_2x_3 + x_3^2 + \sigma_2, x_3^3 + \sigma_2x_3 - 1, \sigma_1, \sigma_2^3 + 9, \sigma_3 - 1\}$$

It is clear that the polynomials f_1 *and* f_3 *reduced to 0 with respect to* T, *but* f_2 *does not. So, in this example, the set* E *consists in a single polynomial:*

$$E = \{\mathsf{NF}_{\preceq}(f_2, T)\} = \{-3x_2x_3^2 - \sigma_2x_2 + \sigma_2x_3 - 3\}$$

To remove spurious solutions, we are interested in computing $\mathbb{V}(\langle T \cup E\rangle)$. Before explaining how to remove spurious solutions, we explain how to generalize to other groups than $\mathfrak{S}_n$:

Proposition 4.123. *Let* $\mathbf{H}$ *be a reflexive group, and* $h_1, \ldots, h_n$ *be* n *invariants such that* $\mathbb{K}[X]^{\mathbf{H}} = \mathbb{K}[h_1, \ldots, h_n]$. *With new variables* $H_1, \ldots, H_n$, *we can reverse the relations between* $x_1, \ldots, x_n$ *and* $h_1, \ldots, h_n$ *by computing a lexicographical Gröbner basis of the ideal* $\langle H_i - h_i, i \in \{1, \ldots, n\}\rangle$ *with* $x_1 > x_2 > \cdots > x_n > H_1 > \cdots > H_n$. *In the case where* $\mathbf{H} = \mathfrak{S}_n$, *we obtain exactly the divided differences.*

The difference between this general case and the case of divided differences is that the Gröbner basis of the previous proposition contains polynomials with leading monomials equal to a power of x_i for all i, but also other polynomials. But we can add these polynomials to E and the following algorithms will also compute the interesting variety.

Example 4.124. *Go back to example 4.122. Removing the useless variables* σ_1 *and* σ_3, *the set* $T = \{T_1, T_2, T_3, T_4\}$ *is a triangular set in* $\mathbb{K}[x_1, x_2, x_3, \sigma_2]$ *consisting in four polynomials with leading monomials* x_1, x_2^2, x_3^3 *and* σ_2^3, *The set* E *has only one polynomial denoted by* $f = -3x_2x_3^2 - \sigma_2x_2 + \sigma_2x_3 - 3$. *Observe that* $\mathsf{LC}_{x_2}(f) = -3x_3^2 - \sigma_2$ *is invertible in* $Q[x_1, x_2, x_3, \sigma_2]/\langle T\rangle$ *with inverse* $g = (6\sigma_2x_3^2 + 9x_3 + 4\sigma_2^2)/9$. *Then, the polynomial* $\tilde{f} = \mathsf{NF}_{\preceq}(f \times g, T) = x_2 - x_3^2\sigma_2 - x_3 - \frac{2}{3}\sigma_2^2 \in \langle T \cup E\rangle$ *is monic in the variable* x_2, *so the polynomials* $T_1, \tilde{f}, T_3, T_4$ *form a triangular set, denoted by* $\tilde{T}$. *Since* $\mathsf{NF}_{\preceq}(T_2, \tilde{T}) = 0$, *we have exactly* $\langle T \cup E\rangle = \langle \tilde{T}\rangle$: *we have removed the spurious solutions because the projection of the variety associated to* $\tilde{T}$ *on the three first variables* x_1, x_2, x_3 *is exactly the variety associated to* $\mathcal{I}$.

We now come to the general approach. Now T denotes a triangular set in some polynomial ring $\mathbb{K}[y_1, \ldots, y_r]$, and E denotes a set of polynomials in $\mathbb{K}[y_1, \ldots, y_r]$. The idea is the same as in example 4.124, but the output could be more than one triangular set, since we obtain a *triangular decomposition* of the ideal $\langle T \cup E\rangle$.

Definition 4.125. *Let* $\mathcal{J}$ *be a zero-dimensional ideal of* $\mathbb{K}[y_1, \ldots, y_r]$. *A triangular decomposition of* $\mathcal{J}$ *is a list* $\mathcal{J}_1, \ldots, \mathcal{J}_\ell$ *of triangular ideals in* $\mathbb{K}[y_1, \ldots, y_r]$, *such that* $\mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{J}_1) \cup \cdots \cup \mathbb{V}(\mathcal{J}_\ell)$

A triangular decomposition is a nice way of manipulating solutions of a polynomial system, because the coefficients of the polynomials lie in $\mathbb{K}$ and the composition allows to compute exact or approximate solutions (depending of $\mathbb{K}$) by solving univariate polynomials. Daniel Lazard [73] gave an algorithm to compute a triangular decomposition of a zero dimensional ideal from a Gröbner Basis of the ideal for the lexicographic ordering. Here, we want to compute this decomposition without previously computing a Gröbner basis.

Following the idea of example 4.124, we will pick up a polynomial in E, and try to invert its leading coefficient (as a univariate polynomial in its main variable) with respect

to the triangular set T. The aim of inverting polynomials modulo a triangular ideal gives the following algoritm 4.126, which is recursive. During the execution of the algorithm, one inversion could fail, which leads to a decomposition of the triangular set $T = \{T_1 \succ \cdots \succ T_r\}$ into two triangular sets. More exactly, in this case one polynomial T_k of T is splitted into two factors T_k^1 and T_k^2 modulo polynomials in T smaller than T_k, which means that $T_k - T_k^1 T_k^2 \in \langle T_{k+1}, \ldots, T_\ell \rangle$. Notice that to invert a polynomial P modulo T, we only need polynomials in T with main variable equal or smaller than the leading variable of P. Thus, the algorithm is written assuming that the leading variable of P, $\mathsf{LV}_{\preceq}(P)$ is equal to $\mathsf{LV}_{\preceq}(T_1) = y_1$. At every recursive step, we had to take only the polynomials of T with smaller or equal leading variable than the polynomial we want to invert, and if this polynomial P is a scalar, we return $1/P$.

Algorithm 4.126: Inversion Algorithm

Input : $0 \neq P \in \mathbb{K}[y_1, \ldots, y_r]$ and a triangular set $T = \{T_1 \succ \cdots \succ T_r\}$ such that $P = \mathsf{NF}_{\preceq}(P, T)$ and $\mathsf{LV}_{\preceq}(P) = \mathsf{LV}_{\preceq}(T_1) = y_1$.
Output: A decomposition $T_k = T_k^1 T_k^2 \mod \langle T_{k+1}, \ldots, T_r \rangle$ or the inverse of P mod T, that is a polynomial Q such that $PQ = 1 \mod T$.

```
c := LC_{y_1}(P); // so P = c y_1^α + o(c y_1^α)
d := Inversion(c, T);
if we obtain a decomposition then
    return the decomposition;
else
    P̃ := NF_⪯(dP, T); //since cd = 1 mod T, P̃ = y_1^α + o(y_1^α).
    Compute a and b such that T_1 = a + bP̃ mod ⟨T_2, ..., T_r⟩;
    //a = NF_⪯(T_1, [P̃, T_2, ..., T_r]), and b is the first cofactor.
    if a = 0 then
        return T_1 = bP̃ mod ⟨T_2, ..., T_r⟩;
    else
        u := Inversion(a, T);
        if we obtain a decomposition then
            return the decomposition;
        else
            return NF_⪯(−dbu, T);
```

Example 4.127. *We give here two simple examples of the execution of the Inversion algorithm 4.126, the first one succeeds and the second one fails and returns a decomposition of the triangular set.*

- *Let T be $\{x^2 - 1, y^2 - 1\}$ and $P = xy$ in $\mathbb{K}[x, y]$ with $x \succ y$. The main variable of P is x and its leading coefficient is y. The inverse of y modulo T is y himself, so $d = y$. Then $\tilde{P} = x$, and $x^2 - 1 = -1 + x \times x$ so, $a = -1$ and $b = x$. Finally, $u = -1$ and we return $\mathsf{NF}_{\preceq}(-y \times x \times (-1), T) = xy$. Indeed, $\mathsf{NF}_{\preceq}(x^2 y^2, T) = 1 \times 1 = 1$.*
- *Let T be $\{x^2 - 1, y^2 - 1\}$ and $P = xy - 1$. P cannot be inversible modulo T because they share the same root $(1, 1)$. If we run the algorithm, $d = y$ and $\tilde{P} = x - y$. Then $x^2 - 1 = 0 + (x+y)\tilde{P} \mod \langle y^2 - 1 \rangle$, so we return the decomposition $x^2 - 1 = (x-y)(x+y) \mod y^2 - 1$.*

Theorem 4.128. *Algorithm 4.126 terminates and outputs the inverse of P or a factorization of an element of T.*

Proof. We prove correctness by induction on the number of variables r and on the degree of the polynomial P as a monic polynomial in its main variable y_1. If $r = 0$ then P is a scalar and the algorithm returns $1/P$. If $r = 1$, then T consists in a single polynomial T_1 and both P and T_1 are univariate in y_1, with $\mathsf{deg}(P) < \mathsf{deg}(T_1)$. Since P is assumed to be non zero, its leading coefficient is a scalar c and its inverse is $d = 1/c$, thus $\tilde{P} = P/c$ is monic. The writing $T_1 = a + b\tilde{P}$ is exactly the Euclidian division of T_1 by $\tilde{P}$. If $a = 0$ then the algorithm returns a decomposition of T_1 into two non trivial factors. Else a is a polynomial of degree less than P, so Inversion(a, T) outputs a correct decomposition of T or the inverse of a modulo T. In the second case, the algorithm outputs $\mathsf{NF}_{\preceq}(-dbu, T)$, but the following equalities hold:

$$-dbu = -b\tilde{P}u \mod T = -u(T_1 - a) \mod T = ua \mod T = 1 \mod T$$

If $r \geq 2$, the proof is the same as in the case $r = 1$, with moduli with respect to $T_2, \ldots, T_r$. Termination is assured by the decrease in the number of variables or the degree in the main variable between the recursive calls. □

With this Inversion algorithm, we are able to give a solution to the problem of computing a triangular decomposition of $T \cup E$ in $\mathbb{K}[y_1, \ldots, y_r]$: we just have to add to T elements of E one by one, using the following Insertion algorithm 4.129. This algorithm is also recursive, this time we do not assume that P and T_1 have same leading variable but when we apply the inversion algorithm, we suppose again that instead of T, we keep only the polynomials with smaller (or equal) leading variable than the polynomial we want to insert. The idea is to try to obtain the inverse of the leading coefficient of P. If we succeed, we can apply the insertion algorithm with a triangular set with one polynomial having smaller degree, and if we fail we obtain a decomposition of a polynomial T_k in T into two factors, which leads to a decomposition of T into two triangular sets T^1 and T^2 such that $\mathbb{V}(T) = \mathbb{V}(T^1) \cup \mathbb{V}(T^2)$. In this case, we apply again the Insertion algorithm twice.

Algorithm 4.129: Insertion Algorithm

Input : $P \in \mathbb{K}[y_1, \ldots, y_r]$ and $T = \{T_1 \succ \cdots \succ T_r\}$ such that $P = \mathsf{NF}_{\preceq}(P, T)$.
Output: A triangular decomposition of the ideal $\langle T \cup \{P\} \rangle$.

```
if P = 0 then
    return T
else
    y_k := LV(P);
    c := LC_{y_k}(P); // c is a polynomial in the variables smaller than y_k.
    d := Inversion(c, T);
    if this inversion fails then
        We obtain a decomposition V(T) = V(T^1) ∪ V(T^2);
        return Insertion(NF_≼(P, T^1), T^1) ∪ Insertion(NF_≼(P, T^2), T^2);
    else
        P̃ := NF_≼(d × P, T); // P̃ is monic in y_k.
        T̃ := T ∪ P̃\{T_k}; // where T_k is the polynomial in T with main variable
        y_k.
        return Insertion(NF_≼(T_k, T̃), T̃);
```

Example 4.130. *This example follows example 4.127. Let T be $\{x^2 - 1, y^2 - 1\}$ and $P = xy - x - y + 1 \in \mathbb{K}[x, y]$. We want to compute a triangular decomposition of the ideal*

$T \cup \{P\}$. The main variable of P is x and $c = y - 1$. Since c is not invertible modulo $y^2 - 1$, we obtain the decomposition $\mathbb{V}(T) = \mathbb{V}(T^1) \cup \mathbb{V}(T^2)$ with $T^1 = \{x^2 - 1, y - 1\}$ and $T^2 = \{x^2 - 1, y + 1\}$. Because $\mathsf{NF}_{\preceq}(P, T^1) = 0$, the result of Insertion($\mathsf{NF}_{\preceq}(P, T^1), T^1$) is T^1 himself. On the other side, $\mathsf{NF}_{\preceq}(P, T^2) = -2x + 2$. Trying to insert this polynomial into T^2 leads to Insertion($\mathsf{NF}_{\preceq}(x^2 - 1, \tilde{T})), \tilde{T}$) with $\tilde{T} = \{x - 1, y + 1\}$, and the result is $\tilde{T}$. Finally, the algorithm returns $\{\{x^2 - 1, y - 1\}, \{x - 1, y + 1\}\}$.

Example 4.131. *Now, we give a complete resolution of the Cyclic-5 problem, on the finite field $\mathbb{K} = \mathbb{F}_{65521}$. The ideal is generated by the polynomials of E :*

$$E = \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 \\ x_1x_2 + x_1x_5 + x_2x_3 + x_3x_4 + x_4x_5 \\ x_1x_2x_3 + x_1x_2x_5 + x_1x_4x_5 + x_2x_3x_4 + x_3x_4x_5 \\ x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5 \\ x_1x_2x_3x_4x_5 - 1 \end{cases}$$

which leads to the following Gröbner basis in $\mathbb{K}[\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5]$:

$$\mathcal{G} = [\sigma_1, \sigma_2 + 3145\sigma_4, \sigma_3^6 + 3125\sigma_3, \sigma_4, \sigma_5 - 1]$$

The degree of all these polynomials is one, except for $\sigma_3^6 + 3125\sigma_3$. So, we work in $\mathbb{K}[x_1, x_2, x_3, x_4, x_5, \sigma_3]$. The triangular set given by the divided differences and the invariant Gröbner Basis is :

$$T = \begin{cases} f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 \\ f_2 &= x_2^2 + x_2x_3 + x_2x_4 + x_2x_5 + x_3^2 + x_3x_4 + x_3x_5 + x_4^2 + x_4x_5 + x_5^2 + 3145\sigma_3^4 \\ f_3 &= x_3^3 + x_3^2x_4 + x_3^2x_5 + x_3x_4^2 + x_3x_4x_5 + x_3x_5^2 + 3145x_3\sigma_3^4 + x_4^3 + x_4^2x_5 + x_4x_5^2 \\ &\quad +3145x_4\sigma_3^4 + x_5^3 + 3145x_5\sigma_3^4 - \sigma_3 \\ f_4 &= x_4^4 + x_4^3x_5 + x_4^2x_5^2 + 3145x_4^2\sigma_3^4 + x_4x_5^3 + 3145x_4x_5\sigma_3^4 - x_4\sigma_3 + x_5^4 \\ &\quad +3145x_5^2\sigma_3^4 - x_5\sigma_3 \\ f_5 &= x_5^5 + 3145x_5^3\sigma_3^4 - x_5^2\sigma_3 - 1 \\ f_6 &= \sigma_3^6 + 3125\sigma_3 \end{cases}$$

We apply the previous algorithm to E and T, and we obtain

$$\begin{cases} x_1 + x_2 + 18346\sigma_3^2 \\ x_2^2 + 18346x_2\sigma_3^2 - 629\sigma_3^4 \\ x_3 + 15725\sigma_3^2 \\ x_4 + 15725\sigma_3^2 \\ x_5 + 15725\sigma_3^2 \\ \sigma_3^5 + 3125 \end{cases} \quad \begin{cases} x_1 + 15725\sigma_3^2 \\ x_2 + 15725\sigma_3^2 \\ x_3 + x_4 + 18346\sigma_3^2 \\ x_4^2 + 18346x_4\sigma_3^2 - 629\sigma_3^4 \\ x_5 + 15725\sigma_3^2 \\ \sigma_3^5 + 3125 \end{cases} \quad \begin{cases} x_1 + 15725\sigma_3^2 \\ x_2 + x_3 + 18346\sigma_3^2 \\ x_3^2 + 18346x_3\sigma_3^2 - 629\sigma_3^4 \\ x_4 + 15725\sigma_3^2 \\ x_5 + 15725\sigma_3^2 \\ \sigma_3^5 + 3125 \end{cases}$$

$$\begin{cases} x_1 + 15725\sigma_3^2 \\ x_2 + 15725\sigma_3^2 \\ x_3 + 15725\sigma_3^2 \\ x_4 + x_5 + 18346\sigma_3^2 \\ x_5^2 + 18346x_5\sigma_3^2 - 629\sigma_3^4 \\ \sigma_3^5 + 3125 \end{cases} \quad \begin{cases} x_1 + x_4^3x_5^3 + x_4^2x_5^4 + x_4 + x_5 \\ x_2 - x_4^3x_5^3 \\ x_3 - x_4^2x_5^4 \\ x_4^4 + x_4^3x_5 + x_4^2x_5^2 + x_4x_5^3 + x_5^4 \\ x_5^5 - 1 \\ \sigma_3 \end{cases} \quad \begin{cases} x_1 + x_5 + 18346\sigma_3^2 \\ x_2 + 15725\sigma_3^2 \\ x_3 + 15725\sigma_3^2 \\ x_4 + 15725\sigma_3^2 \\ x_5^2 + 18346x_5\sigma_3^2 - 629\sigma_3^4 \\ \sigma_3^5 + 3125 \end{cases}$$

This triangular decomposition encodes all of the 70 solutions of the Cyclic-5 problem.

Example 4.132. *We now come back to the example 4.108, invariant under the subgroup* $\mathbf{G} = (\mathbb{Z}/2\mathbb{Z})^4 \rtimes D_5$ *of the Coxeter group* $\mathbf{H} = (\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathfrak{S}_5$*. We wanted to solve the system*

$$\begin{cases} f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - 1 = 5\Re(x_1^2) - \Re(1) = 0 \\ f_2 = x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 - 1 = 5\Re(x_1^4) - \Re(1) = 0 \\ f_3 = x_1^2x_2^2 + x_1^2x_5^2 + x_2^2x_3^2 + x_3^2x_4^2 + x_4^2x_5^2 - 1 = 5\Re(x_1^2x_2^2) - \Re(1) = 0 \\ f_4 = x_1x_2x_3x_4x_5 - 1 = \Re(x_1x_2x_3x_4x_5) - \Re(1) = 0 \\ f_5 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 - 1 = 5\Re(x_1^6) - \Re(1) = 0 \end{cases}$$

and we found with the general algorithm 4.105 the following $\mathbf{H}$*-invariant Gröbner basis:*

$$\mathcal{G} = [H_1 - 1, H_2, H_3, H_4^6 - 10488H_4^5 + 5251H_4^4 - 10492H_4^3 - 5271H_4^2 + 28927H_4 + 18242, H_5 - 1]$$

The set G_H *obtained in this case consist in ten polynomials whose leading monomials are*

$$x_1^2, x_1x_2x_3x_4x_5, x_1x_3^5x_4x_5, x_1x_4^7x_5, x_1x_5^9, x_1H_5, x_2^4, x_3^6, x_4^8, x_5^{10}$$

Then we run the inversion-algorithm twice with the set E *equal to* $\{f_1, \ldots, f_m\}$ *together with the polynomials starting by* $x_1x_2x_3x_4x_5, x_1x_3^5x_4x_5, x_1x_4^7x_5, x_1x_5^9, x_1H_5$ *and the set* T *equal to the other polynomials in* G_H *together with one of the polynomials starting by* H_4^3*. In each case, we obtain a triangular ideal whose associated variety has size 480, so we recover the 960 solutions. Since* $H_5 = 1$ *in this example, the polynomial with leading monomial equal to* x_1H_5 *is already portable into the triangular set, but we don't need to do it before running the algorithm.*

Remark 4.133. *Let* G *be a Gröbner Basis for lexicographical ordering of a zero-dimensional ideal in* $\mathbb{K}[y_1, \ldots, y_r]$*. If we run insertion algorithm with* $T = \{T_1 \succ \cdots \succ T_r\}$ *the elements of* G *having their leading monomial which is a power of* y_i *and* $E = G \backslash T$*, we recover the Lazard Lex-Triangular algorithm [73].*

4.3.3.3 A univariate approach

In this subsubsection, we give another approach to remove spurious solutions. We use the same notations as in the previous subsubsection, that is $T = \{T_1 \succ \cdots \succ T_r\}$ for a triangular set in $\mathbb{K}[Y] = \mathbb{K}[y_1, \ldots, y_r]$ and E another set of polynomials in $\mathbb{K}[Y]$. The idea here is to compute a Gröbner basis for lexicographical ordering of $\langle T \cup E \rangle$. The strategy involves a univariate representation of the algebra $\mathbb{K}[Y]/\langle T \rangle$ and a variant of the FGLM algorithm.

Definition 4.134. *Let $\mathcal{I}$ be a zero-dimensional ideal in $\mathbb{K}[Y]$. a univariate representation of the quotient ring $\mathbb{K}[Y]/\mathcal{I}$ is an isomorphism*

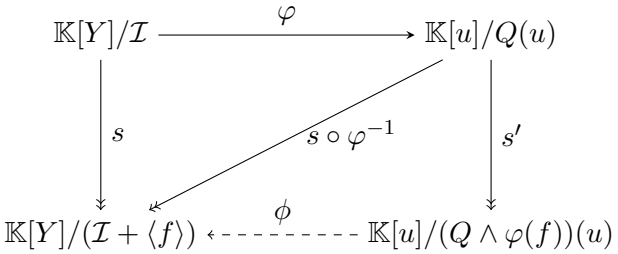
$$\begin{array}{rccc} \varphi: & \mathbb{K}[Y]/\mathcal{I} & \to & \mathbb{K}[u]/Q(u) \\ & y_1,\ldots,y_r & \mapsto & S_1(u),\ldots,S_r(u) \\ & \Lambda & \mapsto & u \end{array}$$

where Λ is a linear form in $y_1,\ldots,y_r$, such that $\mathbb{K}[Y]/\mathcal{I} = \mathbb{K}[\Lambda]$ (Λ is called primitive*), and Q is the characteristic polynomial of the endomorphism of multiplication by Λ in $\mathbb{K}[Y]/\mathcal{I}$.*

In the previous definition, the fact that Λ is primitive is a Zariski open condition on its coefficients, if the field $\mathbb{K}$ is big enough we can choose the coefficients of Λ randomly and we get a primitive linear form with high probability, see [87] for details. The univariate approach to remove spurious solutions follows from the following proposition.

Proposition 4.135. *Let $\mathcal{I}$ be a zero-dimensional ideal in $\mathbb{K}[Y]$ and consider a univariate representation of $\mathbb{K}[Y]/\mathcal{I}$ as in definition 4.134. Let f be in $\mathbb{K}[Y]$. Then an univaraiate representation of $\mathbb{K}[Y]/(\mathcal{I}+\langle f\rangle)$ is given by the univariate quotient $\mathbb{K}[u]/(Q\wedge\varphi(f))(u)$, where $Q\wedge\varphi(f)$ is the greatest common divisor of Q and $\varphi(f)$. The variables y_i are mapped on the images of the S_i in this univariate ring. The image of Λ remains primitive.*

Proof. Consider the following diagram. We need to prove that the kernel of $s\circ\varphi^{-1}$ is $\langle Q\wedge\varphi(f)\rangle$ to prove the existence of the isomorphism ϕ.



By Bezout's relation, $Q\wedge\varphi(f)$ can be written $aQ+b\varphi(f)$, so $\varphi^{-1}(Q\wedge\varphi(f)) = \phi^{-1}(b)f$ and $Q\wedge\varphi(f)$ lies in the kernel of $s\circ\varphi^{-1}$. Reciprocally, let P be in $\mathrm{Ker}(s\circ\varphi^{-1})$. Since φ is an isomorphism, $\varphi^{-1}(P)\in\langle f\rangle$, so P can be written $aQ+b\varphi(f)$ and is a multiple of $Q\wedge\varphi(f)$. □

Now let T be a triangular set in $\mathbb{K}[Y]$ and Q a univariate polynomial associated to a univariate representation of $\mathbb{K}[Y]/\langle T\rangle$, with same notations as in definition 4.134. Then by applying previous proposition $|E|$ times, a univariate representation of $\langle T\cup E\rangle$ is given by:

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{K}[Y]/\langle T\cup E\rangle & \to & \mathbb{K}[u]/\tilde{Q}(u) \\ & y_1,\ldots,y_r & \mapsto & \tilde{S}_1(u),\ldots,\tilde{S}_r(u) \\ & \tilde{\Lambda} & \mapsto & u \end{array}$$

where $\tilde{Q}$ is the greatest common divisor between Q and $\{\varphi(P)\mid P\in E\}$, $\tilde{\Lambda}$ is the image of Λ in $\mathbb{K}[Y]/\langle T\cup E\rangle$ and $\tilde{S}_1,\ldots,\tilde{S}_r$ are the images of the previous $S_1,\ldots,S_r$, which are well defined since $\tilde{Q}$ divides Q. To obtain a lexicographical Gröbner basis of the ideal $\langle T\cup E\rangle$, we just apply the following algorithm 4.136, which is a variant of the FGLM algorithm 1.52.

Algorithm 4.136: Filtering solutions with univariate representation

Input : The polynomial $\tilde{Q}$, the polynomials $\tilde{S}_1, \ldots, \tilde{S}_n$, the morphism $\tilde{\varphi}$.
Output: A lexicographical Gröbner basis of the ideal $\langle T \cup E \rangle$.

$L := [1]$; `//list of monomials in` $\mathbb{K}[Y]$ `sorted by the lexicographic ordering` $\preceq$
$S := [\,]$; `//staircase for` $\preceq$
$V := [\,]$; `//` $V = \tilde{\varphi}(S)$
$G := [\,]$;
while $L \neq [\,]$ **do**
  $m := L[1]$; and remove m from L;
  $v := \tilde{\varphi}(m)$;
  $s := \#S$;
  if $v \in \mathsf{Span}_{\mathbb{K}}(V)$ **then**
    we can find $(\lambda_i) \in \mathbb{K}^s$ such that $v = \sum_{i=1}^{s} \lambda_i \cdot V_i$;
    $G := G \cup \left[m - \sum_{i=1}^{s} \lambda_i \cdot S_i \right]$;
  else
    $S := S \cup [m]$; $\quad V := V \cup [v]$;
    $L := \mathrm{Sort}(L \cup [y_i\, m \mid i = 1, \ldots, r], \preceq)$;
  Remove from L duplicates elements or multiples of $\mathsf{LM}_{\preceq}(G)$;
return G

Termination is assured by the fact that $T_1, \ldots, T_r$ are in the kernel of $\tilde{\varphi}$ so we would find a linear combination between some power $y_i^{\alpha_i}$ and the monomials examined when they are affected to m. Correctness is obvious since the kernel of $\tilde{\varphi}$ is exactly $\langle E \cup T \rangle$.

Example 4.137. *We propose here a different approach of example 4.122. Remember that we wanted to solve* $f_1 = f_2 = f_3 = 0$ *with*

$$f_1 = x_1 + x_2 + x_3 \qquad f_2 = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \qquad f_3 = x_1 x_2 x_3 - 1$$

Since the $\mathfrak{S}_3$*-invariant Gröbner basis of the system is given by* $[\sigma_1, \sigma_2^3 + 9, \sigma_3 - 1]$*, we set* $\mathbb{K} = \mathbb{Q}[\omega]$ *with* ω *a root of the irreducible polynomial* $x^3 + 9$*, and assume that* $\sigma_2 = \omega$*. The divided differences computed in example 4.121 form a triangular set given on* $\mathbb{K}$ *after reductions by*

$$T = \{x_1 + x_2 + x_3, x_2^2 + x_2 x_3 + x_3^2 + \omega, x_3^3 + \omega x_3 - 1\}$$

The linear form $\Lambda = 3x_1 + 2x_2 + x_3$ *is primitive in* $\mathbb{K}[x_1, x_2, x_3]/\langle T \rangle$*, and the characteristic polynomial of multiplication by* Λ *in* $\mathbb{K}[x_1, x_2, x_3]/\langle T \rangle$ *is given by* $Q(u) = u^6 + 6\omega u^4 + 9\omega^2 u^2 - 9$*, which gives the following univariate representation:*

$$\begin{array}{rccl}
\varphi : & \mathbb{K}[Y]/\mathcal{I} = \mathbb{K}[x_1, x_2, x_3]/\langle T \rangle & \to & \mathbb{K}[u]/Q(u) \\
& \Lambda & \mapsto & u \\
& x_1 & \mapsto & S_1(u) = \frac{1}{18}(-u^4 - 5\omega u^2 + 9u - 4\omega^2) \\
& x_2 & \mapsto & S_2(u) = \frac{1}{9}(u^4 + 5\omega u^2 + 4\omega^2) \\
& x_3 & \mapsto & S_3(u) = -\frac{1}{18}(u^4 + 5\omega u^2 + 9u + 4\omega^2)
\end{array}$$

The images of polynomials in $E = \{f_1, f_2, f_3\}$ *by* φ *are all zero but the image of* f_2*, which is given by* $\varphi(f_2)(u) = \frac{1}{2}(u^3 + 3\omega u - 3)$*. Since* $Q(u) = (u^3 + 3\omega u - 3)(u^3 + 3\omega u + 3)$*, the GCD between* Q *and* $\varphi(f_2)$ *is exactly* $\tilde{Q}(u) = 2\varphi(f_2)(u) = u^3 + 3\omega u - 3$*, so the map* $\tilde{\varphi}$ *is given by:*

$$\begin{array}{rccl} \tilde{\varphi}: & \mathbb{K}[\tilde{Y}]/\mathcal{I} = \mathbb{K}[x_1, x_2, x_3]/\langle T \cup E\rangle & \to & \mathbb{K}[u]/\tilde{Q}(u) \\ & \tilde{\Lambda} & \mapsto & u \\ & x_1 & \mapsto & \tilde{S}_1(u) = -\frac{1}{9}(\omega u^2 - 3u + 2\omega^2) \\ & x_2 & \mapsto & \tilde{S}_2(u) = \frac{1}{9}(2\omega u^2 + 3u + 4\omega^2) \\ & x_3 & \mapsto & \tilde{S}_3(u) = -\frac{1}{9}(\omega u^2 + 6u + 2\omega^2) \end{array}$$

We can now apply the previous algorithm. The three first loops add the monomials $1, x_3, x_3^2$ *in the staircase, because their images by* $\tilde{\varphi}$ *are linearly independent:* $\tilde{\varphi}(1) = 1$*,* $9\tilde{\varphi}(x_3) = -\omega u^2 - 6u - 2\omega^2$ *and* $9\tilde{\varphi}(x_3^2) = 3u^2 - \omega^2 u$*. Actually, these elements form a basis of* $\mathbb{K}[u]/\tilde{Q}(u)$*, so any new examined monomial will give an element of the Gröbner basis. The next monomial in* L *is* x_3^3*, which gives* $g_3 = x_3^3 + \omega x_3 - 1$*. Then,* x_2 *gives* $3g_2 = 3x_2 - 3\omega x_3^2 - 3x_3 - 2\omega^2$*. Since we remove from* L *all multiples of* x_3^3 *and* x_2*, the next one is* x_1 *which gives* $3g_1 = 3x_1 + 3\omega x_3^2 + 6x_3 + 2\omega^2$*, and the algorithm stops. The lexicographical reduced Gröbner basis of* $\langle T \cup E\rangle$ *is given by* $\{g_1, g_2, g_3\}$*.*

Remark 4.138. *We could have taken a univariate representation of* $\mathbb{K}[x_1, x_2, x_3, \omega]/T$ *with* T *the triangular set given by divided differences together with* $w^3 + 9$ *as in example 4.124, and we would have found the same result. However, from a complexity point of view, it is easier to compute univariate representations of divided differences only, see the following complexity subsubsection.*

4.3.3.4 Complexity of the approaches

We now briefly examine and compare the complexity of the first and the third approaches. The second one is very general but its complexity is hard to derive. We have mentionned that from the **H**-invariant Gröbner basis, we take a primary decomposition. Since in practice, those bases are very small, we can suppose that the cost of computing such a decomposition is negligible. The first approach has the best complexity, but the two others contain ideas that could give rise to a best approach since we are working only in the field $\mathbb{K}$, and there are exact methods.

Exhaustive search. In algorithm 4.114, the computation of the variety $\mathbb{V}(J_H)$ and the successive **b**, **c** and **a** can be understood in two ways: first, we can perform numerical approximations if we are looking for solutions over $\mathbb{R}$ or $\mathbb{C}$. Otherwise, we can compute in field extensions if we are looking for exact solutions. In both case the complexity is simply $O(m\frac{|\mathbf{H}|}{|\mathbf{G}|}\sum_{\mathbf{b}\in\mathbb{V}(J_H)} C_{\mathbf{b}})$, where $C_{\mathbf{b}}$ is the complexity of computing an approximation of **b** and a corresponding **a**, or an expression of such n-tuples in a suitable extension of $\mathbb{K}$.

Univariate approach. We use notations of the dedicated subsubsection. Once the computation of the univariate representation is done, the computations of GCD are very easy, since they can be done in quasi-polynomial time with respect to the degree of the polynomial Q in the univariate representation. The FGLM-like algorithm to recover a Gröbner basis for lexicographical ordering has complexity $O(r(\mathsf{deg}\tilde{Q}^3))$. Now let discuss about the complexity of computing a univariate representation of a triangular ideal generated by $T = \{T_1 \succ \cdots \succ T_r\}$

in $\mathbb{K}[y_1, \ldots, y_r]$. We denote again by $D(T)$ the product $\prod_{i=1}^{r} \deg_{y_i} T_i$. From [87], it is known that a univariate representation can be computed in $O(D(T)^2)$ operations in $\mathbb{K}$. However, in several particular case, a univariate representation can be computed faster, even in quasi-optimal time in the case of divided differences, see [74].

4.3.4 Implementation and Benchmarks

Comparaison between $\mathbb{K}[X]$ and $\mathbb{K}[X]^{\mathbf{G}}$. We analyse here at a fixed degree the assumption $\dim(\mathbb{K}[X]_d^{\mathbf{G}}) \simeq \dim(\mathbb{K}[X]_d)$ made to analyse the complexity of SAGBI-F_5 algorithm based on asymptotic results. Since $\dim(\mathbb{K}[X]_d) \underset{d\to+\infty}{\longrightarrow} +\infty$, we present here the relative deviation

$$\sigma_d = \frac{\dim(\mathbb{K}[X]_d^{\mathbf{G}}) - \dim(\mathbb{K}[X]_d)/|\mathbf{G}|}{\dim(\mathbb{K}[X]_d)/|\mathbf{G}|} = \frac{|\mathbf{G}|\dim(\mathbb{K}[X]_d^{\mathbf{G}})}{\dim(\mathbb{K}[X]_d)} - 1 \underset{d\to+\infty}{\longrightarrow} 0$$

for several groups. We have already seen the same kind of analysis in section 4.2, for abelian groups. We denote by C_n the cyclic group of order n generated by the matrix M_σ (already seen in example 4.49), and by D_n the dihedral group of order $2n$ generated by M_σ and M_τ, where τ is the permutation $(1\ n)(2\ n-1)\ldots$, which is a product of transpositions. More precisely:

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix} \quad \text{and} \quad M_\tau = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}$$

Table 4.139 presents relative deviations for the Cyclic and Dihedral groups: the convergence of σ_d to 0 is fast.

We are now interested in an analysis of the family $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes D_n$ of subgroups of the Coxeter group (seen in example 4.108, in the case $n = 5$). For a given n, this subgroup is generated by the matrices M_σ, M_τ, and the diagonal matrices with diagonal coefficients beeing 1 or -1, with an even number of -1. This group has size $2^n n$. If n is even, the group contains the scaling $-I_n$, therefore the convergence of the relative standard deviation toward 0 does not hold. Therefore, we only present cases where n is odd. Since the convergence of the relative deviation towards 1 is slower than for the cyclic or dihedral groups, we present in table 4.140 the ratio $|\mathbf{G}|\dim(\mathbb{K}[X]_d^{\mathbf{G}})/\dim(\mathbb{K}[X]_d) \underset{d\to+\infty}{\longrightarrow} 1$. Even if the convergence is slow, we see that the approximation $\dim(\mathbb{K}[X]_d^{\mathbf{G}})/\dim(\mathbb{K}[X]_d) \simeq 1/|\mathbf{G}|$ remains very acceptable in most of the case, since $|\mathbf{G}| = 2^n n$.

Comaparaison between Gröbner bases and Invariant Gröbner bases. We compare here some sizes of Gröbner bases and Invariant Gröbner bases, together with the number of solutions of the corresponding ideals.

Example 4.141. *We deal here with the Cyclic-n problem, for various n. We present the number of polynomials, the maximal number of monomials and the variety size of the lexicographical Gröbner basis and $\mathfrak{S}_n$-invariant Gröbner basis obtained with the Cyclic-n problem, given by the following ideal in the invariant ring $\mathbb{K}[x_1, \ldots, x_n]^{D_n}$:*

$$\mathcal{I}^{D_n} = \langle \Re(x_1), \Re(x_1x_2), \ldots, \Re(x_1x_2\cdots x_n) - 1 \rangle$$

Group \ d	2	3	4	5	10	15
C_4	0.20	0.00	0.14	0.00	0.021	0.00
C_5	0.00	0.00	0.00	0.032	4.0×10^{-3}	1.0×10^{-3}
C_6	0.14	0.071	0.048	0.00	7.0×10^{-3}	0.0007.7
C_7	0.00	0.00	0.00	0.00	0.00	0.00
C_{10}	0.091	0.00	0.021	4.0×10^{-3}	1.5×10^{-3}	1.2×10^{-5}
C_{15}	0.00	0.015	0.00	1.0×10^{-3}	1.2×10^{-5}	3.9×10^{-6}
D_4	1.4	0.60	0.83	0.43	0.32	0.18
D_5	1.0	0.43	0.43	0.27	0.11	0.047
D_6	1.3	0.50	0.52	0.24	0.12	0.047
D_7	1.0	0.33	0.33	0.15	0.049	0.016
D_{10}	1.2	0.27	0.32	0.11	0.029	6.0×10^{-3}
D_{15}	1.0	0.19	0.18	0.047	6.0×10^{-3}	6.7×10^{-4}

Table 4.139 – The relative deviation between $\dim(\mathbb{K}[X]_d^{\mathbf{G}})$ and $\dim(\mathbb{K}[X]_d)/|\mathbf{G}|$ for the Cyclic and Dihedral groups.

$n\backslash d$	15	20	25	30	35	40	50	80	100
5	0.66	1.7	0.75	1.4	0.79	1.3	1.2	1.1	1.1
7	0.33	2.3	0.46	1.8	0.56	1.6	1.5	1.3	1.2
9	0.11	3.7	0.25	2.6	0.36	2.1	1.9	1.5	1.4
11	0.042	6.4	0.11	4.0	0.21	3.0	2.5	1.8	1.6
13	6.1×10^{-3}	12.	0.043	6.4	0.11	4.5	3.5	2.3	2.0
15	6.3×10^{-3}	23.	0.013	11.0	0.048	7.0	5.2	3.1	2.5

Table 4.140 – Ratio $|\mathbf{G}| \dim(\mathbb{K}[X]_d^{\mathbf{G}})/\dim(\mathbb{K}[X]_d)$ for the Coxeter subgroup $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes D_n$.

4.3.4.1 Cyclic group and FGb implementation

As a proof of concept of the efficiency of the method, a implementation of the algorithm 1.68 in the case of the invariant ring $\mathbb{K}[X]^{C_n}$ in C as a part of the FGb program [3] has been done. We have a dedicated implementation for rewriting products $b_i^d \times b_{i'}^{d'}$ as a linear combination of $b_j^{d+d'}$ where $(b_i^d)_{i\in\{1,\ldots,n_d\}}$ is the basis of $\mathbb{K}[X]^{C_n}$ given by $\Re(m)$, with m describing the set of initial monomials. We report in table 4.143, CPU timings for the Cyclic-n problem on $\mathbb{F}_{65521}$ (the computer is a laptop Dell E6500, 4Go RAM). For the tests we compute a SAGBI-basis up to degree D of the invariant ideal, and we choose D big enough so that we can apply the SAGBI-FGLM algorithm 4.101). The results are very promising since it takes 1m30s to compute a SAGBI basis for the Cyclic-9 problem. To give an order of magnitude with the classical approach with Gröbner bases, we have included the CPU time for computing a Gröbner basis using the F_4 algorithm [34], implemented in Magma 2.19, on a computer with an Intel/Xeon with 20 Go RAM).

3. `http://www-polsys.lip6.fr/~jcf/Software/index.html`

$\mathcal{G}$	$\lvert\mathcal{G}\rvert$	Max length of a polynomial in $\mathcal{G}$	$\mathbb{V}(\langle\mathcal{G}\rangle)$
Lex-Gb of $\mathcal{I}^{D_2}$	2	2	2
$\mathfrak{S}_2$-inv Lex-Gb of $\mathcal{I}^{D_2}$	2	2	1
Lex-Gb of $\mathcal{I}^{D_3}$	3	3	6
$\mathfrak{S}_3$-inv Lex-Gb of $\mathcal{I}^{D_3}$	3	2	1
Lex-Gb of $\mathcal{I}^{D_4}$	6	5	dim 1
$\mathfrak{S}_4$-inv Lex-Gb of $\mathcal{I}^{D_4}$	3	2	dim 1
Lex-Gb of $\mathcal{I}^{D_5}$	11	15	70
$\mathfrak{S}_5$-inv Lex-Gb of $\mathcal{I}^{D_5}$	5	2	6
Lex-Gb of $\mathcal{I}^{D_6}$	17	27	156
$\mathfrak{S}_6$-inv Lex-Gb of $\mathcal{I}^{D_6}$	7	4	13
Lex-Gb of $\mathcal{I}^{D_7}$	35	132	924
$\mathfrak{S}_7$-inv Lex-Gb of $\mathcal{I}^{D_7}$	7	9	57
Lex-Gb of $\mathcal{I}^{D_8}$	57	2545	dim 1
$\mathfrak{S}_8$-inv Lex-Gb of $\mathcal{I}^{D_8}$	15	548	dim 1

Table 4.142 – Sizes of the invariant Gröbner bases and the Gröbner bases

Problem	D	D truncated with SAGBI-F_5	Gröbner Basis with F_4 on Magma
Cyclic-7	12	0.06s	0.2s
Cyclic-8	13	0.5s	3.9s
Cyclic-9	15	92.2s	417.1s
Cyclic-10	16	4788s	24h13m

Table 4.143 – Benchmarks with FGb: SAGBI-F_5 for the Cyclic-n problem in $\mathbb{F}_{65521}$

Further work. A Magma implementation of the algorithms has been done, and will be available soon. Notice that the timings in the FGb implementation seem to be bad, compared to the timings with the Abelian F_4 algorithm, presented in table 4.89, but the timings here (in the FGb implementation) date back to 2009. Even if the strategy of applying Abelian F_4 can be better for systems of equations individually invariant under the action of an abelian group (like the Cyclic-n problem), the approach with SAGBI bases can be applied in some cases, where Abelian F_4 cannot. Then, other benchmarks have to be performed, in both C and Magma.

Chapter 5

Gröbner Bases in Monomial Algebras

5.1 Introduction

This work is a common work with Jean-Charles Faugère and Pierre-Jean Spaenlehauer which has been accepted for presentation at the ISSAC' 14 conference.

Context and problem statement. Many polynomial systems or systems of Laurent polynomials arising in applications do not have a dense monomial structure (for instance multi-homogeneous systems, fewnomials, systems invariant under the action of a diagonal matrix group,...). The development of toric geometry during the 70s/80s has led to toric (or sparse) elimination theory [101], a framework designed to study and exploit algorithmically these monomial structures.

Central objects in toric geometry are *semigroup algebras* (also called toric rings), already defined in section 3.2.Semigroup algebras are isomorphic to subalgebras of $\mathbb{K}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ generated by a finite subset of monomials.

Our motivation is to propose fast algorithms to solve symbolically systems whose support lie in one of the following classes of semigroups: semigroups constructed from the points with integer coordinates in a normal lattice polytope $\mathscr{P} \subset \mathbb{R}^n$ (in that case, the algorithms we propose are well-suited for *unmixed* systems: the Newton polytopes of the input polynomials are all equal to $\mathscr{P}$) or semigroups generated by a scattered set of monomials (fewnomial systems).

Main results. Given a 0-dim. system of Laurent polynomials $f_1 = \cdots = f_s = 0$ and a finite subset $M \subset \mathbb{Z}^n$ such that each polynomial belongs to the subalgebra generated by $\{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid \alpha \in M\}$, we associate to M two affine semigroups: $S_M \subset \mathbb{Z}^n$ generated by M and $S_M^{(h)} \subset \mathbb{Z}^{n+1}$ generated by $\{(\alpha, 1) \in \mathbb{Z}^{n+1} \mid \alpha \in M\}$. Under the assumption that S_M contains zero but no nonzero pairs $(\mathbf{s}_1, \mathbf{s}_2) \in S_M^2$ such that $\mathbf{s}_1 + \mathbf{s}_2 = \mathbf{0}$, our solving strategy proceeds by combining the SAGBI-F_5 algorithm 1.68 (called Sparse-F_5 in this context) in the algebra $\mathbb{K}[S_M^{(h)}]$ and a sparse variant in $\mathbb{K}[S_M]$ of the FGLM algorithm 1.52. We define a notion of *sparse Gröbner basis* (definition 5.2) that is computed by the sparse-MatrixF5 algorithm if we know a bound on its maximal degree (this maximal degree is called the *witness degree* of the system). An important feature of sparse GBs is that their definition depends only on the ambient semigroup algebra and not on an embedding in a polynomial algebra. In this sense, they differ conceptually from SAGBI bases, even though Sparse-F_5 is no more than SAGBI-F_5 in this context and Sparse-FGLM has similarities with the SAGBI-FGLM

algorithm proposed in section 4.3 (algorithm 4.101). In the special case $S_M = \mathbb{N}^n$, then sparse Gröbner bases in $\mathbb{K}[S_M]$ are classical Gröbner bases, and sparse-FGLM is the usual FGLM.

At the end of the solving process, we obtain a rational parametrisation of the form

$$Q(T) = 0 \quad \text{and} \quad \forall \alpha \in M \setminus \{\mathbf{0}\}, \quad X_1^{\alpha_1} \cdots X_n^{\alpha_n} - Q_\alpha(T) = 0$$

where $Q \in \mathbb{K}[T]$ is a univariate polynomial, and for all $\alpha \in M$, $Q_\alpha \in \mathbb{K}(T)$ is a rational function. Consequently, the solutions of the input sparse system can be expressed in terms of the roots of the univariate polynomial Q by inverting a monomial map.

The next main result addresses the question of the complexity of this solving process when M is given as the set $\mathscr{P} \cap \mathbb{Z}^n$, where $\mathscr{P} \subset \mathbb{R}^n$ is a lattice polytope of dimension n. It turns out that the complexities of sparse-MatrixF5 and sparse-FGLM algorithms depend mainly on the combinatorial properties of $\mathscr{P}$:

— the normalized volume $\mathrm{vol}(\mathscr{P}) \in \mathbb{N}$;

— the Castelnuovo-Mumford regularity $\mathrm{reg}(\mathbb{K}[S^{(h)}_{\mathscr{P}\cap\mathbb{Z}^n}])$ (definition 3.109), equal to $n+1-\ell$ where ℓ is the smallest integer such that the intersection of $\mathbb{Z}^n$ with the interior of $\ell \cdot \mathscr{P}$ is nonempty;

— the Ehrhart polynomial $\mathsf{HP}_{\mathscr{P}}(\ell)$ which equals the cardinality of $(\ell \cdot \mathscr{P}) \cap \mathbb{Z}^n$ for $\ell \in \mathbb{N}$ (definition 3.101)

We use as indicator of the complexity the *witness degree* which bounds the maximal "sparse degree" (corresponding to an $\mathbb{N}$-grading on $\mathbb{K}[S^{(h)}_{\mathscr{P}\cap\mathbb{Z}^n}]$) in a reduced sparse Gröbner basis. More precisely, we obtain the following complexity estimates:

Theorem 5.1. *Let $\mathscr{P} \subset \mathbb{R}^n$ be a normal lattice polytope of dimension n with one vertex at $\mathbf{0} \in \mathbb{Z}^n$, $(d_1, \ldots, d_n)$ be a sequence of positive integers and $(f_1, \ldots, f_n)$ be a regular sequence of Laurent polynomials in $\mathbb{K}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]^n$, such that the support of f_i is included in $\{X_1^{s_1} \cdots X_n^{s_n} \mid \mathbf{s} \in (d_i \cdot \mathscr{P}) \cap \mathbb{Z}^n\}$. Then a sparse GB of the ideal $\langle f_1, \ldots, f_n \rangle \subset \mathbb{K}[S_{\mathscr{P}\cap\mathbb{Z}^n}]$ can be computed within*

$$O\left(n\, \mathsf{HP}_{\mathscr{P}}(\mathrm{d_{wit}})^\omega\right)$$

*arithmetic operations in $\mathbb{K}$, where $\omega < 2.373$ is a feasible exponent for the matrix multiplication and $\mathrm{d_{wit}} \leq \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^n (d_j - 1)$. Moreover, if $\mathbf{0}$ is a simple vertex of $\mathscr{P}$ (*i.e. *a vertex which is the intersection of n facets), then the sparse-FGLM algorithm executes at most*

$$O\left(\mathsf{HP}_{\mathscr{P}}(1)\left(\mathrm{vol}(\mathscr{P}) \prod_{j=1}^n d_j\right)^3\right)$$

arithmetic operations in $\mathbb{K}$.

Direct consequences of these formulas allow us to derive new complexity bounds for solving regular multi-homogeneous systems. We show that the witness degree of a regular system of n multi-homogeneous polynomials of multi-degree $(d_1, \ldots, d_p)$ with respect to blocks of variables of sizes $(n_1, \ldots, n_p)$ (with $\sum n_i = n$) is bounded by $n + 2 - \max_{i \in \{1,\ldots,p\}}(\lceil (n_i+1)/d_i \rceil)$ (which generalizes the bound $\min(n_1, n_2) + 1$ in the bilinear case [36]). We also propose a variant of Fröberg's conjecture (conjecture 2.43) for sparse systems and a notion of semi-regularity, which yield complexity estimates for solving sparse overdetermined systems.

We have implemented in C a prototype of the sparse-MatrixF5 algorithm, that runs several times faster than the original F_5 algorithm in the FGb software. For instance, we report speed-up ratios greater than 100 for instances of overdetermined bihomogeneous systems.

The implementation also works well for fewnomial systems (although this case is not covered by our complexity analysis).

Related works. Computational aspects of toric geometry and Gröbner bases are investigated in [102]. In particular, [102, Subroutine 11.18] gives an algorithm to compute syzygies of monomials in toric rings, which is an important routine for critical-pairs based algorithms.

Other approaches have been designed to take advantage of the sparse structure in Gröbner bases computations. For instance, the Slim Gröbner bases in [11] describes strategies to avoid increasing the number of monomials during computations. This approach improves practical computations, but does not lead to new asymptotic complexity bounds for classes of sparse systems.

The sparse structure and the connection with toric geometry have also been incorporated to the theory of resultants, and a vast literature has been written on this topic, see *e.g.* [33, 32, 21, 20]. One difficulty in the resultant framework is that it requires genericity assumptions on the input polynomials to ensure that the resultant is not zero. Sparse Gröbner bases are flexible: even if we do not know how to bound the witness degree (*i.e.* when the regularity assumptions of Theorem 5.1 do not hold), we can use ad-hoc techniques to ensure the termination of the sparse-MatrixF5 algorithm. Moreover, the algorithms extend without any modification to the overdetermined case. However, the computational tools that we propose do not exploit mixed monomials structures, which are well-understood in the context of resultants.

Perspectives. Our approach is for the moment limited to *unmixed systems*: all input polynomials have to lie in the same semigroup algebra. A possible extension of this work would be the generalization to mixed systems (where the algorithms would depend on the Newton polytope of each of the polynomials of the system). Some results seem to indicate that such a generalization may be possible: for instance, under genericity assumptions, mixed monomial bases of quotient algebras are explicitly described in [86].

Also, a bound on the witness degree and the complexity analysis is for the moment restricted to the polytopal case. Ensuring termination with a critical pairs approach (such as [102, algorithm 11.17]) could lead to a complete extension of the classical F_5 algorithm to the sparse case.

Finally, finding complexity bounds which explain the efficiency of the sparse Gröbner bases approach for fewnomial systems (see Table 5.35) remains an open problem, and is a work in progress.

Organisation of the chapter. The background material on semigroup algebras and convex geometry that will be used throughout this chapter have been recalled in section 3.2. Section 5.2 introduces sparse Gröbner bases and describes a general solving process for sparse systems. The main algorithms are described in Section 5.3 and their complexities are analyzed in Section 5.4. Finally, we describe in Section 5.5 some results that are direct consequences of this new framework and experimental results in Section 5.6.

5.2 Sparse Gröbner bases

One of the idea behind the sparse Gröbner bases framework is to replace the semigroup $\mathbb{N}^n$ (leading to the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$) by another affine semigroup S (see definition 3.85). First, we have to put an ordering on the monomials in $\mathbb{K}[S]$.

Definition 5.2. *Let S be an affine semigroup. A total ordering on the monomials of $\mathbb{K}[S]$ is called* admissible *if*

— *it is compatible with the internal law of* S*: for any* $\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3 \in S$, $X^{\mathbf{s}_1} \prec X^{\mathbf{s}_2} \Rightarrow X^{\mathbf{s}_1+\mathbf{s}_3} \prec X^{\mathbf{s}_2+\mathbf{s}_3}$*;*
— *for any* $\mathbf{s} \in S \setminus \{\mathbf{0}\}$, $X^{\mathbf{0}} \prec X^{\mathbf{s}}$.

Example 5.3. *In this section, we will take as a small example the affine semigroup generated in* $\mathbb{Z}^2$ *by the three integer points* $\{(1,1),(2,1),(1,2)\}$. *This semigroup leads to the algebra* $\mathbb{K}[S] = \mathbb{K}[xy, x^2y, xy^2]$. *Since* $\mathbb{K}[S] \subset \mathbb{K}[x,y]$, *a total ordering on* $\mathbb{K}[S]$ *is given by the restriction of a total ordering on* $\mathbb{K}[x,y]$ *to* $\mathbb{K}[S]$. *We choose the ordering given by the restriction of the DRL ordering. A picture of the semigroup* S *is presented in figure 5.4*

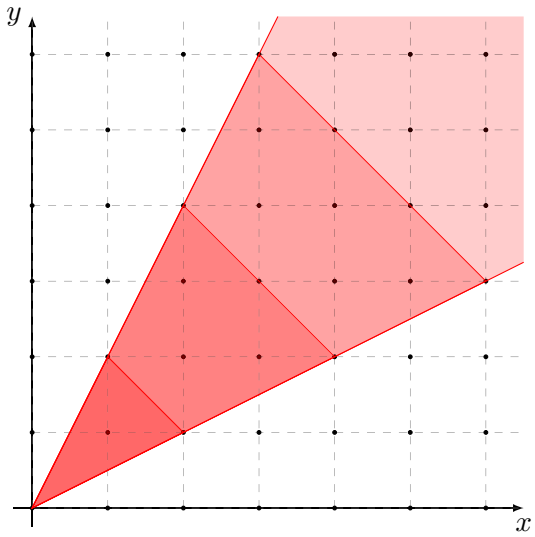


Figure 5.4 – The semigroup S

Notations 5.5. *For a fixed admissible ordering* $\preceq$ *and for any element* $f \in \mathbb{K}[S]$, *we let* $\mathsf{LM}_{\preceq}(f)$ *denote its leading monomial. Similarly, for any ideal* $\mathcal{I} \subset \mathbb{K}[S]$, $\mathsf{LM}_{\preceq}(\mathcal{I})$ *denotes the ideal generated by* $\{\mathsf{LM}_{\preceq}(f) \mid f \in \mathcal{I}\}$ *in* $\mathbb{K}[S]$. *A finite subset* $G \subset \mathcal{I}$ *is called a* sparse Gröbner basis *(abbreviated sGB) of* $\mathcal{I}$ *with respect to* $\preceq$ *if the set* $\{\mathsf{LM}_{\preceq}(g) \mid g \in G\}$ *generates* $\mathsf{LM}_{\preceq}(\mathcal{I})$ *in* $\mathbb{K}[S]$.

Remark 5.6. *With this definition, if* $S \subseteq \mathbb{N}^n$, *a sparse Gröbner basis of* $\mathcal{I} \subseteq \mathbb{K}[S]$ *is no more than a SAGBI Gröbner basis of* $\mathcal{I}$ *in* $\mathcal{A} = \mathbb{K}[S]$, *with definition 1.61. But contrary to SAGBI basis in the general case, in monomial algebras the implication* $f \in \mathcal{A} \implies \mathsf{LM}_{\preceq}(f) \in \mathcal{A}$ *holds, which is a great difference and has to be emphasized.*

Note that monomial orderings exist for any semigroup algebra: the convex hull of a semigroup $S \subset \mathbb{Z}^n$ is a PRPC $\mathscr{C} \subset \mathbb{R}^n$ (see definition 3.87): this is a consequence of the fact that there is no nonconstant invertible monomial in $\mathbb{K}[S]$. Now one can pick n independent linear forms $(\ell_1, \ldots, \ell_n)$ with integer coefficients in the dual cone

$$\mathscr{C}^* = \{\text{linear forms } \ell : \mathbb{R}^n \to \mathbb{R} \mid \forall \mathbf{x} \in \mathscr{C}, \ell(\mathbf{x}) \geq 0\}$$

and set $X^{\mathbf{s}_1} \prec X^{\mathbf{s}_2}$ if and only if the vector $(\ell_1(\mathbf{s}_1), \ldots, \ell_n(\mathbf{s}_1))$ is smaller than $(\ell_1(\mathbf{s}_2), \ldots, \ell_n(\mathbf{s}_2))$ for a classical admissible ordering on $\mathbb{N}^n$.

Note that the assumption that $\mathbb{K}[S]$ contains no nonconstant invertible monomial is a necessary and sufficient condition for the existence of a monomial ordering.

We describe now an algorithmic framework that we use to solve sparse systems of Laurent polynomials. Let $\mathcal{M} \subset \mathbb{Z}^n$ be a non-empty finit subset of $\mathbb{Z}^n$, containing no distinct elements $\mathbf{s}$ and $\mathbf{s}'$ such that $\mathbf{s} + \mathbf{s}' = \mathbf{0}$ (according to the assumptions of Definition 3.85). From now, we will identify a element of $\mathbb{Z}^n$ with the corresponding monomial in the ring of Laurent polynomial $\mathbb{K}[X^{\pm 1}] = \mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let $f_1, \ldots, f_s \in \mathbb{K}[X^{\pm 1}]$ be Laurent polynomials and $(d_1, \ldots, d_s)$ be positive integers such that the supports of each f_i is included in

$$\left\{ \prod_{j=1}^{d_i} m \mid m \in \mathcal{M} \right\}$$

Note that translating $\mathcal{M}$ amounts to multiplying the Laurent polynomials by Laurent monomials: this does not change the set of solutions of the system in the torus $\left(\overline{k} \setminus \{0\}\right)^n$.

Assuming that the system $f_1 = \cdots = f_s = 0$ has finitely-many solutions in $(\overline{k} \setminus \{0\})^n$, we proceed as follows:

1. homogenize $(f_1, \ldots, f_s)$ via definition-proposition 5.10, in order to obtain polynomials $(f_1^{(h)}, \ldots, f_s^{(h)})$;
2. compute a sparse Gröbner basis with respect to a graded ordering of the homogeneous ideal $\mathcal{I} = \langle f_1^{(h)}, \ldots, f_m^{(h)} \rangle \subset \mathbb{K}[S_{\mathcal{M}}^{(h)}]$ by using the SAGBI Matrix F_5 algorithm 5.16, in this sparse context.
3. dehomogenize the output to obtain a sGB of the ideal $\langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[S_{\mathcal{M}}]$ (proposition 5.14);
4. use a sparse variant of FGLM to obtain a zero-dimensional triangular system (hence containing a univariate polynomial) whose solutions are the image of the toric solutions of $f_1 = \cdots = f_s = 0$ by monomial maps (algorithm 5.19);
5. compute the non-zero roots of the univariate polynomial and invert the monomial map to get the solutions.

We focus on the four first steps of this process. The fifth step involves computing the roots of a univariate polynomial, for which dedicated techniques exist and depend on the field $\mathbb{K}$. It also involves inverting a monomial map, which can be achieved by solving a consistent linear system of $|\operatorname{Hilb}(S_{\mathcal{M}})|$ equations in n unknowns.

In the sequel of this section, we investigate the behavior of sparse Gröbner bases under homogenization and dehomogeneization (Steps 1 and 3). We refer the reader to [26, Ch. 2] for geometrical aspects of projective toric varieties and their affine charts. From now on, $\mathcal{M}$ is a set of monomials which verifies the assumptions given in notations 3.95.

Example 5.7. *We follow example 5.3. In this case,* $\mathcal{M} = \{1, xy, x^2y, xy^2\}$*, the semigroup* $S = S_{\mathcal{M}}$ *was drawn in figure 5.4 and the semigroup* $S^{(h)} = S_{\mathcal{M}}^{(h)}$ *is drawn in figure 5.8*

There is a canonical dehomogenization map from $\mathbb{K}[S_{\mathcal{M}}^{(h)}]$ to $\mathbb{K}[S_{\mathcal{M}}]$:

Definition 5.9. *With notations 3.95, the morphism* $\chi_{\mathcal{M}}$*, defined by:*

$$\begin{array}{rccc} \chi_{\mathcal{M}} : & \mathbb{K}[S_{\mathcal{M}}^{(h)}] & \to & \mathbb{K}[S_{\mathcal{M}}] \\ & X^{(\mathbf{s},d)} & \mapsto & X^{\mathbf{s}} \end{array}$$

is a dehomogeneization morphism.

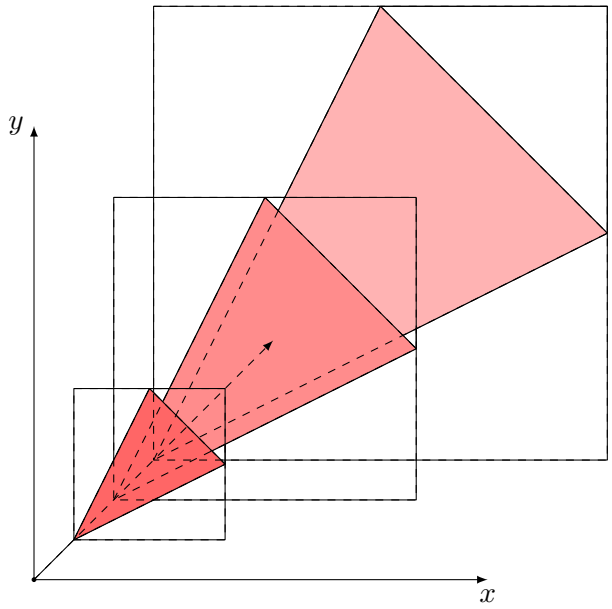


Figure 5.8 – The semigroup $S^{(h)}$

Definition – Proposition 5.10. *With notations 3.95, for any $f \in \mathbb{K}[S_\mathcal{M}]$, we call degree of f, the number*

$$\deg(f) = \min\{d \in \mathbb{N} \mid \chi_\mathcal{M}^{-1}(f) \cap \mathbb{K}[S_\mathcal{M}^{(h)}]_d \neq \emptyset\}$$

Moreover the set $\chi_\mathcal{M}^{-1}(f) \cap \mathbb{K}[S_\mathcal{M}^{(h)}]_{\deg(f)}$ contains a unique element, called the homogenization *of f.*

Proof. The only statement to prove is that $\chi_\mathcal{M}^{-1}(f) \cap \mathbb{K}[S_\mathcal{M}^{(h)}]_{\deg(f)}$ contains a unique element. Actually, the restriction of the map $\chi_\mathcal{M}$ to $\mathbb{K}[S_\mathcal{M}^{(h)}]_d$ is one-to-one: let $f^{(h)}, f'^{(h)} \in \chi_\mathcal{M}^{-1}(f) \cap \mathbb{K}[S_\mathcal{M}^{(h)}]_{\deg(f)}$. Then $\chi_\mathcal{M}(f^{(h)} - f'^{(h)}) = 0$, which implies $f^{(h)} = f'^{(h)}$. □

Example 5.11 (Continuation of exemple 5.7)**.** *Assume now that $\mathbb{K}$ is a small finite field, namely $\mathbb{K} = \mathbb{F}_{31}$. Let $F = \{f_1, f_2\}$ be the following set of polynomials in $\mathbb{K}[x, y]$:*

$$F = \left\{ \begin{array}{l} f_1 = x^2y + 20xy^2 + 17xy + 14, \\ f_2 = x^4y^2 + 4x^3y^3 + 29x^2y^4 + 20x^3y^2 + 5x^2y^3 + 2x^2y^2 + 8x^2y + 29xy^2 + 5xy + 5 \end{array} \right\}$$

Actually, these polynomials have been chose as random linear combinations of monomials in $\mathcal{M}$ and $\mathcal{M}^2 = \{m \times m' \mid m, m' \in \mathcal{M}\}$ with leading coefficient 1. Therefore, f_1 and f_2 belong to $\mathbb{K}[S_\mathcal{M}]$ with f_1 of degree 1 and f_2 of degree 2. Moreover, the homogeneizations of f_1 and f_2 are hf_1 and h^2f_2.

The next step is to prove that dehomogenizing a homogeneous Gröbner basis (with respect to a graded ordering) gives a Gröbner basis of the dehomogenized ideal.

Definition 5.12. *An admissible monomial ordering $\preceq$ on $\mathbb{K}[S_\mathcal{M}^{(h)}]$ is called* graded *if there exists an associated ordering (also denoted $\preceq$) on $\mathbb{K}[S_\mathcal{M}]$ such that*

$$X^{(\mathbf{s}_1,d_1)} \prec X^{(\mathbf{s}_2,d_2)} \quad \Longleftrightarrow \quad \left\{ \begin{array}{c} d_1 < d_2 \text{ or} \\ d_1 = d_2 \text{ and } X^{\mathbf{s}_1} \prec X^{\mathbf{s}_2} \end{array} \right.$$

Example 5.13 (Continuation of example 5.3)**.** *Recall that we put on the monomials of $S = S_{\mathcal{M}}$ the DRL ordering with $x \succ y$. Let h be the third variable in $S^{(h)}$. The natural graded monomial ordering on $\mathbb{K}[S^{(h)}]$ associated to the DRL ordering on $\mathbb{K}[S]$ is given by*

$$x^\alpha y^\beta h^\gamma \prec x^{\alpha'} y^{\beta'} h^{\gamma'} \quad \Longleftrightarrow \quad \gamma < \gamma' \quad or \quad \gamma = \gamma' \quad and \quad x^\alpha y^\beta \prec_{DRL} x^{\alpha'} y^{\beta'}$$

Proposition 5.14. *Let $\mathcal{G}$ be a homogeneous sparse-Gröbner basis of a homogeneous ideal $\mathcal{I} \subset \mathbb{K}[S_{\mathcal{M}}^{(h)}]$ with respect to a graded ordering. Then $\chi_{\mathcal{M}}(\mathcal{G})$ is a sGB of $\chi_{\mathcal{M}}(\mathcal{I})$ with respect to the associated ordering on $\mathbb{K}[S_{\mathcal{M}}]$.*

Proof. First, notice that $\chi_{\mathcal{M}}$ commutes with leading monomials on homogeneous components of $\mathbb{K}[S_{\mathcal{M}}^{(h)}]$: for any $f \in \mathbb{K}[S_{\mathcal{M}}^{(h)}]_d$, $\chi_{\mathcal{M}}(\mathsf{LM}_{\preceq}(f)) = \mathsf{LM}_{\preceq}(\chi_{\mathcal{M}}(f))$. Let $f \in \chi_{\mathcal{M}}(\mathcal{I})$ and $f^{(h)} \in \mathcal{I}$ be a homogeneous polynomial such that f is equal to $\chi_{\mathcal{M}}(f^{(h)})$. Consequently, there exists $g \in \mathcal{G}$ such that $\mathsf{LM}_{\preceq}(g)$ divides $\mathsf{LM}_{\preceq}(f^{(h)})$. Applying $\chi_{\mathcal{M}}$, we obtain that $\mathsf{LM}_{\preceq}(\chi_{\mathcal{M}}(g))$ divides $\mathsf{LM}_{\preceq}(\chi_{\mathcal{M}}(f^{(h)})) = \mathsf{LM}_{\preceq}(f)$. Therefore $\chi_{\mathcal{M}}(\mathcal{G})$ is a sGB of $\chi_{\mathcal{M}}(\mathcal{I})$ for the associated ordering. □

5.3 Algorithms

In this section, we describe variants of the classical algorithms Matrix-F_5 (algorithm 1.44) and FGLM (algorithm 1.52) in the context of semigroup algebras. The resulting Sparse-Matrix F_5 algorithm is no more than the already seen SAGBI-Matrix F_5 algorithm, used in a semigroup algebra.

5.3.1 Sparse-MatrixF5 algorithm

In this subsection, we describe an algorithm, which computes a sparse Gröbner basis of a homogeneous ideal in $\mathbb{K}[S_{\mathcal{M}}^{(h)}]$, truncated in some given degree. Actually, this algorithm has already been entirely described in chapter 1, since it is no more than a specialization of the SAGBI Matrix-F_5 algorithm (algorithm 1.68). However, the framework of monomial algebras is very close to the classical polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ and a critical pairs algorithm could be derived in the same fashion than the F_5-algorithm [35], while it is difficult in a general algebra. We say a few words on this purpose at the end of the subsection.

Algorithm. Remember that, in the SAGBI Matrix F_5-algorithm, we construct SAGBI-Macaulay matrices for each degree. The columns of the matrix at degree d is indexed by a basis of $\mathcal{A}_d$, the component of degree d of the ambient algebra $\mathcal{A}$, and the rows by all products $(b_j^{d-d_i}, f_i)$, b_j describing the basis of $\mathcal{A}_{d-d_i}$. In this context, the SAGBI-Macaulay matrices will be called Sparse-Macaulay matrices. Since the algebra $\mathcal{A} = \mathbb{K}[S_{\mathcal{M}}^{(h)}]$ is generated by monomials in $\mathcal{M}$, we take $\{\prod_{i=1}^d m_i \mid m_i \in \mathcal{M}\}$ as a basis of $\mathbb{K}[S_{\mathcal{M}}^{(h)}]_d$. The relation between the Sparse-Macaulay matrix and a D-sGB is given by:

Definition – Proposition 5.15. *Let $f_1, \ldots, f_s \in \mathbb{K}[S_{\mathcal{M}}^{(h)}]$ be homogeneous polynomials, $\preceq$ a graded monomial ordering, and for $d \in \mathbb{N}$, let G_d be the set of polynomials corresponding to the rows of the reduced row echelon form of the Sparse-Macaulay matrix in degree d of $f_1, \ldots f_s$. Then the following facts hold:*

- *For any $D \in \mathbb{N}$, $G_0 \cup \cdots \cup G_D$ is a D-sGB of $\mathcal{I}$*
- $\chi_{\mathcal{M}}(G_0) \subset \chi_{\mathcal{M}}(G_1) \subset \chi_{\mathcal{M}}(G_2) \subset \cdots$

The smallest integer ℓ such that $\chi_{\mathcal{M}}(G_\ell)$ is a sGB of the ideal $\chi_{\mathcal{M}}(\langle f_1, \ldots, f_s\rangle)$ is called the witness degree *and noted* $\mathrm{d}_{\mathrm{wit}}$.

Proof. The first statement ($G_0 \cup \cdots \cup G_D$ is a D-sGB of $\mathcal{I}$) follows from the fact that G_d is a triangular basis of the vector space $\mathbb{K}[S^{(h)}_{\mathcal{M}}]_d$. The second statement is deduced from the inclusions $\chi_{\mathcal{M}}(\mathbb{K}[S^{(h)}_{\mathcal{M}}]_0) \subset \chi_{\mathcal{M}}(\mathbb{K}[S^{(h)}_{\mathcal{M}}]_1) \subset \ldots$. Let G be a sGB of $\langle f_1, \ldots, f_s\rangle$. Then $\mathrm{d}_{\mathrm{wit}}$ is bounded above by $\max\{\deg(g) \mid g \in G\}$ and is therefore finite. □

Algorithm 5.16: Sparse-Matrix F5

Input : Homogeneous $f_1, \ldots, f_s \in \mathbb{K}[S^{(h)}_{\mathcal{M}}]$ of resp. degrees $(d_1, \ldots, d_s)$, a graded monomial ordering $\preceq$ on $\mathbb{K}[S^{(h)}_{\mathcal{M}}]$, a positive degree D
Output: a D-Gröbner basis of $\langle f_1, \ldots, f_s\rangle$ with respect to $\preceq$

```
for i = 1 to s do G_i := ∅ ;
for d = 1 to D do
    M_{d,0} := ∅, M̃_{d,0} := ∅;
    for i = 1 to s do
        if d < d_i then
            M_{d,i} := M̃_{d,i-1}
        else
            M_{d,i} := matrix obtained by adding new rows X^{(s,d-d_i)} f_i to M̃_{d,i-1}, for all
            monomials X^{(s,d-d_i)} ∈ K[S^{(h)}_M]_{d-d_i} that are not in ⟨LM_⪯(G_{i-1})⟩.
        Compute the row echelon form M̃_{d,i} of M_{d,i};
        Add to G_i all rows of M̃_{d,i} not top reducible by G_i;
return G_s
```

In practice, the choice of the parameter D in Algorithm 5.16 is driven by the explicit bounds on the witness degree that we shall derive in Section 5.4.

Example 5.17.

We explain the behavior of the Sparse-Matrix F_5 algorithm 5.16 on a small example which follows the examples given in the previous section. We set $\mathbb{K} = \mathbb{F}_{31}$ and S the semigroup generated by $\{xy, x^2y, xy^2\}$ in $\mathbb{K}[x, y]$. We are interested in computing a sparse Gröbner basis of the ideal generated by

$$\mathsf{F} = \left\{ \begin{array}{l} f_1 = x^2y + 20xy^2 + 17xy + 14, \\ f_2 = x^4y^2 + 4x^3y^3 + 29x^2y^4 + 20x^3y^2 + 5x^2y^3 + 2x^2y^2 + 8x^2y + 29xy^2 + 5xy + 5 \end{array} \right\}$$

These two polynomials have degree 1 and 2 and their homogeneizations in $\mathbb{K}[S^{(h)}]$ are hf_1 and h^2f_2. Since algorithm 5.16 works only with homogeneous polynomials, we will not indicate the homogeneization variable h in the sequel. Theoretical study shows that D can be set to 4, as we will see in the next section.

At step $d = 1$, only f_1 is considered and the algorithm constructs the matrices

$$\widetilde{M}_{1,2} = M_{1,2} = \widetilde{M}_{1,1} = M_{1,1} = 1 \times f_1 \quad \begin{array}{c} \\ \begin{pmatrix} 1 & 20 & 17 & 14 \end{pmatrix} \end{array} \begin{array}{c} x^2y \quad xy^2 \quad xy \quad 1 \end{array}$$

After this step, we have $\mathcal{G}_1 = \mathcal{G}_2 = \{f_1\}$.

At step $d = 2$, the matrix $M_{2,1}$ is build by writing polynomials $\{mf_1 \mid m \in \mathcal{M}\}$ in a matrix having its columns indexed by $\mathcal{M}^2 = \{x^4y^2, x^3y^3, x^2y^4, x^3y^2, x^2y^3, x^2y^2, x^2y, xy^2, xy, 1\}$. Some reductions can be performed in order to obtain a matrix in row-echelon form, and we indicate $\widetilde{M}_{2,1}$ (the labels of the rows correspond to the original ones, but some rows-reductions have been applied)

$$\widetilde{M}_{2,1} = \begin{array}{c} \\ x^2y \times f_1 \\ xy^2 \times f_1 \\ xy \times f_1 \\ 1 \times f_1 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^4y^2 & x^3y^3 & x^2y^4 & x^3y^2 & x^2y^3 & x^2y^2 & x^2y & xy^2 & xy & 1 \end{array} \\ \begin{pmatrix} 1 & 0 & 3 & 0 & 2 & 21 & 0 & 29 & 20 & 21 \\ 0 & 1 & 20 & 0 & 17 & 0 & 0 & 14 & 0 & 0 \\ 0 & 0 & 0 & 1 & 20 & 17 & 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 20 & 17 & 14 \end{pmatrix} \end{array}$$

Of course, all of these rows are reducible by f_1 and no polynomial is added to $\mathcal{G}_1$. Adding f_2 to this matrix and applying another row-echelon form computation leads to the matrix

$$\widetilde{M}_{2,2} = \begin{array}{c} \\ x^2y \times f_1 \\ xy^2 \times f_1 \\ xy \times f_1 \\ 1 \times f_1 \\ 1 \times f_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^4y^2 & x^3y^3 & x^2y^4 & x^3y^2 & x^2y^3 & x^2y^2 & x^2y & xy^2 & xy & 1 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 20 & 0 & 17 & 15 & 7 \\ 0 & 1 & 0 & 0 & 17 & 14 & 0 & 27 & 8 & 10 \\ 0 & 0 & 0 & 1 & 20 & 17 & 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 20 & 17 & 14 \\ 0 & 0 & 1 & 0 & 0 & 21 & 0 & 4 & 12 & 15 \end{pmatrix} \end{array}$$

The monomial x^2y^4 is not reducible by x^2y (because $y^3 \notin S$). Hence, the polynomial $\tilde{f}_2 = x^2y^4 + 21x^2y^2 + 4xy^2 + 12xy + 15$ is added to $\mathcal{G}_2$ which is now equal to $\{f_1, \tilde{f}_2\}$.

We skip the construction of the matrix $M_{3,1}$ and its reduction to $\widetilde{M}_{3,1}$. In order to build $M_{3,2}$, we have to add to $\widetilde{M}_{3,1}$ the rows mf_2 with m a monomial in $\mathcal{M}$ such that $m \notin \mathsf{LM}_{\preceq}(\langle \mathcal{G}_1 \rangle)$. Since x^2y appears as leading monomial of a row in $\widetilde{M}_{1,1}$, it can be removed. Hence, we just have to add the rows xy^2f_2, xyf_2 and f_2. After reduction, we obtain the following full-rank matrix (the columns indexed by the lowest monomials have been removed):

$$\widetilde{M}_{3,2} = \begin{array}{c} \\ x^4y^2 \times f_1 \\ x^3y^3 \times f_1 \\ x^2y^4 \times f_1 \\ x^3y^2 \times f_1 \\ x^2y^3 \times f_1 \\ x^2y^2 \times f_1 \\ x^2y \times f_1 \\ xy^2 \times f_1 \\ xy \times f_1 \\ 1 \times f_1 \\ xy^2 \times f_2 \\ xy \times f_2 \\ 1 \times f_2 \end{array} \begin{array}{c} \begin{array}{cccccccccccc} x^6y^3 & x^5y^4 & x^4y^5 & x^3y^6 & x^5y^3 & x^4y^4 & x^3y^5 & x^4y^3 & x^3y^4 & x^4y^2 & x^3y^3 & x^2y^4 & \dots \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 20 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 14 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 17 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 20 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 21 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \dots \end{pmatrix} \end{array}$$

The leading monomials of the three new rows (after reduction) are x^2y^4, x^3y^5 and x^3y^6. All these monomials are reducible by $\mathcal{G}_2$ since $x^2y^4 = \mathsf{LM}_{\preceq}(\tilde{f}_2)$, $x^3y^5 = xy\mathsf{LM}_{\preceq}(\tilde{f}_2)$ and $x^3y^6 = xy^2\mathsf{LM}_{\preceq}(\tilde{f}_2)$, with $1, xy, xy^2 \in S$. Hence, no new polynomial is entered in $\mathcal{G}_2$ at this step. We skip the final step ($d = D = 4$), which leads to the full rank matrix $\widetilde{M}_{4,2}$ but does not give a new polynomial in $\mathcal{G}_2$. The algorithm stops and return $\mathcal{G}_2 = \{f_1, \tilde{f}_2\}$ which is actually a sGB of $\langle f_1, f_2 \rangle$.

Remark 5.18. *Actually, the algorithm would have return the homogeneized polynomials* $\{hf_1, h^2\tilde{f}_2\}$ *of* $\mathbb{K}[S^{(h)}]$. *Applying the deshomogeneization morphism* $\chi_{\mathcal{M}}$ *gives us the Gröbner basis* $\{f_1, \tilde{f}_2\}$.

Further work. In order to translate the Sparse-Matrix F_5 algorithm in a F_5 fashion [35], we would have to extend Buchberger's algorithm in the context of a semigroup algebra. There is only one step of the algorithm to modify: the construction of the S-polynomials. Actually, for $\mathbf{s}_1, \mathbf{s}_2 \in S$ two elements of the semigroup, their LCM is replaced by the intersection of the ideals $\langle \mathbf{s}_1 \rangle \cap \langle \mathbf{s}_2 \rangle$. In general, this ideal is not principal. Let $\mathbf{s}_1 \vee \mathbf{s}_2$ denote the minimal generators of $\langle \mathbf{s}_1 \rangle \cap \langle \mathbf{s}_2 \rangle$. Consequently, the S-polynomial of $f_1, f_2 \in \mathbb{K}[S]$ is no longer unique and is actually a set of polynomials defined as

$$\left\{ \frac{X^{\mathbf{s}} f_1}{\mathsf{LT}_{\preceq}(f_1)} - \frac{X^{\mathbf{s}} f_2}{\mathsf{LT}_{\preceq}(f_2)} : \mathbf{s} \in \mathsf{LM}_{\preceq}(f_1) \vee \mathsf{LM}_{\preceq}(f_2) \right\},$$

and the set $\mathsf{LM}_{\preceq}(f_1) \vee \mathsf{LM}_{\preceq}(f_2)$ can be computed via [102, Subroutine 11.21]. Changing only this definition of S-polynomials provides a variant of Buchberger's algorithm in a semigroup algebra $\mathbb{K}[S]$. In addition, with the SAGBI-F_5 criterion 1.69, we get rid of all reductions to zero if the input is a regular sequence in $\mathbb{K}[S]$. An efficient computation of these critical pairs has not been implemented yet and would be an interesting step, in order to improve this approach. For example in the previous algorithm, we would have detected that $\mathcal{G}_2 = \{f_1, \tilde{f}_2\}$ is a sGB and stopped the computation at step $d = 2$.

5.3.2 Sparse-FGLM algorithm

The variant of the FGLM algorithm presented in this section is closed to the SAGBI-FGLM (algorithm 4.101) presented in subsection 4.3.2. Indeed, the Normal Form provided by the sparse Gröbner basis allows us to look for linear combinations of powers of elements of S in the quotient algebra $\mathbb{K}[S]/\mathcal{I}$. However, the context is nicer here, for two reasons:

— the sparse Gröbner basis allows us to test the membership in $\mathcal{I}$ for a polynomial of any degree.

— under the assumption that the semigroup is *simplicial*, the matrices of multiplication by some element in the *Hilbert basis* (see proposition-definition 3.88) of S can be computed easily.

Let $(p_1, \ldots, p_r)$ be the Hilbert basis of a semigroup $S \subset \mathbb{Z}^n$. Given new indeterminates $H = \{H_1, \ldots, H_r\}$, any monomial in $\mathbb{K}[S]$ is the image of a monomial in $\mathbb{K}[H]$ via the morphism

$$\begin{array}{rccc} \varphi : & \mathbb{K}[H_1, \ldots, H_r] & \longrightarrow & \mathbb{K}[S] \\ & H_i & \longmapsto & X^{p_i} \end{array}$$

Given an admissible monomial ordering $\preceq_H$ on the ring $\mathbb{K}[H_1, \ldots, H_r]$, an ideal $\mathcal{I} \subset \mathbb{K}[S]$ and a normal form relative to $\mathcal{I}$ (given for instance by a sparse Gröbner basis of $\mathcal{I}$), Algorithm 5.19 computes a Gröbner basis of $\varphi^{-1}(\mathcal{I})$. Note that

$$\psi\left(Var(\mathcal{I}) \cap (\overline{\mathbb{K}}^*)^n\right) = Var\left(\varphi^{-1}(\mathcal{I})\right) \cap (\overline{\mathbb{K}}^*)^r,$$

where $\psi : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^r$ is the map $\mathbf{x} \mapsto (\mathbf{x}^{p_1}, \ldots, \mathbf{x}^{p_r})$. Also, we would like to point out that Algorithm 5.19 does not depend on the support of the input sparse system, but only on the ambient semigroup $S_{\mathcal{M}}$.

Algorithm 5.19: Sparse FGLM

Input : - a sparse Gröbner-basis $\mathcal{G}$ of $\mathcal{I}$ in $\mathbb{K}[S]$ with respect to $\preceq$
-a monomial ordering $\preceq_H$ on $\mathbb{K}[H_1,\dots,H_r]$
-a monomial map $\varphi : \mathbb{K}[H_1,\dots,H_r] \to \mathbb{K}[S]$

Output: A Gröbner basis in $\mathbb{K}[H_1,\dots,H_r]$ with respect to $\preceq_H$

$L := [1]$; `//list of monomials in` $\mathbb{K}[H_1,\dots,H_r]$
$E := [\,]$; `//staircase for the new ordering` $\preceq_H$
$V := [\,]$; `//` $V = \mathsf{NF}_{\preceq}(\varphi(S), \mathcal{G})$
$G := [\,]$; `//The Gröbner basis in` $\mathbb{K}[H_1,\dots,H_r]$
while $L \neq [\,]$ **do**
  $m := L[1]$; and Remove m from L;
  $v := \mathsf{NF}_{\preceq}(\varphi(m), \mathcal{G})$; (1)
  $e := \#E$;
  if $v \in \mathit{Span}_{\mathbb{K}}(V)$ **then**
    $\exists\,(\lambda_i) \in \mathbb{K}^e$ such that $v = \sum_{i=1}^{e} \lambda_i \cdot V_i$; (2)
    $G := G \cup \left[m - \sum_{i=1}^{e} \lambda_i \cdot E_i \right]$;
    Remove from L the elements top-reducible by G.
  else
    $E := E \cup [m]$; $V := V \cup [v]$; (3)
    $L := \mathrm{Sort}(L \cup [H_i\, m \mid i = 1,\dots,r], \preceq_H)$;
    Remove from L duplicate elements;
Return G;

The main principle of Algorithm 5.19 is similar to the original FGLM Algorithm [39]: we consider the monomials in $\mathbb{K}[H_1,\dots,H_r]$ in increasing order until we obtain sufficiently many linear relations between their normal forms. The only difference is that the computations of the normal forms are performed in $\mathbb{K}[S]$ (using a previously computed sparse Gröbner basis) via the morphism φ. For solving sparse systems, we choose the *lexicographical ordering* for $\preceq_H$.

Theorem 5.20. *Algorithm Sparse-FGLM is correct: it computes the reduced Gröbner basis of the ideal $\varphi^{-1}(\mathcal{I}) \subset \mathbb{K}[H_1,\dots,H_r]$ with respect to $\preceq_H$.*

Proof. Let $G = (g_1,\dots,g_\mu)$ be the output of algorithm 5.19. Set $m_i = \mathsf{LM}_{\preceq}(g_i)$. First, we prove that $G \subset \varphi^{-1}(\mathcal{I})$. Notice that each g_i is of the form $m_i - q$, where $\varphi(q) = \mathsf{NF}_{\preceq}(\varphi(m_i), \mathcal{G})$. Consequently, $\mathsf{NF}_{\preceq}(\varphi(g_i), \mathcal{G}) = 0$ and hence $g_i \in \varphi^{-1}(\mathcal{I})$. Next, let $h \in \mathbb{K}[H]$ be a polynomial such that $\mathsf{LM}_{\preceq}(h) \notin \langle \mathsf{LM}_{\preceq}(G) \rangle$. Up to reducing its nonleading monomials by G, we can assume without loss of generality that all its monomials do not belong to $\langle \mathsf{LM}_{\preceq}(G) \rangle$. Therefore, the normal forms of the images by φ of all the monomials in the support of h are linearly independent in $\mathbb{K}[S]/\mathcal{I}$ (otherwise the linear relation would have been detected by algorithm 5.19), which means that $\mathsf{NF}_{\preceq}(\varphi(h), \mathcal{G}_) \neq 0$ and hence $h \notin \varphi^{-1}(\mathcal{I})$, which concludes the proof that G is a Gröbner basis of $\varphi^{-1}(\mathcal{I})$. The proof that G is reduced is similar. □

As usual, the steps **(1)**, **(2)** and **(3)** are done by linear algebra (at step **(3)** we use the Update procedure 1.54) to maintain a link between the staircase in construction E and

the elements $\mathsf{NF}_{\preceq}(\varphi(u), \mathcal{G})$ for u in E). If S is assumed to be simplicial, a complexity of $O(r \cdot \dim_{\mathbb{K}}(\mathbb{K}[S]/\mathcal{I})^3)$ can be ensured, see the next section.

Example 5.21 (Continuation of example 5.17)**.** *We end up this section by applying briefly the algorithm 5.19 to the sparse Gröbner basis $\mathcal{G}$ computed in the previous example. The staircase (monomials of S that are not reducible by $\mathcal{G}$) is of size 6 and is given by $\mathcal{E} = \{x^3y^4, x^2y^3, x^2y^2, xy^2, xy, 1\}$. The staircase and the other points in S are drawn in figure 5.22.*

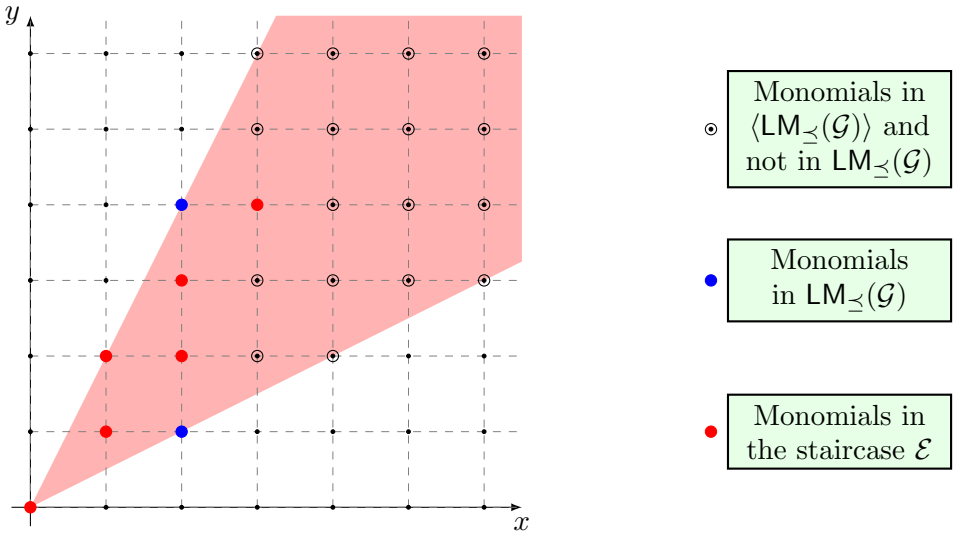


Figure 5.22 – Staircase and leading monomials of the sGB $\mathcal{G}$.

The Hilbert basis of S is $\{x^2y, xy^2, xy\}$. Hence, we introduce three variables H_1, H_2 and H_3 and consider the map

$$\begin{array}{rccc} \varphi: & \mathbb{K}[H_1, H_2, H_3] & \longrightarrow & \mathbb{K}[S] \\ & H_1 & \longmapsto & x^2y \\ & H_2 & \longmapsto & xy^2 \\ & H_3 & \longmapsto & xy \end{array}$$

We put the ordering $\preceq_H$ equal to the lexicographical ordering with $H_1 \succ H_2 \succ H_3$ on $\mathbb{K}[H_1, H_2, H_3]$. The following table indicates the computation of the staircase in the new variables H_1, H_2 and H_3.

m	v	E	$v \in \mathsf{Span}_{\mathbb{K}}(V)$?
H_3^0	1	$[\,]$	*false*
H_3^1	xy	$[1]$	*false*
H_3^2	x^2y^2	$[1, H_3]$	*false*
H_3^3	$14x^2y^3 + 17x^2y^2 + 4xy^2 + 23xy + 21$	$[1, H_3, H_3^2]$	*false*
H_3^4	$14x^3y^4 + 25x^2y^3 + 2x^2y^2 + 6xy^2 + 9xy + 16$	$[1, H_3, H_3^2, H_3^3]$	*false*
H_3^5	$15x^3y^4 + 11x^2y^3 + 13x^2y^2 + 13xy^2 + 21xy$	$[1, H_3, H_3^2, H_3^3, H_3^4]$	*false*
H_3^6	$18x^3y^4 + 22x^2y^3 + 15x^2y^2 + 2xy^2 + 27xy + 11$	$[1, H_3, H_3^2, H_3^3, H_3^4, H_3^5]$	*true*

Since $\mathsf{NF}_{\preceq}(H_3^6, \mathcal{G})$ is linearly dependent of $\{\mathsf{NF}_{\preceq}(H_3^i, \mathcal{G}) \mid 0 \leq i \leq 5\}$, the polynomial given by this dependence (namely $H_3^6 + 28H_3^5 + 13H_3^4 + 13H_3^3 + 25H_3^2 + 23H_3 + 4$) is added to the

Gröbner basis in construction. The next monomials that have to be examinated are H_2 and H_1 which also lead to new polynomials. The algorithm stops and returns

$$\mathcal{G}_H = \left\{ \begin{array}{l} H_1 + 7H_3^5 + 8H_3^4 + 9H_3^3 + 19H_3^2 + 25H_3 + 7 \\ H_2 + 26H_3^5 + 12H_3^4 + 29H_3^3 + 13H_3^2 + 12H_3 + 5 \\ H_3^6 + 28H_3^5 + 13H_3^4 + 13H_3^3 + 25H_3^2 + 23H_3 + 4 \end{array} \right\}$$

In practice, the semigroup S is simplicial, and this computation has been done by first computing the multiplication matrices in $\mathbb{K}[S]/\langle\mathcal{G}\rangle$ by xy, xy^2 and x^2y, in the same fashion than the computation of the multiplication matrices in the classical FGLM algorithm 1.52.

5.4 Complexity

This section is devoted to the complexity of Algorithms 5.16 and 5.19 when the input system is a homogeneous (semi-)regular sequence in a polytopal algebra $\mathbb{K}[\mathscr{P}]$.

Complexity model. All the complexity bounds count the number of arithmetic operations $\{+, \times, -, \div\}$ in $\mathbb{K}$; each of them is counted with unit cost. It is not our goal to take into account operations in the semigroup S.

The next goal is to bound $\mathrm{d_{wit}}$ (see definition-proposition 5.15) via the Hilbert series of $\mathbb{K}[S]/\mathcal{I}$. In the case of regular sequences, this Hilbert series can be easily computed by the classical formula:

Proposition 5.23. *Let $\mathscr{P}$ be a normal lattice polytope, $f_1, \ldots, f_s \in \mathbb{K}[\mathscr{P}]$ be a homogeneous regular sequence of homogeneous polynomials of respective degrees $(d_1, \ldots, d_s)$ and $\mathcal{I} = \langle f_1, \ldots, f_s\rangle \subset \mathbb{K}[\mathscr{P}]$. Then*

$$\mathsf{HS}_{\mathbb{K}[\mathscr{P}]/\mathcal{I}}(z) = \mathsf{HS}_{\mathscr{P}}(z) \cdot \prod_{i=1}^{s}(1 - z^{d_i}).$$

Proof. This is only a specialisation of corollary 2.23 in this context. □

Example 5.24 (Continuation of example 5.21)**.** *The semigroup algebra $\mathbb{K}[S^{(h)}]$ is a polytopal algebra since $\mathcal{M} = \{1, xy, x^2y, xy^2\}$ are the integer points of a polytope. The Hilbert series $\mathsf{HS}_{\mathscr{P}}(z)$ can be easily computed by hand in this case, and is equal to $\frac{Q(z)}{(1-z)^3}$ with $Q(z) = 1+z+z^2$. Notice that this is coherent with the result stated at the end of the section 3.2 since Q is a polynomial with positive coefficients of degree $n - \ell + 1$, with $n = 2$ and $\ell = 1$ is the smallest integer such that $\ell \cdot \mathscr{P}$ has an integer interior point. Hence, if (f_1, f_2) is regular of degrees $(1, 2)$, $\mathsf{HS}_{\mathbb{K}[\mathscr{P}]/\mathcal{I}}(z) = \frac{Q(z)(1+z)}{1-z}$.*

The next lemma gives an explicit bound for the witness degree of regular sequences in a polytopal algebra $\mathbb{K}[\mathscr{P}]$ when $\mathscr{P}$ is normal:

Lemma 5.25. *Let $\mathscr{P} \subset \mathbb{R}^n$ be a normal lattice polytope and $f_1, \ldots, f_n$ be a homogeneous regular sequence in $\mathbb{K}[\mathscr{P}]$ of degrees $(d_1, \ldots, d_n)$. Then any $\left[\mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1)\right]$-sGB of the ideal $\mathcal{I} = \langle f_1, \ldots, f_n\rangle$ is a sGB of $\mathcal{I}$. In other words $\mathrm{d_{wit}} \leq \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1)$.*

Proof. By proposition 5.23 and with the notations of proposition 3.103, the Hilbert series of $\mathbb{K}[\mathscr{P}]/\mathcal{I}$ is equal to

$$\begin{aligned} \mathsf{HS}_{\mathscr{P}}(z)\prod_{i=1}^{n}(1-z^{d_i}) &= \frac{Q(z)\prod_{i=1}^{n}(1-z^{d_i})}{(1-z)^{n+1}} \\ &= \frac{Q(1)\prod_{i=1}^{n} d_i}{1-z} + K(z) \end{aligned}$$

where $K(z) \in \mathbb{Z}[z]$ is a univariate polynomial with $\deg(K(z)) = \mathrm{reg}(\mathbb{K}[\mathscr{P}]) - 1 + \sum_{i=1}^{p}(d_i - 1)$. Now, notice that the Hilbert series of $\mathbb{K}[\mathscr{P}]/\mathcal{I}$ is equal to that of $\mathbb{K}[\mathscr{P}]/\mathsf{LM}_{\preceq}(\mathcal{I})$. Therefore $\mathsf{HP}_{\mathbb{K}[\mathscr{P}]/\mathsf{LM}_{\preceq}(\mathcal{I})}(d)$ is constant for $d \geq \deg(K(z)) + 1$. Since $\ell < \ell'$ implies $\ell\mathscr{P} \subset \ell'\mathscr{P}$, we obtain

$$\max\{d \in \mathbb{N} \mid \exists X^{(\mathbf{s},d)} \notin \mathsf{LM}_{\preceq}(\mathcal{I}) \text{ s.t } \mathbf{s} \in (d\cdot\mathscr{P}) \cap \mathbb{Z}^n \text{ and } \mathbf{s} \notin ((d-1)\cdot\mathscr{P}) \cap \mathbb{Z}^n\} = \deg(K(z)) + 1.$$

Consequently, minimal generators of $\mathsf{LM}_{\preceq}(\mathcal{I})$ and hence minimal homogeneous Gröbner bases of $\mathcal{I}$ have degree at most $\deg(K(z)) + 2 = \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1)$. □

Example 5.26 (Continuation of example 5.24)**.** *With $\mathcal{I} = \langle f_1, f_2\rangle$, the Hilbert series of $\mathbb{K}[\mathscr{P}]/\mathcal{I}$ can also be written $\mathsf{HS}_{\mathbb{K}[\mathscr{P}]/\mathcal{I}}(z) = \frac{6}{1-z} - 5 - 3z - z^2 = \frac{Q(1)\prod_{i=1}^{n} d_i}{1-z} + K(z)$ with $d_1 = 1, d_2 = 2$ and $K(z) = -5 - 3z - z^2$. We recover the fact that the maximal degree of a monomial in the staircase has degree $\deg(K(z)) + 1 = 3$. That is why we took $D = 4$ in the Sparse-Matrix F_5 algorithm in example 5.17.*

Now that we have an upper bound for the witness degree, we can estimate the cost of computing a sGB by reducing the Macaulay matrix in degree $\mathrm{d_{wit}}$ (although the sparse-Matrix F5 algoritm is a much faster way to compute a sGB in practice, it is not easy to bound precisely its complexity). Note that $\mathrm{reg}(\mathbb{K}[\mathscr{P}])$ in the following theorem can be deduced from Prop. 3.110.

Theorem 5.27. *With the same notations as in Lemma 5.25, the complexity of computing a sGB of $\chi_{\mathscr{P}\cap\mathbb{Z}^n}(\langle f_1, \dots f_n\rangle) \subset \mathbb{K}[S_{\mathscr{P}\cap\mathbb{Z}^n}]$ by reducing the Macaulay matrix in degree $\mathrm{d_{wit}}$ is bounded above by*

$$O\left(n\,\mathsf{HP}_{\mathscr{P}}(\mathrm{d_{wit}})^{\omega}\right)$$

where $\mathrm{d_{wit}} \leq \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1)$ and ω is a feasible exponent for the matrix multiplication ($\omega < 2.373$ with [108]).

Proof. Let $\mathcal{I} \subset \mathbb{K}[\mathscr{P}]$ be the ideal generated by $(f_1, \dots, f_n)$. The number of columns and rows of the Macaulay matrix in degree d are respectively

$$\begin{aligned} \mathrm{nb_{cols}} &= \mathsf{HP}_{\mathscr{P}}(d), \\ \mathrm{nb_{rows}} &= \textstyle\sum_{i=1}^{n} \mathsf{HP}_{\mathscr{P}}(d - \deg(f_i)) \leq n\,\mathsf{HP}_{\mathscr{P}}(d). \end{aligned}$$

Consequently, the row echelon form of such a matrix can be computed within $O(n\,\mathsf{HP}_{\mathscr{P}}(d)^{\omega})$ field operations [97, Prop. 2.11]. By Proposition 5.14 and Lemma 5.25, for

$$d = \mathrm{d_{wit}} \leq \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1 + \sum_{j=1}^{n}(d_j - 1),$$

this provides a sGB of $\chi_{\mathscr{P}\cap\mathbb{Z}^n}(\mathcal{I})$. □

We now investigate the complexity of Algorithm 5.19 when $\mathcal{I} \subset \mathbb{K}[S]$ is a zero-dimensional ideal, and use the same notations as in Section 5.3.2. Notice that the map φ induces an isomorphism $\psi : \mathbb{K}[H]/\varphi^{-1}(\mathcal{I}) \to \mathbb{K}[S]/\mathcal{I}$ and therefore Algorithm 5.19 may be seen as a way to change the representation of $\mathbb{K}[S]/\mathcal{I}$.

Theorem 5.28. *Set $\delta = \dim_{\mathbb{K}}(\mathbb{K}[S]/\mathcal{I})$ and let r be the cardinality of the Hilbert basis of S. If S is a simplicial affine semigroup (see Def. 3.91) and $\mathbb{K}[S]$ is Cohen-Macaulay, then given a sGB of $\mathcal{I}$, algorithm 5.19 computes the Gröbner basis G with at most $O(r \cdot \delta^3)$ operations in $\mathbb{K}$.*

Proof. Once the r matrices of size $\delta \times \delta$ representing the multiplications by p_i in the canonical monomial basis of $\mathbb{K}[S]/\mathcal{I}$ are known, Step **(1)** in Algorithm 5.19 can be achieved in $O(\delta^2)$ as in the classical FGLM Algorithm 1.52. Steps **(2)** and **(3)** are done by linear algebra as in FGLM, which leads to a total complexity of $O(r \cdot \delta^3)$ since the same analysis holds. It remains to prove that the multiplication matrices can be constructed in $O(r \cdot \delta^3)$ operations (this is a consequence of proposition 1.49 in the classical case). Since $\mathbb{K}[S]$ is Cohen-Macaulay and S is simplicial, we obtain by [89, Thm. 1.1] that for any two distinct $p_i, p_j \in \mathrm{Hilb}(S)$ and for any $\mathbf{s} \in S$, if $\mathbf{s} - p_i$ and $\mathbf{s} - p_j$ are in S then $\mathbf{s} - p_i - p_j \in S$. With this extra property, the proof of proposition 1.49 extends to semigroup algebras. □

If the input system is a regular sequence of Laurent polynomials, then δ can be bounded by the mixed volume of their Newton polytopes by Kushnirenko-Bernstein's Theorem [8].

5.5 Dense, multi-homogeneous and overdetermined systems

In this section, we specialize Theorems 5.27 and 5.28 to several semigroups to obtain new results on the complexity of solving inhomogeneous systems with classical Gröbner bases algorithms ($\mathscr{P}$ is the standard simplex), multi-homogeneous systems ($\mathscr{P}$ is a product of simplices) and we state a variant of Fröberg's conjecture for overdetermined sparse systems.

Inhomogeneous dense systems. If $\mathscr{P} = \Delta_n$ is the standard simplex in $\mathbb{R}^n$, then computations of a sparse Gröbner basis in the cone over Δ_n correspond to classical Gröbner bases computations using the so-called "sugar strategy" introduced in [52]. Applying directly Theorems 5.27 and 5.28 with $\mathscr{P} = \Delta_n$ gives

Corollary 5.29. *Let $f_1, \ldots, f_n$ be a regular sequence of inhomogeneous polynomials of respective degrees $(d_1, \ldots, d_n)$ in $\mathbb{K}[x_1, \ldots, x_n]$. Then the complexity of computing a classical Gröbner basis of $\langle f_1, \ldots, f_n \rangle$ with respect to a graded monomial ordering is bounded by*

$$O\left(n\binom{n + \mathrm{d}_{\mathrm{wit}}}{n}^{\omega}\right),$$

where $\mathrm{d}_{\mathrm{wit}} \leq 1 + \sum_{i=1}^{n}(d_i - 1)$.

This statement was already known under the assumption that the system of the homogeneous parts of highest degree $f_1^{\infty}, \ldots, f_n^{\infty}$ is also regular, see *e.g.* [3]. However, this condition is not verified for several systems appearing in applications. Up to our knowlegde, this is the first time that such complexity results are obtained for inhomogenous systems without any assumption on $f_1^{\infty}, \ldots, f_n^{\infty}$.

Multi-homogeneous systems. Another class of polynomials appearing frequently in applications are *multi-homogeneous systems*. A polynomial of multi-degree $(d_1, \ldots, d_\ell)$ w.r.t.

a partition of the variables in blocks of sizes $(n_1, \ldots, n_\ell)$ is a polynomial whose Newton polytope is included in $d_1\Delta_{n_1} \times \cdots \times d_\ell\Delta_{n_\ell}$. In that case, the associated polytope is a product of simplices, which allows us to state the following complexity theorem:

Theorem 5.30. *Let $f_1, \ldots, f_n$ be a regular sequence of polynomials of multi-degree $(d_1, \ldots, d_n)$ w.r.t. a partition of the variables in blocks of sizes $(n_1, \ldots, n_\ell)$ (with $n_1+\cdots+n_\ell = n$). Then the combined complexity of Steps (1) to (4) of the solving process in Section 5.2 is bounded by*

$$O\left(n\, \mathsf{HP}_{\mathscr{P}}(\mathrm{d_{wit}})^\omega + n\,\mathrm{vol}(\mathscr{P})^3\right)$$

where $\mathscr{P} = d_1\Delta_{n_1} \times \cdots \times d_\ell\Delta_{n_\ell}$, $\mathrm{d_{wit}}$ is less than or equal to $n+2-\max_{i\in\{1,\ldots,\ell\}}(\lceil (n_i+1)/d_i\rceil)$, the Hilbert polynomial evaluated at $\mathrm{d_{wit}}$ is equal to $\mathsf{HP}_{\mathscr{P}}(\mathrm{d_{wit}}) = \binom{n_1+\mathrm{d_{wit}}\cdot d_1}{n_1}\cdots\binom{n_\ell+\mathrm{d_{wit}}\cdot d_\ell}{n_\ell}$ and $\mathrm{vol}(\mathscr{P}) = \binom{n}{n_1,\ldots,n_\ell}\prod_{i=1}^\ell d_i^{n_i}$.

Proof. Applying Theorems 5.27 and 5.28 with $\mathscr{P}$ equal to $d_1\Delta_{n_1} \times \cdots \times d_\ell\Delta_{n_\ell}$ yields the complexity bound in terms of $\mathrm{d_{wit}}$, $\#\,\mathrm{Hilb}(S_{\mathscr{P}\cap\mathbb{Z}^n})$ and δ. First, notice that the semigroup generated by $\mathscr{P}\cap\mathbb{Z}^n$ is $\mathbb{N}^n$, and hence $\#\,\mathrm{Hilb}(S_{\mathscr{P}\cap\mathbb{Z}^n}) = n$. Next, the polytope

$$\beta(d_1\Delta_{n_1} \times \cdots \times d_\ell\Delta_{n_\ell})$$

has an interior lattice point if and only if for all i, $\beta d_i\Delta_{n_i}$ has an interior lattice point, that is if and only if $\beta d_i > n_i$. The smallest β that verifies this condition is

$$\max(\lceil (n_1+1)/d_1\rceil, \ldots, \lceil (n_\ell+1)/d_\ell\rceil).$$

By Prop. 3.110, $\mathrm{reg}(\mathbb{K}[\mathscr{P}]) = n + 1 - \max(\lceil (n_1+1)/d_1\rceil, \ldots, \lceil (n_\ell+1)/d_\ell\rceil)$. Since the polynomials $f_1, \ldots, f_n$ have degree 1 in $\mathbb{K}[\mathscr{P}]$, we get

$$\mathrm{d_{wit}} \le \mathrm{reg}(\mathbb{K}[\mathscr{P}]) + 1.$$

Finally, notice that the unnormalized volume of $d\Delta_q \in \mathbb{R}^q$ is $d^q/q!$. Consequently, the unnormalized volume of $\mathscr{P}$ is $\prod_{i=1}^\ell d_i^{n_i}/n_i!$. Normalizing the volume amounts to multiplying this value by $n!$, which yields the formula for $\mathrm{vol}(\mathscr{P})$ and equals the multi-homogeneous Bézout number. The number of solutions (counted with multiplicity) is classically bounded by this value and hence $\delta \le \mathrm{vol}(\mathscr{P})$. □

Finally, we state a variant of Fröberg's conjecture (conjecture 2.43) in the sparse framework, leading to a notion of "sparse semi-regularity". It provides a bound on the witness degree of generic overdetermined sparse systems: this conjecture can be used to adjust the parameter D of Algorithm 5.16.

Conjecture 5.31. *Let $\mathscr{P} \subset \mathbb{R}^n$ be a normal lattice polytope, $(d_1, \ldots, d_s) \in \mathbb{N}^s$ be a sequence of integers with $s > n$. If $f_1, \ldots, f_s \in \mathbb{C}[\mathscr{P}]$ are generic homogeneous polynomials of respective degrees $(d_1, \ldots, d_s)$, then*

$$\mathsf{HS}_{\mathbb{C}[\mathscr{P}]/\langle f_1,\ldots,f_s\rangle}(z) = \left[\mathsf{HS}_{\mathscr{P}}(z)\prod_{i=1}^s(1-z^{d_i})\right]_+,$$

where $[\ ]_+$ means truncating the series expansion at its first nonpositive coefficient. Systems for which this equality holds are called semi-regular*. The witness degree of a semi-regular sequence is bounded above by the index of the first zero coefficient in the series expansion of $\mathsf{HS}_{\mathbb{C}[\mathscr{P}]/\langle f_1,\ldots,f_s\rangle}(z)$.*

Example 5.32. *Let $f_1, \ldots, f_7$ be a system of inhomogeneous bilinear polynomials in $\mathbb{K}[X_1, X_2, Y_1, Y_2, Y_3]$ with coefficients chosen at random. The support of each of these polynomials is included in $\mathscr{P} = \Delta_2 \times \Delta_3$, and therefore we see them as homogeneous elements of degree 1 in the polytopal algebra $\mathbb{K}[\mathscr{P}]$. Note that $\mathsf{HP}_{\mathscr{P}}(d) = \binom{d+2}{2}\binom{d+3}{3}$, and it is easy to check with a computer algebra software that*

$$\mathsf{HS}_{\mathscr{P}}(z) = \sum_{d=0}^{\infty} \mathsf{HP}_{\mathscr{P}}(d) z^d = \frac{3t^2 + 6t + 1}{(1-t)^6}.$$

If Conjecture 5.31 holds, then the ideal $\mathcal{I} \subset \mathbb{K}[\mathscr{P}]$ generated by $f_1, \ldots, f_7$ has Hilbert series

$$\mathsf{HS}_{\mathbb{K}[\mathscr{P}]/\mathcal{I}}(z) = \left[(1-z)(3z^2+6z+1)\right]_+ = \left[1 + 5z - 3z^2 - 3z^3\right]_+ = 1 + 5z$$

A computation performed with our Magma implementation of the sparse matrix-F_5 algorithm confirms that this is indeed the Hilbert series obtained.

5.6 Experimental results

In this section, we estimate the speed-up that one can expect for solving sparse systems or systems of Laurent polynomials via sparse Gröbner bases computations, compared to classical Gröbner bases algorithms. The same linear algebra routines are used in the compared implementations. Consequently, the speed-up reflects the differences between the characteristics (size, sparseness,...) of the matrices that have to be reduced.

Workstation. All experiments have been conducted on a 2.6GHz `IntelCore i7`. We compare in this section timings of our prototype implementation in C of sparse-MatrixF5 with the implementation of the F_5 algorithm in the FGb library. We report more detailed experimental results on a benchmarks' webpage [1], together with a preliminary implementation in Magma. In all these experiments, the base field $\mathbb{K}$ is the finite field $\mathbb{F}_{65521}$. All tests are done with overdetermined systems with one rational solution in $\mathbb{F}_{65521}^n$. The goal is to recover this solution. In that case, the Sparse-FGLM algorithm is not necessary since the sparse Gröbner basis describes explicitly the image of the solution by a monomial map. In several settings, we report the speed-up obtained with our prototype implementation.

Bilinear systems. In Table 5.33, we focus on overdetermined bilinear systems. For $(n_x, n_y, m) \in \mathbb{N}^3$, we generate a system of m polynomials with support $\Delta_{n_x} \times \Delta_{n_y}$ uniformly at random in the set of such systems which have at least one solution in $\mathbb{F}_{65521}^{n_x+n_y}$.

Systems of bidegree $(2,1)$. In Table 5.34, we report the performances on overdetermined systems with support $2\Delta_{n_x} \times \Delta_{n_y}$. Note that we obtain important speed-ups when $n_x < n_y$ (more than 19000 for $(n_x, n_y, m) = (3, 10, 24)$).

Fewnomial systems. In Table 5.35, we report performances on fewnomial systems. The complexity analysis in Section 5.4 do not apply to this context because the semigroup algebra in which we compute is not normal. However, the correctness of the algorithms still holds. The systems are generated as follows: for $(n, t, m) \in \mathbb{N}^3$ we pick t monomials of degree 2 in n variables uniformly at random and we generate a system of m polynomials with this support in $\mathbb{F}_{65521}[X_1, \ldots, X_n]$ with random coefficients such that there is at least one solution in $\mathbb{F}_{65521}^n$. The computations are done w.r.t. the semigroup generated by the t monomials. Note that for some specific instances, the speed-up factor can be as high as 16800 compared to classical Gröbner basis computations.

1. `http://www-polsys.lip6.fr/~jcf/Software/benchssparse.html`

(n_x, n_y, m)	sparse Matrix-F_5	F_5 (FGb)	Speed-up
(2,29,40)	0.12s	5.2s	43
(2,39,53)	0.49s	36.7s	74
(2,49,65)	1.53s	298.5s	195
(2,59,78)	4.63s	852.3s	184
(6,19,52)	1.10s	25.2s	22
(6,21,56)	2.13s	51.5s	24
(6,27,71)	7.07s	236.0s	33

Table 5.33 – Overdetermined bilinear systems in (n_x, n_y) variables and m equations

(n_x, n_y, m)	sparse Matrix-F_5	F_5 (FGb)	Speed-up
(1,34,36)	0.2s	395.1s	1975
(1,39,41)	0.45s	1641s	3646
(1,44,46)	0.75s	3168.8s	4225
(2,15,25)	0.09s	410.1s	4556
(2,17,27)	0.15s	1894.7s	12631
(2,19,30)	0.4s	5866.1s	14665
(3,10,24)	0.15s	2937.7s	19584
(10,4,50)	23.1s	1687.3s	73
(11,5,66)	155.1s	6265.8s	40
(12,6,86)	872.2s	27093.3s	31

Table 5.34 – Systems in (n_x, n_y) variables of bidegree $(2, 1)$ and m equations

(n, t, m)	sparse Matrix-F_5	F_5 (FGb)	Speed-up
(80,240,221)	0.10s	54.5s	545
(80, 240, 223)	0.08s	16.3s	203
(150, 450, 434)	0.24s	161.2s	671
(300, 900, 881)	4.56s	11301.0s	2478
(120, 240, 233)	0.01s	16.8s	16800
(40, 160, 128)	0.21s	5.93s	28
(60, 240, 211)	0.55s	29.04s	52

Table 5.35 – Fewnomials systems

Bibliography

[1] A. Albouy. The symmetric central configurations of four equal masses. *Contemporary Mathematics*, 198:131–135, 1996.

[2] H. Aref, P. K. Newton, M. A. Stremler, T. Tokieda, and D. L. Vainchtein. Vortex crystals. *Advances in Applied Mathematics*, 39, 2002.

[3] Gwenolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. Comparison between XL and Gröbner basis algorithms. In *ASIACRYPT 2004*, LNCS, pages 157–167, 2004.

[4] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université Paris 6, 2004.

[5] M. Bardet, J.-C Faugère, and B. Salvy. On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[6] Magali Bardet, Jean-Charles Faugere, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA*, volume 5, 2005.

[7] Daniel J Bates, Jonathan D Hauenstein, Andrew J Sommese, and Charles W Wampler. *Numerically solving polynomial systems with Bertini*, volume 25. SIAM, 2013.

[8] D. Bernstein. The number of roots of a system of equations. *Funct. Anal. and its Appli.*, 9(3):183–185, 1975.

[9] Anna M Bigatti. Computation of hilbert-poincaré series. *Journal of Pure and Applied Algebra*, 119(3):237–253, 1997.

[10] Richard P Brent. *Algorithms for matrix multiplication.* Stanford University, 1970.

[11] Michael Brickenstein. Slimgb: Gröbner bases with slim polynomials. *Revista Matemática Complutense*, 23(2):453–466, 2010.

[12] Markus P Brodmann and Rodney Y Sharp. *Local cohomology: an algebraic introduction with geometric applications.* Cambridge University Press, 1998.

[13] Winfried Bruns, Joseph Gubeladze, and Ngô Viêt Trung. Normal polytopes, triangulations, and Koszul algebras. *J. fur die reine und angewandte Mathematik*, 485:123–160, 1997.

[14] B. Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3-4):475 – 511, 2006. Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday).

[15] Laurent Busé and Jean-Pierre Jouanolou. A computational approach to the discriminant of homogeneous polynomials. arXiv reference : arXiv:1210.4697.

[16] E. Campbell and D. Wehlau. *Modular invariant theory*, volume 139. Springerverlag Berlin Heidelberg, 2011.

[17] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. *Applied Algebra, Algebraic Algorithms and Error-*, 1993.

[18] J. F. Canny, E. Kaltofen, and L. Yagati. Solving systems of nonlinear polynomial equations faster. In *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*, ISSAC '89, pages 121–128, New York, NY, USA, 1989. ACM.

[19] J.F. Canny. *Complexity of Robot Motion Planning*. PhD thesis, Massachusetts Institute of Technology, 1988.

[20] John F. Canny and Ioannis Z. Emiris. An efficient algorithm for the sparse mixed resultant. In *Applied Algebra, Algebraic Algo. and Error-correcting Codes*, pages 89–104. Springer, 1993.

[21] John F. Canny and Ioannis Z. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47:417–451, 1999.

[22] C. Chevalley. Invariants of finite groups generated by reflections. *American Journal of Mathematics*, 77(4):778–782, 1955.

[23] A. Colin. Solving a system of algebraic equations with symmetries. *J. Pure Appl. Algebra*, 117/118:195–215, 1997. Algorithms for algebra (Eindhoven, 1996).

[24] Stéphane Collart, Michael Kalkbrener, and Daniel Mall. Converting bases with the gröbner walk. *Journal of Symbolic Computation*, 24(3):465–469, 1997.

[25] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[26] David A Cox, John B Little, and Henry K Schenck. *Toric varieties*. AMS, 2011.

[27] H. Derksen and G. Kemper. *Computational Invariant Theory*. Encyclopaedia of Mathematical Sciences. Springer, 2002.

[28] T. Dirksen and H. Aref. Close pairs of relative equilibria for identical point vortices. *Phys. Fluids*, 23, 2011.

[29] Eugene Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *CR Acad. Sci. Paris*, 254:616–618, 1962.

[30] D. Eisenbud. *Commutative Algebra with a view toward algebraic geometry*, volume 150. Springer Verlag, 1995.

[31] I. Emiris and J.F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *Journal of Symbolic Computation*, 20(2):117–149, 1995.

[32] Ioannis Z Emiris. Toric resultants and applications to geometric modelling. In *Solving polynomial equations*, pages 269–300. Springer, 2005.

[33] Ioannis Z Emiris and Victor Y Pan. Symbolic and numeric methods for exploiting structure in constructing resultant matrices. *J. of Symbolic Computation*, 33(4):393–413, 2002.

[34] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[35] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[36] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *Journal Of Symbolic Computation*, 46(4):406–437, 2011. Available online 4 November 2010.

[37] J.-C. Faugère, M. Safey El Din, and T. Verron. On the complexity of computing gröbner bases for quasi-homogeneous systems. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, New York, NY, USA, 2013. ACM.

[38] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Sub-cubic change of ordering for gröbner basis. a probabilistic approach. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, New York, NY, USA, 2014. ACM. accepted.

[39] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[40] J.-C. Faugère, M. Hering, and J. Phan. The membrane inclusions curvature equations. *Advances in Applied Mathematics*, 31(4):643–658, June 2003.

[41] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 151–158, New York, NY, USA, 2009. ACM.

[42] J.-C. Faugère, P.-J Spaenlehauer, and J. Svartz. Sparse gröbner bases: the unmixed case. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, New York, NY, USA, 2014. ACM. accepted.

[43] J.-C. Faugère and J. Svartz. Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 170–178, New York, NY, USA, 2012. ACM.

[44] J.-C. Faugère and J. Svartz. Groebner bases of ideals invariant under a commutative group : the non-modular case. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, New York, NY, USA, 2013. ACM.

[45] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. On the complexity of the generalized minrank problem. *Journal of Symbolic Computation*, 55:30–58, 2013.

[46] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[47] P. Fleischmann. The noether bound in invariant theory of finite groups. *Advances in Mathematics*, 156(1):23–32, 2000.

[48] J. Fogarty. On noether's bound for polynomial invariants of a finite group. *Electronic Research Announcements of the American Mathematical Society*, 7(2):5–7, 2001.

[49] William Fulton. *Introduction to Toric Varieties*. Princeton University Press, 1993.

[50] François Le Gall. Power of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, New York, NY, USA, 2014. ACM. accepted.

[51] K. Gatermann. Symbolic solution polynomial equation systems with symmetry. In *Proceedings of the international symposium on Symbolic and algebraic computation*, ISSAC '90, pages 112–119, New York, NY, USA, 1990. ACM.

[52] Alessandro Giovini, Teo Mora, Gianfranco Niesi, Lorenzo Robbiano, and Carlo Traverso. "One sugar cube, please" or selection strategies in the Buchberger algorithm. In *ISSAC '91*, pages 49–54. ACM, 1991.

[53] M. Giusti, G. Lecerf, and B. Salvy. A gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[54] H. von Helmholtz. Über Integrale der hydrodynamischen Gleichungen, welche den Wirbelbewegungen entsprechen. *Reine Angew. Math.*, 55:25–55, 1858. English translation by Tait, P.G., 1867. On integrals of the hydrodynamical equations, which express vortex-motion. Philos. Mag. 33(4), 485–512.

[55] D. Hilbert. *Theory of algebraic invariants*. Cambridge University Press, 1993.

[56] M. Hochster. Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes. *The Annals of Mathematics*, 96(2):318–337, 1972.

[57] M. Hochster and J. Eagon. Cohen-macaulay rings, invariant theory, and the generic perfection of determinantal loci. *American Journal of Mathematics*, 93(4):1020–1058, 1971.

[58] J. Hoffstein, J. Pipher, and J.H. Silverman. Ntru: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin, 1998.

[59] Evelyne Hubert and Irina A Kogan. Rational invariants of a group action. construction and rewriting. *Journal of Symbolic Computation*, 42(1):203–217, 2007.

[60] Evelyne Hubert and Irina A Kogan. Smooth and algebraic invariants of a group action: local and global constructions. *Foundations of Computational Mathematics*, 7(4):455–493, 2007.

[61] Evelyne Hubert and George Labahn. Rational Invariants of Finite Abelian Groups. available online: `http://hal.inria.fr/hal-00921905`, December 2013.

[62] Evelyne Hubert and George Labahn. Scaling invariants and symmetry reduction of dynamical systems. *Foundations of Computational Mathematics*, 13(4):479–516, 2013.

[63] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In Komei Fukuda, Joris Hoeven, Michael Joswig, and Nobuki Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[64] Irving Kaplansky. *Commutative rings*. University of Chicago Press Chicago, 1974.

[65] D. Karagueuzian and P. Symonds. The module structure of a group action on a polynomial ring: a finiteness theorem. *Journal of the American Mathematical Society*, 20(4):931–967, 2007.

[66] Lord Kelvin. On vortex atoms. *Proceedings of the Royal Society of Edinburgh*, VI:94–105, 1867. Reprinted in Phil. Mag. Vol. XXXIV, 1867, pp. 15-24.

[67] G. Kemper and A. Steel. Some algorithms in invariant theory of finite groups. In *Computational Methods for Representations of Groups and Algebras*, pages 267–285. Springer, 1999.

[68] M. Kreuzer and L. Robbiano. *Computational commutative algebra 2*, volume 2. Springer, 2005.

[69] Julian D Laderman. A noncommutative algorithm for multiplying 3× 3 matrices using 23 multiplications. *Bulletin of the American Mathematical Society*, 82(1):126–128, 1976.

[70] Serge Lang. *Introduction to algebraic geometry*, volume 109. Addison-Wesley Reading, Mass., 1972.

[71] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer Algebra, EUROCAL'83*, volume 162 of *LNCS*, pages 146–156. Springer, 1983.

[72] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Appl. Math.*, 33(1-3):147–160, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[73] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 15:117–132, 1992.

[74] R. Lebreton and É. Schost. Algorithms for the universal decomposition algebra. In *ISSAC '12: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, ISSAC '12, pages 234–241, New York, NY, USA, 2012. ACM. accepted.

[75] F.S. Macaulay. Some formulæ in elimination. *Proceedings of the London Mathematical Society*, s1-35(1):3–38, 1902.

[76] I.G. MacDonald. Polynomials associated with finite cell-complexes. *J. London Math. Soc.*, 4:181–192, 1971.

[77] V.V. Meleshko and H. Aref. A bibliography of vortex dynamics 1858-1956. *Adv. Appl. Mech.*, 41(106), 2007.

[78] E. Miller and B. Sturmfels. *Combinatorial commutative algebra*, volume 227. Springer Verlag, 2005.

[79] J.L. Miller. Effective algorithms for intrinsically computing sagbi-groebner bases in a polynomial ring over a field. *LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES*, pages 421–433, 1998.

[80] E. Noether. Der endlichkeitssatz der invarianten endlicher gruppen. *Mathematische Annalen*, 77(1):89–92, 1915.

[81] T. Oda. *Convex bodies and algebraic geometry*. Springer, 1988.

[82] Victor Y Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12):97–138, 1996.

[83] Victor Y Pan, Brian Murphy, Rhys Eric Rosholt, Guoliang Qian, and Yuqing Tang. Real root-finding. In *Proceedings of the 2007 international workshop on Symbolic-numeric computation*, pages 161–169. ACM, 2007.

[84] Victor Y Pan and Ai-Long Zheng. New progress in real and complex polynomial root-finding. *Computers & Mathematics with Applications*, 61(5):1305–1334, 2011.

[85] Keith Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590, 2010.

[86] Paul Pedersen and Bernd Sturmfels. Mixed monomial bases. In *Algorithms in algebraic geometry and applications*, pages 307–316. Springer, 1995.

[87] A. Poteaux and É. Schost. Modular composition modulo triangular sets and applications. *computational complexity*, pages 1–54, 2010.

[88] L. Robbiano and M. Sweedler. Subalgebra bases. *Commutative algebra*, pages 61–87, 1990.

[89] JC Rosales and Pedro A Garcia-Sanchez. On Cohen-Macaulay and Gorenstein simplicial affine semigroups. *Proceedings of the Edinburgh Mathematical Society*, 41(3):517–538, 1998.

[90] J.-P. Serre. Groupes finis d'automorphismes d'anneaux locaux réguliers. In *Colloque d'Algebre (Paris, 1967), Exp*, volume 8, 1968.

[91] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag New York, 1977.

[92] G.C. Shephard and J.A. Todd. Finite unitary reflection groups. *Canad. J. Math*, 6(2):274–301, 1954.

[93] P.-J. Spaenlehauer. *Solving multi-homogeneous and determinantal systems. Algorithms - Complexity - Applications.* PhD thesis, Université Paris 6, 2012.

[94] R. P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (new series)*, 1:475–511, 1979.

[95] Richard P Stanley. Decompositions of rational convex polytopes. *Ann. Discrete Math. v6*, pages 333–342, 1980.

[96] S. Steidel. Gröbner bases of symmetric ideals. *Journal of Symbolic Computation*, 54(0):72 – 86, 2013.

[97] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, University of Waterloo, 2000.

[98] Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.

[99] Adam Strzeboński and Elias P. Tsigaridas. Univariate real root isolation in multiple extension fields. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 343–350, New York, NY, USA, 2012. ACM.

[100] B. Sturmfels. *Algorithms in Invariant Theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.

[101] Bernd Sturmfels. Sparse elimination theory. In *Proc. Comp. Algebraic Geom. and Commut. Algebra*, pages 377–396. Cambridge Univ. Press, 1991.

[102] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8. AMS, 1996.

[103] P. Symonds. On the castelnuovo-mumford regularity of the cohomology ring of a group. *Journal of the American Mathematical Society*, 23(4):1159–1173, 2010.

[104] N.M. Thiéry. Computing minimal generating sets of invariant rings of permutation groups with sagbi-grobner basis. *Discrete Mathematics and Theoretical Computer Science*, 315:328, 2001.

[105] Jan Verschelde. Algorithm 795: Phcpack: A general-purpose solver for polynomial systems by homotopy continuation. *ACM Transactions on Mathematical Software (TOMS)*, 25(2):251–276, 1999.

[106] Jan Verschelde, Pierre Verlinden, and Ronald Cools. Homotopies exploiting newton polytopes for solving sparse polynomial systems. *SIAM J. on Numerical Analysis*, 31(3):915–930, 1994.

[107] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, 2013.

[108] Virginia Vassilevska Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proc. of STOC'12*, pages 887–898. ACM, 2012.