THÈSE de DOCTORAT de l'UNIVERSITÉ PARIS VI
Spécialité :
INFORMATIQUE

présentée par :

Philippe AUBRY

pour obtenir le grade de DOCTEUR de l'UNIVERSITÉ PARIS VI

Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.

Soutenue le mercredi 13 janvier 1999

Composition du jury :

M. Manuel BRONSTEIN	Examinateur
M. André GALLIGO	Rapporteur
M. Daniel LAZARD	Directeur de thèse
M. Jean-François PERROT	Président
M. Dongming WANG	Examinateur
M. Paul ZIMMERMANN	Rapporteur

Introduction

Le calcul formel (ou symbolique) est un domaine qui se situe à la charnière des mathématiques et de l'informatique. On cherche à résoudre algébriquement des problèmes d'essence mathématique par des moyens informatiques. L'intérêt est de calculer de manière exacte en manipulant des symboles qui ont une portée générale. Le résultat d'un calcul pourra être alors directement exploité avec des valeurs particulières pour ces symboles, contrairement à des techniques numériques où il faudrait recommencer tout le calcul à chaque changement de valeur. Cette exactitude a un coût. Pour la résolution de systèmes d'équations polynomiales, elle permet cependant d'obtenir des informations globales sur l'ensemble des zéros du système alors que l'on étudie généralement des propriétés locales avec des techniques d'analyse numérique. De plus, il ne faut pas oublier que le calcul formel est une discipline plus jeune que le calcul numérique. Néanmoins il paraît primordial pour son développement que des réalisations pratiques efficaces soient élaborées. Le travail présenté ici tente de contribuer à cet objectif, qui demande un investissement équilibré sur les aspects théoriques et les soucis d'implantation du calcul formel.

L'axe de cette thèse est la résolution pratique de systèmes d'équations polynomiales. Mais les liens entre différentes parties des mathématiques sont fréquents et nos résultats nous ont aussi mené à développer notre travail en théorie de Galois effective. Nous avons obtenu des résultats d'ordre mathématique exploitables algorithmiquement et à des fins d'optimisation. De plus, nos implantations réalisées dans le cadre le plus général montrent que notre approche à l'aide d'*ensembles triangulaires de polynômes* est particulièrement performante dans le domaine de la théorie de Galois par rapport à des techniques plus éprouvées et mieux optimisées en machine telles que celles fondées sur les *bases de Gröbner*.

En calcul formel, la résolution de systèmes d'équations polynomiales est un problème fondamental, dans le sens où c'est la source d'applications variées et que sa complexité le rend extrêmement difficile. Les applications sont en effet multiples. Nous en détaillerons certains aspects par la suite, mais en voici déjà un aperçu :

- problème des n-corps en mécanique céleste,
- cinématique des robots,
- compression d'images,
- preuve automatique de théorèmes,
- calcul de groupes de Galois et détermination du corps de décomposition d'un polynôme en théorie de Galois.

Les techniques symboliques de résolution de systèmes polynomiaux font intervenir des algorithmes qui sont très souvent de complexité au moins exponentielle. On doit alors porter une grande attention à la représentation des données et à l'implantation pour rendre les calculs réalisables. Les meilleurs algorithmes théoriques permettent de savoir ce qui est possible mais sont parfois plus lents que les meilleurs algorithmes *pratiques*, dont la complexité n'est pas toujours connue. De plus, dans le cas où le nombre de solutions d'un système n'est pas fini, se présente le problème de donner une description de l'ensemble de ces solutions.

Un système d'équations polynomiales en n variables $x_1, x_2, \ldots, x_n$ à coefficients dans un corps k correspond à un ensemble F de polynômes de $k[x_1, \ldots, x_n]$ dont on cherche les zéros communs. La méthode de résolution la plus répandue consiste à remplacer F par un système appelé base de Gröbner, qui a des propriétés particulières permettant d'obtenir des informations d'ordre algébrique importantes avec les algorithmes appropriés. Elle est développée depuis les travaux de Buchberger [Buc65] et a fait l'objet d'implantations de plus en plus efficaces. Cependant, si le système de départ est formé de polynômes de degré maximal d, alors la base de Gröbner obtenue peut contenir un nombre de polynômes de l'ordre de $d^{2^{O(n)}}$.

Pour des raisons d'efficacité et de lisibilité des solutions, on a intérêt à scinder le problème lorsque c'est possible. On calcule alors une décomposition du système de départ en plusieurs systèmes. Cette approche a été utilisée sur les bases de Gröbner en factorisant des polynômes en cours de calcul. Une autre possibilité, étudiée principalement depuis [Wu87], consiste à effectuer une décomposition à l'aide d'ensembles triangulaires de polynômes. En supposant les variables de F ordonnées de sorte que $x_1 < x_2 < \ldots < x_n$ (on peut s'y ramener par renumérotation), un ensemble $T \subseteq k[x_1, \ldots, x_n]$ est triangulaire si pour toute variable x_i il existe au plus un polynôme p de T dont x_i est la plus grande variable.

Le nombre réduit des éléments d'un ensemble triangulaire de polynômes est un facteur positif. Ces ensembles permettent de lire facilement des propriétés géométriques. Il est néanmoins préférable de leur imposer des conditions supplémentaires pour optimiser cette lisibilité et leur fournir des caractéristiques géométriques intrinsèques satisfaisantes. Par exemple, le degré de la variété du système peut être surestimé. L'ajout de propriétés supplémentaires permettra alors de lire directement ce degré, notamment en rendant les polynômes square-free dans des tours d'extensions. Différents algorithmes de décomposition basés sur l'utilisation d'ensembles triangulaires ont été présentés depuis [Wu87]. Les conditions imposées aux ensembles triangulaires varient d'une méthode à l'autre. Il en va de même concernant la relation entre les zéros communs des polynômes de départ et les ensembles triangulaires calculés. Il est donc difficile de comparer les possibilités pratiques de ces différents algorithmes. Nous avons réalisé en collaboration avec M. Moreno Maza un premier travail de comparaison expérimentale pour quatre d'entre elles. On y constate en particulier l'hétérogénéité du sens de résolution. Ce travail est exposé dans le chapitre 7.

La complexité des méthodes «triangulaires» pourrait être simplement exponentielle selon [GM90]. Cela justifie leur développement si on compare au comportement doublement exponentiel des bases de Gröbner dans le pire des cas. Malheureusement, ces méthodes ne bénéficient pas encore d'implantations aussi optimisées que celles fondées sur les bases de Gröbner. Nous verrons pourtant plus loin que les implantations que nous avons réalisées dans le système généraliste de calcul formel AXIOM basé sur le langage LISP peuvent dans certains cas, être performantes par rapport à des implantations adaptées pour le calcul de bases de Gröbner et écrites en C.

Nos résultats sont prometteurs même s'il reste beaucoup à faire pour calculer directement des décompositions triangulaires dans des problèmes difficiles. Le passage de nos implantations dans un langage plus efficace pourrait donc être un prolongement naturel du travail présenté ici. Actuellement les techniques de triangulation offrent tout de même une complémentarité au calcul de bases de Gröbner. En effet, une décomposition triangulaire fournit généralement plus d'informations géométriques sur l'ensemble des zéros du système que la seule base de Gröbner. Mais dans les cas difficiles, le seul moyen d'obtenir une telle décomposition est de calculer d'abord une base de Gröbner du système à l'aide d'un logiciel efficace, et d'appliquer ensuite une méthode triangulaire sur cette base. De manière similaire, lorsque le système a un nombre fini de solutions, le calcul de Représentation Univariée Rationnelle [Rou96] est plus facile à partir d'une décomposition triangulaire du système qu'à partir d'une base de Gröbner.

Au cours de cette thèse, notre travail s'est développé dans plusieurs directions. La subdivision ci-dessous ne signifie pas du tout un cloisonnement car ces différents aspects sont en interaction :

(i) théorique : un travail de base mathématique est nécessaire pour comprendre, optimiser et développer des algorithmes. La découverte de nouvelles structures et propriétés permet d'envisager de nouveaux algorithmes. Le chapitre 6 donne une illustration de ce phénomène en théorie de Galois. On peut aussi mentionner le travail entamé par F. Rouillier (INRIA Nancy) et M. Safey (LIP6) visant à résoudre les problèmes de décision sur les variétés algébriques réelles et qui utilise certains résultats mathématiques du chapitre 4.

(ii) algorithmique : les avancées sont souvent obtenues à partir du travail mathématique ci-dessus. Nos algorithmes permettent en particulier d'améliorer l'efficacité de méthodes de décomposition triangulaire existantes et de proposer de nouvelles spécifications.

(iii) implantation et expérimentation : on doit prêter attention à disposer de structures de données adaptées. L'implantation des fonctions de base sur les polynômes est primordiale pour l'efficacité. L'implantation de domaines correspondant à une hiérarchie de notions d'ensembles triangulaires s'inscrit dans un travail de programmation objet. La partie de comparaison expérimentale demande beaucoup d'investissement; elle induit une réflexion sur le comportement des implantations qui font évoluer celles-ci. Nous avons implanté une méthode de décomposition triangulaire proposée par D. Wang [Wan93b] et la méthode de décomposition de M. Kalkbrener [Kal93] [Kal95]. Nous avons optimisé cette dernière grâce au travail théorique mené sur la notion d'ensemble triangulaire.

(iv) applications : c'est d'une part la recherche et l'étude de systèmes qui correspondent à des problèmes autres que des exemples-tests. L'autre aspect concerne l'intérêt de nos résultats pour des questions indépendantes du problème de la résolution de systèmes algébriques. Jusqu'à maintenant, l'utilisation de la notion d'ensemble triangulaire pour

> d'autres buts que la résolution de systèmes, s'est essentiellement limitée à la démonstration automatique de théorèmes en géométrie. Nous ouvrons de nouveaux horizons puisque l'apport de notre *technologie* permet des avancées en théorie de Galois.

On peut dégager trois parties dans cet ouvrage. La première présente les notions, les résultats mathématiques et les algorithmes permettant la résolution de systèmes algébriques par des ensembles triangulaires de polynômes (chapitres 1 à 5). Dans la deuxième partie, composée de l'unique chapitre 6, sont développés des outils en théorie de Galois effective. La troisième présente des travaux d'implantation et d'expérimentation et quelques applications de nos implantations (chapitres 7 et 8). Le document est structuré comme suit. Précisons que chaque chapitre est précédé d'un résumé auquel on se reportera pour plus de détails.

Le premier chapitre présente le problème de la résolution de systèmes algébriques. Le second chapitre met en place les définitions et propriétés de base qui seront utilisés par la suite.

On s'intéresse dans le chapitre 3 aux anneaux de polynômes en une variable. Après quelques faits connus, nous introduisons la notion nouvelle d'idéal *quasi-monogène régulier* dans ces anneaux et en présenterons les propriétés principales qui nous fournissent l'essence de certaines preuves concernant les ensembles triangulaires. La dernière section traite du calcul de pgcd de polynômes lorsque l'anneau de base est un produit de corps. On y présente le principe dynamique de calcul de pgcd qui est utilisé par nos algorithmes du chapitre 5.

Le chapitre 4 étudie les propriétés des ensembles triangulaires. Il prolonge le travail mené en collaboration avec M. Moreno Maza et D. Lazard dans [ALM99] en faisant apparaître plusieurs résultats nouveaux. Nous présentons dans le théorème 4.1.4 un nouveau résultat de structure sur l'*idéal saturé* d'un ensemble triangulaire. On s'intéresse ensuite à quelques types particuliers d'ensembles triangulaires. Le concept d'*ensemble caractéristique* de Ritt et de Wu est examiné dans la section 4.2. Nous introduisons dans la section 4.3 une définition simple dont nous montrons l'équivalence avec le concept de *chaîne régulière* de M. Kalkbrener. Puis nous dégageons la structure de produit de corps associée dans laquelle travaillent les algorithmes du chapitre 5. Une synthèse des relations entre ces différentes théories est exprimée dans le théorème d'équivalence de la section 4.6. Finalement, la section 4.7 contribue au rapprochement avec la théorie des bases de Gröbner.

Le chapitre 5 présente des algorithmes qui permettent de calculer des décompositions de variétés algébriques en ensembles triangulaires. À la base de ce travail se trouvent des algorithmes proposés par M. Kalkbrener dans [Kal93]. Nous en construisons d'autres qui permettent de décomposer une variété avec des spécifications plus fortes. Nous avons implanté ces algorithmes en AXIOM. Les calculs de pgcd modulo un ensemble triangulaire interviennent de façon intensive pour de telles décompositions comme dans la méthode de décomposition triangulaire de D. Lazard [Laz91a] [Mor97]. Nous sommes passés pour plus d'efficacité de l'algorithme de type euclidien présenté par M. Kalkbrener à un algorithme basé sur la méthode des sous-résultants, puis nous avons adapté plus récemment les améliorations apportées par L. Ducos à cet algorithme des sous-résultants [Duc96] [Duc97] pour les utiliser avec nos ensembles triangulaires.

La deuxième partie de cette thèse est uniquement composée du chapitre 6 qui peut se lire de façon indépendante. Elle traite de la théorie de Galois algébrique constructive et nécessite donc l'introduction de la terminologie nécessaire pour travailler dans ce domaine. La lecture de cette partie n'est pas nécessaire pour la compréhension du reste du document car son objet principal n'est pas la résolution de systèmes polynomiaux. On y retrouvera néanmoins certains liens avec ce problème. Ce chapitre reprend l'article [AV98] (en anglais) réalisé en collaboration avec A. Valibouze (LIP6) et présenté à la conférence internationale MEGA'98. Nos résultats passent par une nouvelle approche qui développe des liens avec l'algèbre commutative, qui se limitaient jusqu'à maintenant aux notions d'idéal des relations et d'idéal des relations symétriques. Nous y précisons la structure d'idéaux plus généraux qui interviennent en théorie de Galois et proposons de nouveaux algorithmes qui permettent de calculer de manière algébrique les résolvantes relatives ainsi que la base de Gröbner lexicographique d'un tel idéal, qui a pour particularité d'être aussi un ensemble triangulaire.

La dernière partie du document commence avec le chapitre 7, rédigé en anglais, qui présente un travail de comparaison expérimentale de quatre méthodes de décomposition de systèmes polynomiaux à l'aide d'ensembles triangulaires que nous avons réalisé avec M. Moreno Maza [AM99]. Ces quatres méthodes ont été implantées dans le langage orienté-objet AXIOM, dans un cadre commun pour partager les mêmes routines de base et permettre une comparaison significative. Le travail de conception mené à cette occasion est illustré dans la figure 7.1 p. 115, qui présente les catégories et les domaines implantés correspondant aux propriétés des différentes méthodes étudiées. La complexité des algorithmes de décomposition triangulaires n'est pas encore connue et les considérations de complexité ne sont de toutes façons pas suffisantes pour le développement du calcul formel. Il est par conséquent important d'évaluer pratiquement les possibilités des algorithmes au niveau pratique pour des exemples-tests connus. Mais il faut aussi les évaluer avec des exemples provenant de la physique, de l'analyse numérique, du traitement du signal, ...

Le chapitre 8 illustre enfin l'intérêt de nos implantations avec quelques applications. Nos nouveaux algorithmes permettent de résoudre de façon performante des problèmes de théorie de Galois algébrique constructive. D'autre part, les méthodes de décomposition triangulaire complètent les bases de Gröbner dans des problèmes de compression d'images. Enfin, nos implantations peuvent être utilisées efficacement pour résoudre certains systèmes provenant du problème des n-corps en mécanique céleste.

On trouvera à la fin de la thèse deux annexes et un index. La première annexe est composée de rappels d'algèbre commutative qui sont utiles pour la compréhension de résultats du chapitre 4. La seconde rappelle quelques éléments de base sur la notion de base de Gröbner.

Table des matières

Chapitre 1

Variétés et systèmes algébriques

Résumé

Nous rappelons dans ce court chapitre quelques notions et propriétés afférentes aux variétés algébriques. Nous précisons ensuite ce qu'on peut entendre par résoudre un système d'équations polynomiales. On peut en effet distinguer la résolution au sens géométrique, où l'on ne s'intéresse qu'à l'ensemble des solutions du système, de la résolution au sens algébrique où l'on désire conserver la stucture algébrique de l'idéal engendré par les polynômes du système. Les méthodes de résolution basées sur les ensembles triangulaires de polynômes (définis dans le chapitre 2) se limitent à l'aspect géométrique du problème.

1.1 Variétés algébriques

Dans tout l'ouvrage, on considère un corps commutatif k et une extension K du corps k. Soit n un entier strictement positif et $x_1 < \ldots < x_n$ des variables, ordonnées algébriquement indépendantes sur k. On note $[1, n]$ l'ensembles des entiers compris entre 1 et n. Pour tout $i \in [1, n]$ on pose $\mathbf{P}_i = k[x_1, \ldots, x_i]$. Par convention $\mathbf{P}_0$ désigne le corps k.

On désignera par A un anneau commutatif unitaire. Pour une partie E de A on désigne par $\langle E \rangle_A$ l'idéal engendré par E dans A. Pour $E = \{a_1, \ldots, a_n\}$ on note $\langle a_1, \ldots, a_n \rangle_A$. Lorsqu'aucune confusion n'est à craindre on écrit simplement $\langle E \rangle$. Si E est vide, on pose par convention $\langle \emptyset \rangle = \{0\}$. Un idéal I de A est dit *propre* s'il est distinct de A. Dans tout le document le radical d'un idéal I est noté $\sqrt{I}$.

Soit F un sous-ensemble de $\mathbf{P}_n$. On appelle *zéro* de F tout élément z de K^n tel que $f(z) = 0$ pour tout $f \in F$. On note alors $\mathbf{V}_K(F)$ l'ensemble des zéros de F. Pour un polynôme p de $\mathbf{P}_n$ et une partie V de K^n, on dira que p s'annule sur V si $p(z) = 0$ pour tout $z \in V$.

Définition 1.1.1 *Une partie V de K^n est une k-*variété *s'il existe une partie F de $\mathbf{P}_n$ tel que $V = \mathbf{V}_K(F)$. Dans la suite, si aucune confusion n'est à craindre on dira simplement* variété *pour une k-variété et on notera $\mathbf{V}(F)$ au lieu de $\mathbf{V}_K(F)$.*

Remarque 1.1.2 Il est clair que tout zéro de $F \subset \mathbf{P}_n$ est un zéro de l'idéal engendré par F dans $\mathbf{P}_n$ et vice-versa, d'où l'égalité suivante :

$$\mathbf{V}_K(F) \quad = \quad \mathbf{V}_K(\langle F \rangle) \; .$$

Définition 1.1.3 *Soit V une k-variété de K^n. On appelle* idéal associé à V *sur k l'idéal de $\mathbf{P}_n$ composé des polynômes qui s'annulent sur V. On le note $\mathbf{Id}_k(V)$ ou $\mathbf{Id}(V)$ si aucune confusion n'est à craindre.*

Rappelons quelques propriétés classiques.

Proposition 1.1.4 *Soit I et J deux idéaux de $\mathbf{P}_n$. Soit V et W deux sous-ensembles de K^n. On a alors les propriétés suivantes:*

(i) $I \subseteq \mathbf{Id}_k(\mathbf{V}_K(I))$

(ii) $V \subseteq \mathbf{V}_K(\mathbf{Id}_k(V))$

(iii) $I \subseteq J \;\Rightarrow\; \mathbf{V}(J) \subseteq \mathbf{V}(I)$

(iv) $V \subseteq W \;\Rightarrow\; \mathbf{Id}_k(W) \subseteq \mathbf{Id}_k(V)$

(v) $\mathbf{V}(I) \cup \mathbf{V}(J) \;=\; \mathbf{V}(I \cap J) \;=\; \mathbf{V}(I\,.\,J)$

(vi) $\mathbf{V}(I) \cap \mathbf{V}(J) \;=\; \mathbf{V}(I + J)$

(vii) $\mathbf{Id}_k(V \cap W) \;=\; \mathbf{Id}_k(V) + \mathbf{Id}_k(W)$

(viii) $\mathbf{Id}_k(V \cup W) \;=\; \mathbf{Id}_k(V) \cap \mathbf{Id}_k(W)$.

Preuve. Les quatre premiers points se déduisent clairement des définitions. Vérifions (v). Les inclusions

$$I\,.\,J \;\subseteq\; I \cap J \;\subseteq\; I\,,\,J$$

entraînent

$$\mathbf{V}(I) \,\cup\, \mathbf{V}(J) \;\subseteq\; \mathbf{V}(I \bigcap J) \;\subseteq\; \mathbf{V}(I\,.\,J)\;.$$

Réciproquement, soit ζ un élément de K^n tel que $\zeta \notin \mathbf{V}(I) \,\cup\, \mathbf{V}(J)$. Il existe $p \in I$ tel que $p(\zeta) \neq 0$ et $q \in J$ tel que $q(\zeta) \neq 0$. Par conséquent l'élément pq de IJ ne s'annule pas sur ζ. Les égalités suivantes s'obtiennent facilement de manière similaire. □

Proposition 1.1.5 *Si V et W sont deux k-variétés de K^n alors*

(i) $\mathbf{V}_K(\mathbf{Id}_k(V)) \;=\; V$,

(ii) $V \;\subseteq\; W \quad\Longleftrightarrow\quad \mathbf{Id}_k(W) \;\subseteq\; \mathbf{Id}_k(V)$.

Preuve. Il existe $F \subseteq \mathbf{P}_n$ tel que $V = \mathbf{V}_K(\langle F \rangle)$. On a clairement $\langle F \rangle \subseteq \mathbf{Id}_k(V)$ d'où $\mathbf{V}_K(\mathbf{Id}_k(V)) \subseteq V$ par le point (iii) de la proposition 1.1.4. De plus, cette même proposition affirme l'inclusion réciproque. Pour (ii), l'implication directe est encore donnée dans la proposition 1.1.4. La réciproque résulte de (i) après passage aux variétés associées. □

Ci-dessous, nous présentons rapidement la notion de clôture de Zariski pour des parties de K^n. Elle apparaîtra dans le théorème 2.2.21 qui précise la relation entre deux notions associées aux ensembles triangulaires. Mentionnons que la notion de clôture intervient naturellement pour la projection de variétés algébriques et l'étude des *idéaux d'élimination*. On pourra voir à ce sujet le chapitre 3 de [CLO92].

Définition 1.1.6 *Soit W une partie de K^n. La* clôture de Zariski *de W sur k, notée $\overline{W}$, est la plus petite k-variété qui contient W.*

Proposition 1.1.7 *Soit W une partie de K^n. On a $\overline{W} = \mathbf{V}_K(\mathbf{Id}_k(W))$.*

Preuve. Soit V une variété de K^n telle que $W \subset V$. On en déduit $\mathbf{Id}_k(V) \subseteq \mathbf{Id}_k(W)$ puis $\mathbf{V}_K(\mathbf{Id}_k(W)) \subseteq \mathbf{V}_K(\mathbf{Id}_k(V))$. On a ainsi $\mathbf{V}_K(\mathbf{Id}_k(W)) \subseteq V$ d'après la proposition 1.1.5. L'assertion en résulte immédiatement. □

1.2 Résolution de systèmes algébriques

On constate avec l'égalité (i) de la proposition 1.1.5 que la connaissance de l'idéal associé à une variété permet de retrouver celle-ci. Par contre, il n'est pas possible de reconstruire un idéal seulement à partir de la donnée de sa variété associée. En effet, prenons par exemple l'idéal $I = \langle x_1^2, x_2^3 \rangle$ dans $\mathbf{P}_2$. Il est clair que sa variété associé est $V = \{\,(0,0)\,\}$. Malheureusement, la seule connaissance de cette variété n'est pas suffisante pour en déduire I. On peut aisément vérifier que $\mathbf{Id}_k(V) = \langle x_1, x_2 \rangle$, qui contient I comme le précise le point (i) de la proposition 1.1.4, mais l'inclusion est stricte. Ce phénomène provient du fait qu'il existe une multitude d'idéaux dont V est la variété, comme on le voit simplement avec les idéaux du type $\langle x_1^l, x_2^m \rangle$. Cependant, le théorème classique des zéros de Hilbert (Nullstellensatz) ci-dessous précise le lien entre un idéal I de $\mathbf{P}_n$ et l'idéal des polynômes qui s'annulent sur les zéros de I dans le cas où l'extension K est algébriquement close. On pourra consulter la section 16.5 de [vdW91] pour la preuve.

Théorème 1.2.1 (Nullstellensatz fort) *Soit k un corps et K une extension algébriquement close de k. Si I est un idéal de $\mathbf{P}_n$ alors*

$$\mathbf{Id}_k(\mathbf{V}_K(I)) = \sqrt{I} \; .$$

Le Nullstellensatz permet, pour K algébriquement clos, d'établir une bijection entre l'ensemble des k-variétés de K^n et l'ensemble des idéaux radicaux de $\mathbf{P}_n$ avec les opérations **Id** et **V**. Nous supposerons désormais que K est algébriquement clos, la situation classique consistant à prendre pour K le corps des complexes et $k = \mathbb{Q}$. Un *système algébrique* est la donnée d'un ensemble fini F de polynômes de $\mathbf{P}_n$.

Soit I l'idéal de $\mathbf{P}_n$ engendré par F. Mathématiquement, «résoudre» le système F c'est déterminer la variété $V = \mathbf{V}_K(F) = \mathbf{V}_K(I)$. Cela peut être entendu de plusieurs manières. D'un point de vue numérique, pour $K = \mathbb{C}$ on cherchera à trouver un ensemble de n-uplets $(a_1, \ldots, a_n)$ de K^n qui fournissent des valeurs approchées des coordonnées des points de V. On peut aussi adopter une approche formelle pour décrire exactement la variété V; c'est dans ce cadre que nous nous plaçons. En utilisant la correspondance entre variétés et idéaux, il s'agit alors de déterminer un ou plusieurs ensembles de polynômes qui décrivent le radical de I de façon plus satisfaisante que F lui-même. Ce qu'on entend par «satisfaisant» dépend étroitement de l'usage qu'on veut faire de la solution. On effectue ainsi une *résolution géométrique* du problème. Mais nous avons vu plus haut qu'en passant de l'idéal I à sa variété, autrement dit à son radical, on perdait de l'information. On peut donc choisir de conserver l'information maximale tout au long du calcul pour obtenir en fin de compte une description de l'idéal I lui-même. C'est ce que nous appellerons une *résolution algébrique*.

Une forme bien connue de résolution algébrique est basée sur l'utilisation de bases de Gröbner. La notion de base de Gröbner et ses principales propriétés sont rappelées dans l'annexe B (le lecteur pourra consulter [BW93] ou [CLO92] pour plus de détails à ce sujet). Cette résolution consiste à calculer une base de Gröbner de l'idéal I. Lorsque le système a un nombre fini de solutions, on peut ainsi obtenir pour l'ordre lexicographique un système G de générateurs de I sous la forme :

$$\begin{cases} g_1(x_1) \\ g_{2,1}(x_1, x_2) \\ \ldots \\ g_{2,r_2}(x_1, x_2) \\ \ldots \\ g_{n,1}(x_1, \ldots, x_n) \\ \ldots \\ g_{n,r_n}(x_1, \ldots, x_n) \; . \end{cases}$$

À partir du système G on peut répondre à certaines questions qui n'étaient en général pas accessibles directement avec le système de départ. Il est possible, par exemple, de dire algorithmiquement si un polynôme p donné appartient ou non à l'idéal I en calculant la *forme normale* de p par rapport à G.

Les développements effectués à partir de l'algorithme de Buchberger [Buc65] ont permis des implantations de plus en plus efficaces de cette méthode (GB [Fau94], MAGMA [CP97],...) bien que la complexité de cet algorithme soit doublement exponentielle en le nombre de variables [Huy86]. Récemment, la nouvelle génération d'algorithmes présentée par J.C. Faugère [Fau97] offre encore des progrès considérables.

Néanmoins la lecture de la géométrie du système sur une base de Gröbner n'est pas forcément facile. Pour y remédier, on peut utiliser comme alternative, ou en complément, une méthode de résolution géométrique qui représente l'ensemble des zéros du système à l'aide de systèmes triangulaires de polynômes. Dans ce cadre, une solution du système est alors constituée d'une famille finie de systèmes triangulaires T_j qui, dans le cas où le nombre de zéros est fini, s'écrivent sous la forme

$$\begin{cases} g_1(x_1) \\ g_2(x_1, x_2) \\ g_3(x_1, x_2, x_3) \\ \dots \\ g_n(x_1, \dots, x_n) \; . \end{cases}$$

L'expression des zéros de F en fonction des T_j peut être variable selon les algorithmes employés. Toujours dans le cas d'un nombre fini de zéros, avec de *bonnes* méthodes, on aura $\mathbf{V}_K(F) = \cup_j \mathbf{V}_K(T_j)$ et des polynômes g_i dont l'image dans $(\mathbf{P}_{i-1}/\langle g_1, \dots, g_{i-1}\rangle)[x_i]$ est unitaire. On peut alors déduire aisément avec un tel résultat les solutions numériques. Attention, si le système de départ admet une infinité de zéros alors certains des g_i ci-dessus peuvent être absents. De plus, l'expression de $\mathbf{V}_K(F)$ en fonction des T_j ne correspond pas obligatoirement à celle donnée ci-dessus (voir les sections 5.4 et 5.5), mais nécessite des notions qui sont introduites plus loin.

Lorsque le système F est de dimension zéro, une autre façon de résoudre au sens algébrique consiste à calculer une Représentation Univariée Rationnelle (RUR) du système [Rou98]. Une implantation efficace de F. Rouillier [Rou96] permet de calculer une telle représentation à partir d'une base de Gröbner de I pour un ordre quelconque. Cette représentation a pour intérêt de conserver les multiplicités des zéros du système F et d'être particulièrement adaptée à la recherche des zéros réels du système. La RUR est aussi un ensemble triangulaire mais comporte une variable supplémentaire t, et s'écrit sous la forme

$$\begin{cases} p(t) \\ g_1(t, x_1) \\ g_2(t, x_2) \\ g_3(t, x_3) \\ \dots \\ g_n(t, x_n) \end{cases}$$

où les g_i sont linéaires en x_i. Pour obtenir une décomposition en plusieurs RUR, il faudrait encore factoriser le polynôme $p(t)$, dont le degré est celui de l'idéal I et peut donc être élevé. Si on ne cherche pas à conserver les multiplicités, le calcul de RUR et les méthodes de décomposition triangulaire que nous présentons dans ce document peuvent alors être complémentaires. En effet, le calcul de RUR est plus facile à partir d'une décomposition triangulaire qu'à partir d'une base de Gröbner de I car le degré des variétés associées aux ensembles triangulaires obtenus est plus petit que celui de l'idéal de départ. On obtient de cette façon plusieurs RUR qui ont l'avantage d'être plus compactes qu'une RUR calculée à partir d'une base de Gröbner de I. Ce phénomène est particulièrement visible sur des exemples qui se scindent en beaucoup de composantes (comme les cyclic-n [Bjö85]).

Chapitre 2

Les structures de base

Résumé

Ce chapitre présente les structures de données que nous utilisons dans nos algorithmes. Nous introduisons les notions liées à la représentation récursive des polynômes que nous utilisons. Dans les méthodes de décomposition triangulaire de systèmes de polynômes de $k[x_1, \ldots, x_n]$, les polynômes sont considérés comme des polynômes à une variable sur l'anneau $k[x_1, \ldots, x_{n-1}]$. La terminologie associée à cette vision récursive est précisée dans la première section. Nous y examinons aussi quelques propriétés de la pseudo-division. Cette opération est en effet à la base de nos algorithmes.

La section 2 présente la notion d'ensemble triangulaire de polynômes et la terminologie associée dont nous aurons besoin dans tout le document. Les différentes notions de réduction par un ensemble triangulaire sont rappelées. Grâce à la propriété que nous établissons dans le lemme 2.2.11, la proposition 2.2.13 relie la réduction par un ensemble triangulaire avec le concept de monôme de tête, bien connu dans la théorie des bases de Gröbner, et permet de montrer les résultats de la section 4.7 concernant les ensembles triangulaires extraits d'une base de Gröbner . On introduit ensuite le concept fondamental de *saturé d'un ensemble triangulaire* dont le théorème 2.2.21 précise la relation avec la notion de *zéros réguliers*.

2.1 Polynômes

Nous précisons dans cette section les définitions et notations qui concernent les polynômes à plusieurs variables que nous manipulerons ensuite. La vision naturelle des polynômes associée aux méthodes que nous présenterons plus loin est une vision récursive. Sommairement, un polynôme p sera considéré comme un polynôme univarié en la variable la plus grande qui apparaît dans p. C'est une représentation tout-à-fait différente de celle utilisée dans la théorie des bases de Gröbner où l'on considère un polynôme comme une somme de monômes. Certaines notions similaires dans cette dernière théorie et dans celle basée sur les ensembles triangulaires pourraient prêter à confusion quand on utilise les deux théories simultanément. Pour cette raison nous utilisons une terminologie spécifique introduite dans [ALM99]. Cette terminologie n'est pas non plus complètement nouvelle puisque le concept important d'*initial* défini ci-dessous est standard en algèbre différentielle.

2.1.1 Définitions et notations

Pour un polynôme p de $\mathbf{P}_n$ on désignera le degré de p en la variable x_i par $\mathsf{deg}(p, x_i)$.

Définition 2.1.1 *Soit p un polynôme de $\mathbf{P}_n$ tel que $p \notin k$. La* variable principale *de p, qu'on désigne par $\mathsf{mvar}(p)$, est la plus grande des variables $x_1, \ldots, x_n$ qui apparaît dans p.*

Définition 2.1.2 *Soit p un polynôme non constant de $\mathbf{P}_n$ tel que $\mathsf{mvar}(p) = x_i$. Posons $p = cx_i^d + r$ où d est le degré de p en x_i, et c le coefficient de tête de p en x_i. On définit les notions suivantes :*

- *le degré d est appelé* degré principal *de p. Il est noté $\mathsf{mdeg}(p)$.*
- *le coefficient $c \in \mathbf{P}_{n-1}$ est appelé* initial *de p et noté $\mathsf{init}(p)$.*
- *le polynôme r est appelé* queue *de p, qu'on note $\mathsf{tail}(p)$.*
- *le terme cx_i^d est appelé* tête *de p, désigné par $\mathsf{head}(p)$.*

Exemple 2.1.3 Soit $n = 4$. Si $p = (x_2x_3 + x_2^3)x_4 - 2x_1$ alors on a $\mathsf{mvar}(p) = x_4$, $\mathsf{mdeg}(p) = 1$, $\mathsf{init}(p) = x_2x_3 + x_2^3$ et $\mathsf{tail}(p) = -2x_1$.

L'ordre partiel sur les polynômes de $\mathbf{P}_n$ que nous définissons ci-dessous est introduit dans [Rit66].

Définition 2.1.4 *Soit $p, q \in \mathbf{P}_n$. On dit que p est* plus petit que q pour l'ordre de Ritt *et on écrit $p \prec_r q$ si l'une des conditions suivantes est satisfaite :*

(i) $p \in k$ *et* $q \notin k$,

(ii) $p, q \notin k$ *et* $\mathsf{mvar}(p) < \mathsf{mvar}(q)$,

(iii) $p, q \notin k$ *et* $\mathsf{mvar}(p) = \mathsf{mvar}(q)$ *et* $\mathsf{mdeg}(p) < \mathsf{mdeg}(q)$.

On dit que p est plus grand que q pour l'ordre de Ritt *et on écrit $p \succ_r q$ si $q \prec_r p$. Les polynômes p et q sont* équivalents pour l'ordre de Ritt *si on a ni $p \prec_r q$, ni $p \succ_r q$. On écrit alors $p \sim_r q$.*

Remarque 2.1.5 Soit $p \in \mathbf{P}_n$ tel que $p \notin k$. On a alors

$$\mathsf{init}(p) \prec_r p \quad \text{et} \quad \mathsf{tail}(p) \prec_r p \ .$$

De plus, il est clair que toute suite de $\mathbf{P}_n$ de premier élément p qui est décroissante pour l'ordre de Ritt est finie.

2.1.2 Réduction et normalisation

La notion de réduction est importante pour la terminaison de certains algorithmes de décomposition triangulaire. Celle de normalisation apparaît dans [Laz91a]; c'est une notion cruciale de la méthode de décomposition en ensembles triangulaires proposée dans ce dernier article. Les définitions données ici induisent de façon naturelle les notions de réduction et de normalisation pour les ensembles triangulaires qui seront données plus loin.

Définition 2.1.6 *Soit $p, q \in \mathbf{P}_n$ tels que $q \notin k$. On dit que p est* réduit par rapport à *q et on écrit* $\mathsf{red?}(p, q)$ *si l'une des conditions suivantes est satisfaite :*

(i) $p \prec_r q$,

(ii) $p \notin k$ *et* $\mathsf{mvar}(p) > \mathsf{mvar}(q)$ *et* $\mathsf{red?}(\mathsf{init}(p), q)$ *et* $\mathsf{red?}(\mathsf{tail}(p), q)$.

La réduction, qu'on appelle aussi quelquefois *réduction forte*, se caractérise de façon simple.

Proposition 2.1.7 *Pour des polynômes p et q de $\mathbf{P}_n$ tels que $q \notin k$, les assertions suivantes sont équivalentes :*

(i) $\mathsf{red?}(p, q)$,

(ii) $\mathsf{deg}(p, \mathsf{mvar}(q)) < \mathsf{mdeg}(q)$.

Preuve. L'équivalence est triviale pour les éléments de k qui sont les éléments minimaux dans $\mathbf{P}_n$ pour l'ordre de Ritt. La remarque 2.1.5 permet d'obtenir le résultat par une induction sur p. □

Précisons maintenant de façon similaire une notion plus faible de réduction, dite *au sens des initiaux itérés*. Une caractérisation simple en termes de degrés est donnée ensuite dans la proposition 2.1.10.

Définition 2.1.8 *Soit $p, q \in \mathbf{P}_n$ tels que $q \notin k$. On dit que p est* initialement réduit par rapport à *q et on écrit* $\mathsf{iRed?}(p, q)$ *si l'une des conditions suivantes est satisfaite :*

(i) $p \prec_r q$,

(ii) $p \notin k$ *et* $\mathsf{mvar}(p) > \mathsf{mvar}(q)$ *et* $\mathsf{iRed?}(\mathsf{init}(p), q)$.

La définition suivante permet de caractériser la réduction au sens des initiaux itérés et d'introduire le concept de normalisation.

Définition 2.1.9 *Soit p un polynôme de $\mathbf{P}_n$. L'ensemble des* initiaux itérés *de p est la partie de $\mathbf{P}_n$ notée $\mathsf{iter}(p)$ définie comme suit : si $p \in k$ alors $\mathsf{iter}(p) = \emptyset$, sinon $\mathsf{iter}(p) = \{p\} \cup \mathsf{iter}(\mathsf{init}(p))$.*

Il est clair que pour une variable v donnée, il existe au plus un élément de $\mathsf{iter}(p)$ qui admet v pour variable principale. Par exemple, l'ensemble des initiaux itérés du polynôme $p = (x_2x_3 + x_2^3)x_4 - 2x_1$ est donné par $\mathsf{iter}(p) = \{x_2, x_2x_3 + x_2^3, p\}$.

Le résultat suivant se démontre de la même façon que la proposition 2.1.7 .

Proposition 2.1.10 *Pour des polynômes p et q de $\mathbf{P}_n$ tels que $q \notin k$, les assertions suivantes sont équivalentes :*

(i) $\mathsf{iRed?}(p, q)$,

(ii) $\forall h \in \mathsf{iter}(p) \setminus k,\ \mathsf{mvar}(h) = \mathsf{mvar}(q) \ \Rightarrow\ \mathsf{mdeg}(h) < \mathsf{mdeg}(q)$.

Définition 2.1.11 *Soit $p, q \in \mathbf{P}_n$ tels que $q \notin k$. On note $v = \mathsf{mvar}(q)$. On dit que p est* normalisé *par rapport à q si aucun polynôme de l'ensemble $\mathsf{iter}(p)$ n'admet v comme variable principale.*

Remarque 2.1.12 Si p est normalisé par rapport à q alors p est initialement réduit par rapport à q.

Exemple 2.1.13 Soit $p = (x_2x_3 + x_2^3)x_4 - 2x_1$ déjà donné ci-dessus. Le polynôme p est normalisé (mais non réduit) par rapport au polynôme x_1 puisqu'aucun élément de $\mathsf{iter}(p)$ n'a pour variable principale x_1. Si $q = x_1x_2^2 - 3$ alors p n'est pas normalisé par rapport à q puisque le polynôme x_2 est un élément de $\mathsf{iter}(p)$ dont la variable principale est la même que celle de q. Il est clair que p n'est pas réduit par rapport à q. Cependant p est initialement réduit par rapport à q car $\mathsf{mdeg}(x_2) < \mathsf{mdeg}(q)$. Enfin avec $q = x_3^2 - 2x_1x_2x_3 + 3x_1$ on peut constater que p peut être réduit par rapport à q sans être normalisé.

Notation 2.1.14 *Soit F une partie de $\mathbf{P}_n$ et i un entier de $[1, n]$. On note*

$$F^-_{x_i} \;=\; F \cap \mathbf{P}_{i-1} \quad \text{et} \quad F^+_{x_i} \;=\; \{f \in F \;\mid\; \mathsf{mvar}(f) > x_i\} \ .$$

2.1.3 Propriétés de la pseudo-division

Notation 2.1.15 *Soit A un anneau commutatif unitaire. Soient $p, f \in A[X]$ avec $p \neq 0$. On notera $\mathsf{lc}(p)$ le coefficient du monôme de plus haut degré de p et $\mathsf{deg}(p)$ ce degré. On désigne par $\mathsf{prem}(p, f)$ et $\mathsf{pquo}(p, f)$ le pseudo-reste et le pseudo-quotient de p par f. Rappelons que ces polynômes sont définis par :*

(i) $\delta \;=\; \max(0, \mathsf{deg}(p) - \mathsf{deg}(f) + 1)$,

(ii) $\mathsf{lc}(f)^{\delta}\, p \;=\; \mathsf{pquo}(p,f)\, p \;+\; \mathsf{prem}(p,f)$,

(iii) $\mathsf{prem}(p,f) \neq 0 \implies \mathsf{deg}(\mathsf{prem}(p,f),X) < \mathsf{deg}(f)$.

Donnons d'abord quelques propriétés immédiates de la pseudo-division.

Proposition 2.1.16 *Soit A un anneau intègre et c un élément non nul de A. Soit $p \in A[X]$ et $f \in A[X] \setminus A$. On note h l'initial de f et $\delta = max(\mathsf{deg}(p,X) - \mathsf{deg}(f,X)+1,0)$. Si r est le pseudo-reste de p par f, alors on a :*

(i) $\mathsf{prem}(cp,f) \;=\; c\,r$,

(ii) $\mathsf{prem}(p,cf) \;=\; c^{\delta}\, r$.

Preuve. Il existe un unique polynôme q tel que $h^{\delta}p = qf + r$. On a alors $h^{\delta}(cp) = (cq)f + cr$. Si $r \neq 0$ alors $cr \neq 0$ et $\mathsf{deg}(cr,X) < \mathsf{deg}(f,X)$. Si r est nul alors cr aussi. Dans les deux cas, le résultat (i) découle donc de l'unicité du pseudo-reste.

On montre (ii) maintenant. Si $\delta = 0$ alors $\mathsf{prem}(p,f) = p$ et l'égalité est évidente. Si $\delta > 0$ alors on a $h^{\delta}\, c^{\delta}\, p = c^{\delta-1}\, q\,(cf) + c^{\delta}\, r$. Puisque hc est l'initial de cf et $\mathsf{deg}(c^{\delta}r,X) < \mathsf{deg}(f,X)$ dans le cas où r est non nul, l'unicité du pseudo-reste assure encore ici le résultat. □

Nous verrons que les notions de réduction pour les ensembles triangulaires sont liées à une situation où le polynôme p de la proposition 2.1.16 a une variable principale plus grande que celle de f. On s'intéresse ci-dessous au propriétés particulières à ce cas de figure.

Proposition 2.1.17 *Soit i et j deux entiers de $[1,n]$ tels que $i < j$. On considère deux polynômes f et p de $\mathbf{P}_n$ tels que $\mathsf{mvar}(f) = x_i$ et $\mathsf{mvar}(p) = x_j$. On pose $h = \mathsf{init}(f)$ et $p = \sum_{k=0}^{d} p_k x_j^k$, où $d = \mathsf{mdeg}(p)$. Pour tout entier k on pose $\mu_k = \mathsf{deg}(p,x_i) - \mathsf{deg}(p_k,x_i)$. Alors si $\mathsf{deg}(p,x_i) \geq \mathsf{deg}(f,x_i)$ on a*

$$\mathsf{prem}(p,f) \;=\; \sum_{k=0}^{d} h^{\mu_k}\, \mathsf{prem}(p_k,f)\, x_j^k \; .$$

Preuve. Soit r le pseudo-reste de p par f et $\delta = \mathsf{deg}(p,x_i) - \mathsf{deg}(f,x_i) + 1$. De même $\delta_k = \mathsf{deg}(p_k,x_i) - \mathsf{deg}(f,x_i) + 1$. Il existe un polynôme q tel que

$$h^{\delta}p = qf + r \; . \tag{2.1}$$

Notons p_k (resp. q_k, r_k) le coefficient de p (resp. q, r) de degré k en x_j. La variable x_j n'apparaissant ni dans f ni dans h, on obtient

$$h^{\delta}p_k = q_k f + r_k \; . \tag{2.2}$$

Par conséquent on a

$$h^{\delta_k}(h^{\mu_k}p_k) = q_k f + r_k \; . \tag{2.3}$$

Puisque $\mathsf{deg}(r_k,x_i) < \mathsf{deg}(r,x_i) < \mathsf{mdeg}(f)$, on en conclut $r_k = \mathsf{prem}(h^{\mu_k}p_k, f)$. Comme x_i n'est pas une variable de h, il suffit ensuite d'appliquer la proposition 2.1.16 pour obtenir $r_k = h^{\mu_k}\mathsf{prem}(p_k,f)$. □

Le corollaire ci-dessous est une conséquence immédiate de la proposition 2.1.17.

Corollaire 2.1.18 *Avec les hypothèses de la proposition 2.1.17, on a*

- $\mathsf{prem}(p, f) = 0 \iff (\forall k \in [0, d])\ \mathsf{prem}(p_k, f) = 0$.
- $\mathsf{deg}(\mathsf{prem}(p, f), \mathsf{mvar}(p)) = \mathsf{mdeg}(p) \iff \mathsf{prem}(p_d, f) \neq 0$,

2.2 Ensembles triangulaires

2.2.1 Définitions et notations

Dans cette section nous donnons les définitions les plus générales concernant les ensembles triangulaires. La notion de réduction est rappelée. Celle-ci est primordiale dans certains algorithmes utilisant les ensembles triangulaires. La terminaison des algorithmes de Ritt [Rit66] et de Wu [Wu87] est basée sur la notion d'ensemble triangulaire *réduit* (qu'on trouve sous les termes anglais de «chain» dans [Rit66] et de «ascending set» dans [Wu87]). D'autres notions plus faibles de réduction sont utiles pour améliorer l'efficacité de la méthode de Wu. Nous précisons en particulier celle d'ensemble triangulaire *initialement réduit* qui apparaît dans les relations entre bases de Gröbner et ensembles triangulaires étudiées dans la partie 4.7.

Définition 2.2.1 *Une partie T de $\mathbf{P}_n$ est appelé un* ensemble triangulaire *si aucun élément de T n'appartient au corps de base k et si pour tout couple d'éléments distincts (p, q) de T on a $\mathsf{mvar}(p) \neq \mathsf{mvar}(q)$.*

Une variable $v \in \{x_1, \ldots, x_n\}$ est dite algébrique *par rapport à T s'il existe un polynôme p de T tel que $v = \mathsf{mvar}(p)$. Dans le cas contraire v est dite* transcendante *par rapport à T. L'ensemble des variables qui sont algébriques par rapport à T est noté $\mathsf{algVar}(T)$. Si T n'est pas vide, on note $\mathsf{mvar}(T)$ le plus grand élément de $\mathsf{algVar}(T)$.*

Exemple 2.2.2 Soit $n \geq 4$. Le sous-ensemble $\{x_1^3 x_2 + 1, x_1 x_2^2 - 1\}$ de $\mathbf{P}_n$ n'est pas un ensemble triangulaire. Par contre $T_1 = \{x_1 x_2^2 - 3, x_3^2 - 2x_1 x_2 x_3 + 3x_1, (x_2 x_3 + x_2^3)x_4 - 2x_1\}$ est un ensemble triangulaire, et $\mathsf{algVar}(T_1) = \{x_2, x_3, x_4\}$.

Remarque 2.2.3 Si p est un polynôme de $\mathbf{P}_n$ alors $\mathsf{iter}(p)$, l'ensemble des initiaux itérés de p (voir définition 2.1.9), est un ensemble triangulaire.

Notation 2.2.4 *Soit T un ensemble triangulaire de $\mathbf{P}_n$ et i un entier de $\{1, \ldots, n\}$. Si x_i est une variable algébrique par rapport à T alors on note T_{x_i} l'unique polynôme de T de variable principale x_i. Rappelons aussi que*

$$T_{x_i}^- = T \cap \mathbf{P}_{i-1} \quad \text{et} \quad T_{x_i}^+ = \{t \in T \mid \mathsf{mvar}(t) > x_i\} .$$

La terminologie associée au concept de réduction avec les ensembles triangulaires provient naturellement de celle introduite dans la section 2.1 concernant la réduction entre deux polynômes.

Définition 2.2.5 *Soit $p \in \mathbf{P}_n$ et T un ensemble triangulaire de $\mathbf{P}_n$. On dit que p est* réduit *(resp.* initialement réduit*, resp.* normalisé*) par rapport à T si p est réduit (resp. initialement réduit, resp. normalisé) par rapport à chaque élément de T. On écrit alors respectivement* $\mathsf{red?}(p, T)$*,* $\mathsf{iRed?}(p, T)$ *et* $\mathsf{normalized?}(p, T)$*.*

Un ensemble triangulaire de $\mathbf{P}_n$ est dit réduit *(resp.* initialement réduit*, resp.* normalisé*) si pour chaque $t \in T$ tel que $v = \mathsf{mvar}(p)$, on a $\mathsf{red?}(t, T_v^-)$ (resp. $\mathsf{iRed?}(t, T_v^-)$, resp. $\mathsf{normalized?}(t, T_v^-)$).*

Exemple 2.2.6 Soit $n \geq 4$. L'ensemble triangulaire T_1 (exemple 2.2.2) de $\mathbf{P}_n$ est un ensemble triangulaire initialement réduit, mais il n'est ni réduit, ni normalisé (consulter l'exemple 2.1.13). L'ensemble triangulaire $T_2 = \{x_1x_2^2 - 3, x_3 - 2x_1x_2, (x_2x_3 + x_2^3)x_4 - 2x_1\}$ n'est pas initialement réduit puisque le degré en x_3 de l'initial du troisième polynôme n'est pas strictement inférieur au degré principal du deuxième polynôme $x_3 - 2x_1x_2$. L'ensemble $T_3 = \{x_1x_2^2 - 3, x_3 - 2x_1x_2, 3(x_2 + 2x_1)x_4 - 2x_1\}$ est réduit mais pas normalisé. Enfin $T_4 = \{x_1x_2^2 - 3, x_3 - 2x_1x_2, (12x_1^3 + 9)x_4 + 2x_1^2x_2 - 4x_1^3\}$ est un ensemble triangulaire normalisé.

La définition d'un ensemble triangulaire réduit donnée ci-dessus correspond à celle de [Rit66] et [Wu87]. Cependant la notion d'ensemble triangulaire initialement réduit est plus faible que celle d'ensemble triangulaire *réduit en tête* que Wu appelle «ascending set in the weak sense» (voir p. 6 de [Wu87]). Un ensemble triangulaire T est réduit en tête si l'initial de tout élément t de T est réduit par rapport à T. Pour être initialement réduit, il suffit que pour chaque polynôme $p \in \mathsf{iter}(t) \setminus \{t\}$ tel qu'il existe $t' \in T$ avec $\mathsf{mvar}(p) = \mathsf{mvar}(t')$ on ait $\mathsf{red?}(p, t')$. Wu avait remarqué que ses calculs étaient souvent plus rapides lorsqu'il n'utilisait aucune notion de réduction. Mais la terminaison de son algorithme n'était alors plus assurée. La notion de réduction par rapport aux initiaux itérés permet d'assurer la terminaison de l'algorithme de Wu tout en pouvant bénéficier d'une plus grande efficacité qu'avec les notions de réduction plus fortes utilisées par Wu.

Passons maintenant à la notion de pseudo-reste par rapport à un ensemble triangulaire. Étant donné un ensemble triangulaire T et un polynôme p de $\mathbf{P}_n$, on peut construire par pseudo-divisions successives un polynôme r réduit par rapport à T comme il est précisé ci-dessous. En vue de l'étude des ensembles caractéristiques dans la section 4.2, on définit alors l'ensemble des polynômes p qui se réduisent ainsi à 0 (notation 2.2.8).

Notation 2.2.7 *Soit $p, q \in \mathbf{P}_n$ avec $q \notin k$. Dans toute la suite, on désigne par* $\mathsf{prem}(p, q)$ *et* $\mathsf{pquo}(p, q)$ *respectivement le pseudo-reste et le pseudo-quotient de p par q, considérés comme des polynômes en la variable* $\mathsf{mvar}(q)$*. Soit $T \subseteq \mathbf{P}_n$ un ensemble triangulaire. Si $T = \emptyset$ on définit $\mathsf{prem}(p, T) = p$ sinon $\mathsf{prem}(p, T) = \mathsf{prem}(\mathsf{prem}(p, T_v), T_v^-)$ où v est la plus grande variable de* $\mathsf{algVar}(T)$*. Par exemple, avec*

$$T_4 = \{x_1(x_1 - 1), x_1x_2 - 1\}$$

et

$$p = x_2^2 + x_1x_2 + x_1^2 \ ,$$

on a

$$\mathsf{prem}(p,T) \;=\; \mathsf{prem}(\mathsf{prem}(p,T_{x_2}),T_{x_1}) \;=\; \mathsf{prem}(x_1^4+x_1^2+1,T_{x_1}) \;=\; 2\;x_1+1\;.$$

Notation 2.2.8 *Soit T un ensemble triangulaire de $\mathbf{P}_n$. On désigne par $\mathsf{red}_{\mapsto 0}(T)$ le sous-ensemble de $\mathbf{P}_n$ défini par :*

$$\mathsf{red}_{\mapsto 0}(T) \;=\; \{p \in \mathbf{P}_n \;\mid\; \mathsf{prem}(p,T)=0\}$$

Remarque 2.2.9 L'ensemble $\mathsf{red}_{\mapsto 0}(T)$ n'est pas nécessairement un idéal de $\mathbf{P}_n$. En effet, considérons l'ensemble triangulaire $T_4 = \{x_1^2 - x_1, x_1x_2 - 1\}$ donné dans la notation 2.2.7. On pose $p = -(x_1^2 - x_1)x_2 + x_1 - 1$ et $q = (x_1^2 - x_1)x_2$. On vérifie immédiatement que $\mathsf{prem}(p,T) = \mathsf{prem}(q,T) = 0$. On a pourtant $p+q = x_1 - 1$ donc $(p+q) \notin \mathsf{red}_{\mapsto 0}(T)$. De plus, puisque $p+q \in \langle T \rangle$, on constate que $\mathsf{red}_{\mapsto 0}(T)$ ne contient pas toujours l'idéal engendré par T.

La propriété suivante apparaît dans [Wu84] sous le nom de *remainder formula.*

Proposition 2.2.10 *Soit $p \in \mathbf{P}_n$ et $T = \{t_1,\ldots,t_m\}$ un ensemble triangulaire non vide de $\mathbf{P}_n$. On note c_k l'initial de t_k. Alors on a $\mathsf{red?}(\mathsf{prem}(p,T),T)$. De plus il existe des entiers naturels $e_1,\ldots,e_m$ et des polynômes $q_1,\ldots,q_m$ de $\mathbf{P}_n$ tels que*

$$c_1^{e_1}\cdots c_m^{e_m}p \;=\; q_1t_1+\cdots+q_mt_m+\mathsf{prem}(p,T)\;.$$

Preuve. Ce résultat est facilement obtenu par récurrence sur m en utilisant la proposition 2.1.7. □

Les propriétés suivantes seront principalement exploitées dans les sections 4.2 et 4.7.

Lemme 2.2.11 *Soit T un ensemble triangulaire de $\mathbf{P}_n$ et p un polynôme non nul de $\mathbf{P}_n$. Si $\mathsf{prem}(p,T)=0$ alors il existe un polynôme $c \in \mathsf{iter}(p)$ de variable principale v tel que*

(i) $v \in \mathsf{algVar}(T)$,

(ii) $\mathsf{mdeg}(c) \geq \mathsf{mdeg}(T_v)$,

(iii) $\mathsf{prem}(c,T)=0$.

Preuve. Il est clair que $p \notin k$ donc $\mathsf{iter}(p)$ est non vide. On raisonne par récurrence sur le nombre d'éléments de $\mathsf{iter}(p)$. Supposons que $\mathsf{iter}(p) = \{p\}$ et posons $v = \mathsf{mvar}(p)$. Remarquons d'abord que

$$\mathsf{prem}(\mathsf{init}(p),T_v^-) \neq 0 \tag{2.4}$$

puisque $\mathsf{init}(p)$ est une constante non nulle. Si v était transcendante on aurait $\mathsf{prem}(p,T_v^-) = \mathsf{prem}(p,T) = 0$ donc $\mathsf{prem}(\mathsf{init}(p),T_v^-) = 0$ selon le corollaire 2.1.18, ce qui contredit l'égalité (2.4). On en déduit que $v \in \mathsf{algVar}(T)$. Si on avait maintenant $\mathsf{mdeg}(p) < \mathsf{mdeg}(T_v)$ il en résulterait que $\mathsf{prem}(p, T_v^-) = \mathsf{prem}(p, T) = 0$ comme dans le cas précédent, et on aboutirait encore à une contradiction. Finalement, il suffit de prendre $c = p$. Supposons maintenant que $\mathsf{iter}(p) \neq \{p\}$ et posons $h = \mathsf{init}(p)$. Si p ne vérifie pas les conditions voulues alors on a $\mathsf{mvar}(p)$ transcendante par rapport à T ou bien $\mathsf{mvar}(p)$ algébrique et $\mathsf{mdeg}(p) < \mathsf{mdeg}(T_v)$. Il en résulte dans les deux cas que $\mathsf{prem}(p, T_v^-) = \mathsf{prem}(p, T) = 0$ et le corollaire 2.1.18 entraîne alors $\mathsf{prem}(\mathsf{init}(p), T_v^-) = 0$. Puisqu'ainsi $\mathsf{prem}(\mathsf{init}(p), T) = 0$, on conclut avec l'hypothèse de récurrence. □

Remarque 2.2.12 Soit p un polynôme non constant de $\mathbf{P}_n$ et $h_1 \prec_r h_2 \prec_r \ldots \prec_r h_s = p$ l'ensemble des éléments de $\mathsf{iter}(p)$. Notons leur variable principale respectivement $x_{i_1} < x_{i_2} \ldots < x_{i_s}$ et $d_j = \mathsf{mdeg}(h_j)$. On a alors

$$\mathsf{lm}(p) = \prod_{1 \leq j \leq s} x_{i_j}^{d_j} \; .$$

A partir du lemme 2.2.11 on déduit alors clairement la proposition suivante qui est primordiale pour l'étude des liens entre bases de Gröbner et ensembles caractéristiques dans la section 4.7.

Proposition 2.2.13 *Soit T un ensemble triangulaire de $\mathbf{P}_n$ et p un polynôme non nul de $\mathbf{P}_n$. Si* $\mathsf{prem}(p, T) = 0$ *alors* $\mathsf{lm}(p)$ *n'est pas réduit par rapport à T.*

La notion d'ensemble triangulaire *standard* précisée ci-dessous est plus faible que celle d'ensemble triangulaire initialement réduit. Elle est utilisée dans certains algorithmes de décomposition triangulaire [CG90] [Wan93b]. Tout en restant assez générale, elle est adéquate pour établir certains résultats de la section 4.2 et intervient ainsi dans le théorème 4.6.1 qui permet d'unifier des notions provenant de différentes théories.

Définition 2.2.14 *Un ensemble triangulaire T de $\mathbf{P}_n$ est dit* standard *s'il n'est pas vide et si pour toute variable v de* $\mathsf{algVar}(T)$ *on a* $\mathsf{prem}(\mathsf{init}(T_v), T_v^-) \neq 0$. *Le terme anglais original correspondant est* fine triangular set.

Proposition 2.2.15 *Tout ensemble triangulaire non vide initialement réduit est standard.*

Preuve. C'est une conséquence du lemme 2.2.11. □

2.2.2 Saturé et zéros réguliers

Dans les méthodes de résolution de systèmes d'équations algébriques qui travaillent avec des ensembles triangulaires, ce n'est pas généralement la k-variété associée à un ensemble triangulaire T que l'on prendra en compte. Dans des méthodes telles que celles de Wu [Wu87], Wang [Wan93b], Lazard et Moreno Maza [Laz91a] [Mor97], on considère l'ensemble des *zéros réguliers* de T (définition 2.2.20).

D'autre part, nous verrons plus loin que les spécifications de la méthode de Kalkbrener [Kal93] et des extensions que nous en obtenons, font intervenir la notion d'*idéal saturé* de T (définition 2.2.16). Le concept d'idéal saturé d'un ensemble triangulaire apparaît sous un autre nom dans [CG90]. Cependant, le concept plus général d'idéal saturé par rapport à un sous-ensemble multiplicativement clos d'un anneau est standard en algèbre commutative (voir [Bou61a], p. 90).

Cette section précise les notions précédentes qui nous permettront d'étudier les propriétés des ensembles triangulaires de polynômes.

Définition 2.2.16 *Soit $T \subseteq \mathbf{P}_n$ un ensemble triangulaire non vide et h le produit des initiaux des polynômes de T. On appelle* idéal saturé *de T, ou plus simplement* saturé *de T, l'idéal de $\mathbf{P}_n$, noté $\mathsf{sat}(T)$ et défini par :*

$$\mathsf{sat}(T) \ = \ \{p \in \mathbf{P}_n \ \mid \ (\exists n \in \mathbb{N}) \ h^n p \in \langle T \rangle\} \ .$$

Lorsque $T = \emptyset$ on pose $\mathsf{sat}(T) = \{0\}$.

Notation 2.2.17 *Pour $i \in \{0, \ldots, n\}$, si T est un ensemble triangulaire inclus dans $\mathbf{P}_i$, on désigne par $\mathsf{sat}_i(T)$ l'idéal saturé de T dans $\mathbf{P}_i$.*

La propriété suivante s'obtient de façon triviale avec la proposition 2.2.10.

Proposition 2.2.18 *Pour tout ensemble triangulaire $T \subseteq \mathbf{P}_n$ on a la relation suivante :*

$$\mathsf{red}_{\mapsto 0}(T) \subseteq \mathsf{sat}(T) \ .$$

Remarque 2.2.19 L'inclusion ci-dessus peut ne pas correspondre à une égalité. Il suffit de reprendre l'exemple donné dans la remarque 2.2.9, où $\mathsf{red}_{\mapsto 0}(T)$ ne contient pas $\langle T \rangle$ et n'est même pas un idéal.

Définition 2.2.20 *Soit $T \subseteq \mathbf{P}_n$ un ensemble triangulaire non vide et h le produit des initiaux des polynômes de T. On appelle* zéro régulier *de T tout zéro de T sur lequel h ne s'annule pas. L'ensemble des zéros réguliers de T est désigné par $\mathbf{W}(T)$:*

$$\mathbf{W}(T) \ = \ \mathbf{V}(T) \setminus \mathbf{V}(h) \ .$$

Théorème 2.2.21 *Pour un ensemble triangulaire T de $\mathbf{P}_n$ non vide, on a :*

$$\overline{\mathbf{W}(T)} \ = \ \mathbf{V}(\mathsf{sat}(T))$$

Preuve. C'est une application de la proposition A.1.16 puisque par définition $\mathbf{V}(\mathsf{sat}(T)) = \mathbf{V}(\langle T \rangle : h^\infty)$, où h est le produit des initiaux des éléments de T. □

Définition 2.2.22 *Un ensemble triangulaire T est dit* consistant *si $\mathbf{W}(T) \neq \emptyset$, autrement dit si $\mathsf{sat}(T) \neq \mathbf{P}_n$ ou encore $h \notin \sqrt{\langle T \rangle}$.*

Exemple 2.2.23 L'ensemble triangulaire $T = \{x_2^2 - x_1^2, (x_1 + x_2)x_3 - 2x_1^2, (x_3 - x_1)x_4 + x_1\}$ n'est pas consistant. On vérifie effectivement que l'ensemble des zéros de T est paramétré par

$$V = \{(0, 0, 0, t), t \in K\} \cup \{(0, 0, t, 0), t \in K, t' \in K\} \ .$$

Tout zéro de T est donc zéro d'un initial de T.

On peut se demander pourquoi s'intéresser à l'idéal saturé de T plutôt qu'à l'idéal engendré par T lui-même. En fait, le saturé de T présente des propriétés intrinsèques que n'a pas l'idéal $\langle T \rangle$. Les exemples suivants illustrent comment peut se manifester cette insuffisance. Le lecteur pourra aussi consulter les exemples 4.3.7 et 4.3.9 donnés plus loin.

Exemple 2.2.24 Intéressons-nous à l'exploitation numérique des zéros d'un ensemble triangulaire. Avec une telle structure, il semble naturel de vouloir déterminer successivement les valeurs possibles de x_1, puis x_2 etc... en substituant à chaque étape dans un polynôme de variable principale x_i les variables $x_1, \ldots, x_{i-1}$ déjà étudiées. Prenons $T = \{x_1^2 - x_1, x_3 - x_2, x_2x_4 - x_1\}$ et voyons les difficultés qui peuvent survenir lorsqu'on essaie d'obtenir les zéros de T. On détermine les zéros du premier polynôme, puis la valeur de x_2 peut être quelconque. Ensuite x_3 doit être égal à x_2. Mais lors de l'étude du polynôme de variable principale x_4, on est amené à considérer la possibilité $x_1 = 0$ et $x_2 = 0$, ce qui montre que l'on ne se trouve pas dans le cadre d'une résolution par substitution successive. On remarque facilement que le fait de prendre en compte les zéros réguliers permet d'éviter cet écueil. On a déjà mentionné qu'on pouvait toutefois aboutir à un ensemble de zéros réguliers vide.

Exemple 2.2.25 Nous verrons dans la section 4.1 que le saturé de T est équidimensionnel et que la dimension de $\mathsf{sat}(T) = n - s$ où s est le nombre d'éléments de T. On n'a rien de tout ça pour l'idéal $\langle T \rangle$. En effet, soit $T = \{x_1^2 - x_1, x_1x_3 - x_2, x_1x_4 - x_2\}$. L'ensemble V des zéros de T peut être paramétré comme suit :

$$V = \{(1, t, t, t), t \in K\} \cup \{(0, 0, t, t'), t \in K, t' \in K\} \; .$$

On constate donc que la dimension de V, c'est-à-dire la dimension de $\langle T \rangle$, est 2, avec une composante de dimension 1 et une autre de dimension 2. Le passage au saturé permet d'éliminer la seconde composante pour obtenir finalement un idéal de dimension 1.

Chapitre 3

Anneaux de polynômes

Résumé

Nous avons déjà précisé que la résolution de systèmes polynomiaux à l'aide d'ensembles triangulaires faisait intervenir naturellement une vision récursive des polynômes. Nous traitons généralement les polynômes de $\mathbf{P}_n$ comme des polynômes en une variable sur $\mathbf{P}_{n-1}$. De plus, nous considérons souvent plutôt que ces polynômes eux-mêmes, leur image dans un anneau de polynômes en une variable sur un anneau total de fractions défini par un ensemble triangulaire. C'est en effet cette image qui importe dans les algorithmes de la section 5.

Ce chapitre commence par la présentation de quelques propriétés des extensions d'idéaux d'un anneau A dans $A[X]$. Certaines sont classiques mais d'autres correspondent plutôt à des exercices d'algèbre commutative. N'ayant pas trouvé ces derniers résultats dans la littérature classique, nous en donnons leur preuve car ils sont nécessaires pour établir la plupart des propriétés relatives aux ensembles triangulaires.

La seconde section introduit la notion nouvelle d'*idéal quasi-monogène*, qui correspond aux idéaux J de $A[X]$ engendrés par un idéal I de A et un polynôme $f \in A[X] \setminus A$. Nous en dégageons les propriétés principales, plus particulièrement lorsque cet idéal est *régulier*, c'est-à-dire quand l'initial du polynôme f n'est pas diviseur de zéro modulo I. Nous montrons que notre notion d'idéal quasi-monogène régulier se comporte bien pour le passage aux idéaux d'élimination (proposition 3.2.5) et mettons en évidence qu'on peut dans ce cas caractériser l'idéal saturé de J par l'initial de f en termes de pseudo-reste (propositions 3.2.9 et 3.2.10).

Les propriétés étudiées dans ces deux premières sections sont fondamentales puisqu'elles recouvrent les deux cas de figure qu'on rencontre en travaillant récursivement avec les chaînes régulières ou ensembles triangulaires réguliers (définitions 4.3.3 et 4.4.5). Le travail que nous avons réalisé sur les concepts de ces deux premières sections a fourni le moteur inductif de résultats apparus dans [AM97] puis publiés dans [ALM99], qui sont présentés ici dans le théorème 4.3.11 sous une forme plus large et dans le théorème 4.4.11.

Nous nous intéressons finalement dans la troisième section au cas où A est un produit de corps. À partir de la définition la plus générale possible d'un pgcd, on dispose sur de telles structures de propriétés presque similaires à celles observées dans le cas d'un corps. Cette partie permet de comprendre le principe de gestion dynamique de scindages des algorithmes ggcd de [Kal93] et [Kal95] et subResGcd du chapitre 5, qui sont à la base de méthodes de décomposition triangulaire que nous avons implantées. L'isomorphisme que nous établirons

dans le théorème 4.4.14 montre que ces algorithmes calculent un pgcd sur un produit de corps et fournit une validation mathématique à l'algorithme ggcd de M. Kalkbrener. Il montre aussi la base commune avec les autres algorithmes de gestion dynamique de scindages présentés dans [MR95] et [Mor97], ce qui n'avait rien d'évident jusqu'alors.

3.1 Idéaux de A[X] engendrés par un idéal de A

Soit A un anneau commutatif unitaire. On examine les relations entre les idéaux de A et leur extension dans l'anneau de polynômes $A[X]$ par l'homomorphisme injectif canonique. Pour un idéal I de A, nous désignerons dans tout le document par $I[X]$ l'extension I^e de I dans $A[X]$. Dans le cas particulier d'un anneau de polynômes en une variable les propriétés des extensions rappelées dans la proposition A.1.4 se renforcent. Ensuite, la proposition 3.1.4 permet de caractériser les ensembles composés respectivement des éléments inversibles, des nilpotents et des diviseurs de zéro de $A[X]$. Les propriétés de la proposition 3.1.5 sont des propriétés de base pour l'étude des ensembles triangulaires et seront couramment utilisées dans l'ouvrage.

Notation 3.1.1 *Dans toute la suite, on désigne par* $\mathbf{Un}(A)$ *l'ensemble des unités de* A *et par* $\mathbf{Div}(A)$ *l'ensemble des éléments de* A *qui sont diviseurs de zéro. Le nilradical de* A*, c'est-à-dire l'idéal des éléments nilpotents de* A*, est noté* $\mathbf{Nil}(A)$*.*

Proposition 3.1.2 *Soit* I *un idéal de* A*. Soit* $p \in A[x]$ *tel que* $p = \sum_{i=0}^{d} c_i x^i$*. Alors*

$$p \in I[X] \iff \forall i \in \{1, \ldots, d\},\ c_i \in I.$$

Preuve. Supposons que $p \in I[X]$. Il existe $a_1, \ldots, a_m \in I$ et $p_1, \ldots, p_m \in A[x]$ tels que $p = \sum_{j=1}^{m} a_j p_j$. On ordonne alors p suivant ses puissances croissantes et on constate que chaque coefficient c_i est une somme de a_j, donc un élément de I. L'implication réciproque est triviale. □

Proposition 3.1.3 *Soit* I*,* I_1 *et* I_2 *des idéaux de l'anneau* A*. On a :*

(*i*) $I[X] \cap A = I$

(*ii*) $(I_1 \cap I_2)[X] = I_1[X] \cap I_2[X]$.

Preuve. Montrons (i). Tout d'abord, il est clair que $I \subseteq I[X] \cap A$. Réciproquement, si $p \in I[X] \cap A$ alors la proposition 3.1.2 entraîne immédiatement que $p \in I$.

Passons à (ii). Puisque $(I_1 \cap I_2) \subseteq I_1$ on a $(I_1 \cap I_2)[X] \subseteq I_1[X]$ et de la même façon $(I_1 \cap I_2)[X] \subseteq I_2[X]$, ce qui prouve l'inclusion directe. Considérons maintenant $p \in I_1[X] \cap I_2[X]$. On pose $p = \sum_{i=0}^{d} c_i X^i$. L'application de la proposition 3.1.2 à I_1 (resp. I_2) entraîne que $c_i \in I_1$ (resp. $c_i \in I_2$) pour tout $1 \leq i \leq d$. On en déduit immédiaement que $p \in (I_1 \cap I_2)[X]$ donc $I_1[X] \cap I_2[X] \subseteq (I_1 \cap I_2)[X]$. □

Proposition 3.1.4 *On note* B *l'anneau de polynômes* $A[X]$*. Soit* $f = \sum_0^n a_i X^i$ *un polynôme de* B *avec* $a_i \in A$ *et* $a_n \neq 0$*. Alors on a :*

(*i*) $(f \in \mathbf{Un}(B)) \iff ((a_0 \in \mathbf{Un}(A))$ et $(a_1, \ldots, a_n \in \mathbf{Nil}(A)))$,

(*ii*) $(f \in \mathbf{Nil}(B)) \iff (a_0, \ldots, a_n \in \mathbf{Nil}(A))$,

(*iii*) $(f \in \mathbf{Div}(B)) \iff (\exists a \in A \mid (a \neq 0)$ et $(af = 0))$.

Preuve. Vérifions (i). Cette propriété est immédiate si $n=0$. Supposons maintenant $n>0$ et vérifions tout d'abord l'implication directe. On suppose donc qu'il existe $g \in A[X]$ tel que $fg=1$. On pose $g=\sum_0^m b_j X^j$. Quitte à introduire des b_j nuls, on peut supposer : $m \geq n$. On a alors :

$$\begin{cases} a_n b_m & = & 0 \\ a_n b_{m-1} + a_{n-1} b_m & = & 0 \\ a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m & = & 0 \\ & \vdots & \\ a_n b_0 + \cdots + a_0 b_n & = & 0 \end{cases}$$

En multipliant la seconde équation par a_n on tire des deux premières équations $a_n^2 b_{m-1}=0$. Puis, en multipliant la troisième équation par a_n^2 on obtient $a_n^3 b_{m-2}=0$. Par récurrence, il vient $a_n^{m+1} b_0 = 0$. Or on a $a_0 b_0 = 1$. Par suite $a_n^{m+1}=0$ et donc $a_n \in \mathbf{Nil}(\mathrm{A})$. À l'aide de la proposition A.2.28 on en déduit que $f - a_n X^n = \sum_0^{n-1} a_i X^i$ est une unité. On montre ainsi que tous les a_i pour $1 \leq i \leq n$ sont nilpotents. Enfin, a_0 est une unité puisque l'on a $a_0 b_0 = 1$. La réciproque est immédiate à l'aide de la proposition A.2.28.

Vérifions (ii). Si f est nilpotent, alors $1+Xf$ est une unité, d'après la proposition A.2.28. Par suite, avec (i), on en tire $a_0, \ldots, a_n$ nilpotents. La réciproque s'obtient en élevant f à une puissance assez grande.

Vérifions (iii). Supposons tout d'abord qu'il existe g non nul dans $A[X]$ tel que $fg=0$. On choisit g de degré minimal avec cette propriété. On pose $g=\sum_0^m b_j X^j$ avec $b_m \neq 0$. Soit $r \in \mathbb{N}$ tel que $0 \leq r \leq n$. On a :

$$\Big(\sum_r^n a_i X^i\Big) g \;=\; -\Big(\sum_0^{r-1} a_i X^i\Big) g$$

dont le degré est inférieur ou égal à $r-1+m$. Posons $h = (\sum_r^n a_i X^{i-r})\, g$. Supposons que h ne soit pas nul. Alors, son degré est inférieur strictement à celui de g. Or on a :

$$\Big(\sum_r^n a_i X^{i-r}\Big)\, g\, f = 0$$

C'est-à-dire :

$$hf = 0$$

Comme g est de degré minimal avec le fait d'appartenir à $0 : \langle f \rangle$, le polynôme h doit être nul. On a donc :

$$\Big(\sum_r^n a_i X^{i-r}\Big)\, g = 0$$

Pour $r=n$ on en déduit : $a_n g = 0$. Puis, pour avec $r=n-1, \ldots, r=0$, il vient :

$$a_{n-1} g = a_{n-2} g = \cdots = a_0 g = 0$$

Par suite, tous les produits $a_i b_j$ sont nuls. On en déduit la conclusion. La réciproque est immédiate. □

Proposition 3.1.5 *Soit I un idéal de l'anneau A et h un élément de A. Les propriétés ci-dessous sont alors vérifiées :*

(i) $A[X]/(I[X]) \;\simeq\; (A/I)[X]$,

(*ii*) *I premier* $\Longleftrightarrow I[X]$ *premier,*

(*iii*) $\sqrt{I[X]} = \sqrt{I}[X]$,

(*iv*) *I primaire* $\Longleftrightarrow I[X]$ *primaire,*

(*v*) $(I : h^\infty)[X] = (I[X]) : h^\infty$.

Preuve. La propriété (i) est classique. Elle s'obtient en considérant l'homomorphisme surjectif d'anneaux ϕ de $A[X]$ dans $(A/I)[X]$ défini de la manière suivante :

- $\phi(X) = X$,
- $\forall a \in A,\ \phi(a) = \overline{a}^I$.

En utilisant la proposition 3.1.2, on vérifie que ϕ a pour noyau $I[X]$ ce qui prouve (i).

On utilise l'isomorphisme ϕ pour établir les équivalences suivantes : I premier $\Longleftrightarrow A/I$ intègre $\Longleftrightarrow (A/I)[X]$ intègre $\Longleftrightarrow A[X]/(I[X])$ intègre $\Longleftrightarrow I[X]$ premier.

Soit $p \in A[X]$. En utilisant l'isomorphisme ϕ on a : $p \in \sqrt{I[X]} \Longleftrightarrow p$ est nilpotent dans $A[X]/I[X] \Longleftrightarrow p$ est nilpotent dans $(A/I)[X]$. Il résulte du point (ii) de la proposition 3.1.4 que $p \in \sqrt{I[X]}$ si et seulement si chaque coefficient de p appartient à $\sqrt{I}$, ce qui prouve la relation (iii).

Vérifions (iv). Montrons tout d'abord que si I est primaire dans A alors $I[X]$ est primaire dans $A[X]$. Il suffit d'établir que tout diviseur de zéro dans $(A/I)[X]$ est nilpotent. Soit $p = \sum_{i=0}^{d} c_i X^i \in A[X]$ dont la classe résiduelle dans $(A/I)[X]$ est un diviseur de zéro. Alors, d'après le point (iii) de la proposition 3.1.4 il existe $a \in A$ tel que

$$\overline{a}^I \neq 0 \text{ et } ap \in I[X] .$$

Comme I est primaire, on en déduit que chaque coefficient c_i de f a une puissance dans I. Ainsi, chaque $\overline{c_i}^I$ est un nilpotent dans A/I et par conséquent p est nilpotent dans $(A/I)[X]$ (voir proposition 3.1.4). Réciproquement, supposons que $I[X]$ soit primaire dans $A[X]$ et vérifions que I est primaire dans A. Soit a et b dans A avec $ab \in I$ et $b \notin I$. Nous avons aussi : $ab \in I[X]$ et $b \notin I[X]$. L'idéal $I[X]$ étant primaire, on obtient $a^m \in I[X]$ pour un entier m. On a ainsi $a^m \in I[X] \cap A$, et par conséquent $a^m \in I$ d'après la proposition 3.1.3.

Passons finalement à (v). Soit a un élément de $I : h^\infty$. Il est clair que $a \in I[X] : h^\infty$. Par conséquent l'idéal engendré par $I : h^\infty$ dans $A[X]$ est contenu dans $I[X] : h^\infty$, ce qui montre l'inclusion directe. Réciproquement, si $p = \sum_{i=1}^{d} c_i x^i \in I[X] : h^\infty$ alors il existe un entier m tel que $h^m c_i \in I$ pour tout $i \in [1, d]$. On a donc $c_i \in I : h^\infty$ pour tout i, d'où $p \in (I : h^\infty)[X]$.
□

Pour finir on rappelle le résultat bien connu ci-dessous (voir [Kap74], théorème 149) qui précise la hauteur d'un idéal premier (définition A.3.1) dans $A[X]$ selon que celui-ci est une extension ou non d'un idéal premier de A.

Proposition 3.1.6 *Soit $\mathcal{P}$ un idéal premier dans un anneau noethérien A. Soit $\mathcal{P}'$ un idéal premier dans l'anneau de polynômes $A[X]$ tel que $\mathcal{P}' \cap A = \mathcal{P}$. Alors*

- $\mathcal{P}' = \mathcal{P}[X] \Rightarrow \mathsf{ht}(\mathcal{P}') = \mathsf{ht}(\mathcal{P})$,
- $\mathcal{P}' \neq \mathcal{P}[X] \Rightarrow \mathsf{ht}(\mathcal{P}') = \mathsf{ht}(\mathcal{P}) + 1$.

3.2 Idéaux de A[X] quasi-monogènes

On introduit dans cette section des outils généraux qui s'appliquent directement par induction pour les ensembles triangulaires de polynômes. Avec la notion nouvelle d'idéal quasi-monogène régulier nous dégageons les propriétés fondamentales pour l'étude des *ensembles triangulaires réguliers* et des *chaînes régulières* présentée dans le chapitre 4. Les résultats de cette section conjugués aux propriétés de la section précédente, permettent effectivement de traiter les deux cas distingués par la construction inductive d'ensembles triangulaires dans plusieurs des preuves des résultats importants du chapitre 4. Dans toute la section A est un anneau noethérien. On notera le degré d'un polynôme p de $A[X]$ par $\mathsf{deg}(p)$. Par abus de notation, l'image d'un polynôme $p \in A[X]$ dans $(A/I)[X]$ par l'homomorphisme canonique sera désignée par $\overline{p}^I$.

Définition 3.2.1 *Soit A un anneau noethérien. On appelle* idéal quasi-monogène *de l'anneau polynomial $A[X]$ tout idéal J de $A[X]$ qui peut s'écrire*

$$J = \langle I \cup \{f\} \rangle_{A[X]}$$

où I est un idéal de A et $f \in A[X] \setminus A$. On notera alors $J = (I, f)$.

Nous étudions plus particulièrement dans cette section les propriétés de certains idéaux quasi-monogènes. Il nous faut d'abord renforcer la définition 3.2.1 pour obtenir des propriétés intéressantes. On cherche par exemple à avoir $J \cap A = I$. Cette égalité n'est évidemment pas vérifiée dans le cas général comme le montre le contre-exemple simple ci-dessous.

Exemple 3.2.2 Soit $A = \mathbb{Q}[Y]$ et $f = YX + 1$. Soit I l'idéal de A engendré par $Y^2 + Y$. L'inclusion $I \subset J \cap A$ est stricte puisque le polynôme $Y + 1 = (Y + 1)f - X(Y^2 + Y)$ est un élément de $J \cap A$, mais qu'il n'appartient pas à I. Remarquons de plus que si on prend pour I l'idéal engendré par Y^2 alors on a même $J \cap A = A$.

Définition 3.2.3 *Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène de $A[X]$. On dit que J est régulier si pour tout idéal premier $\mathcal{P}$ de A associé à I, on a $\mathsf{init}(f) \notin \mathcal{P}$.*

D'après la proposition A.1.23 il est équivalent de dire : l'idéal quasi-monogène (I, f) est régulier si $\mathsf{init}(f)$ n'est pas diviseur de zéro dans l'anneau quotient A/I.

Remarque 3.2.4 Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène de $A[X]$. Pour tout idéal premier $\mathcal{P}$ associé à I, il est clair que le degré de f modulo $\mathcal{P}$ est égal au degré de f. Il en est de même pour le degré de f modulo I.

Proposition 3.2.5 *Soit A un anneau noethérien. Pour tout idéal quasi-monogène régulier $J = (I, f)$ de $A[X]$ on a $I = J \cap A$.*

Preuve. L'inclusion directe étant triviale, il suffit de montrer que $(I, f) \cap A \subseteq I$. Soit $p \in J \cap A$. Il existe donc $r \in I[X]$ et $q \in A[X]$ tels que $p = r + qf$. Puisque $\overline{r}^I = 0$, on en conclut que

$$\overline{p}^I = \overline{q}^I \, \overline{f}^I .$$

Par hypothèse l'initial de f n'est pas diviseur de zéro modulo I. Si on suppose $\overline{q}^I \neq 0$, on a par conséquent $\mathsf{deg}(\overline{p}^I) = \mathsf{deg}(\overline{q}^I) + \mathsf{deg}(\overline{f}^I)$. Puisque $\mathsf{deg}(\overline{f}^I) > 0$ (remarque 3.2.4) on obtient $\mathsf{deg}(\overline{p}^I) > 0$, ce qui contredit le fait que p est dans l'anneau A. On a donc $\overline{q}^I = 0$ et par suite $\overline{p}^I = 0$. □

Corollaire 3.2.6 *Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène régulier de $A[X]$. On pose $h = \mathsf{init}(f)$. Alors on a $I = (J : h^\infty) \cap A$.*

Preuve. Il suffit de montrer $(J : h^\infty) \cap A \subseteq I$. Soit $a \in J : h^\infty \cap A$. Il existe un entier m tel que $h^m a$ est dans J. Puisque $h \in A$ la proposition 3.2.5 entraîne $h^m a \in I$. Le résultat découle alors du corollaire A.1.21. □

En utilisant la relation $\sqrt{J^c} = \sqrt{J}^c$ (proposition A.1.4), on obtient immédiatement les égalités suivantes.

Corollaire 3.2.7 *Sous les hypothèses du corollaire 3.2.6, on a :*

- $\sqrt{J \cap A} = \sqrt{I}$,
- $\sqrt{(J : h^\infty) \cap A} = \sqrt{I}$.

Lemme 3.2.8 *Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène régulier de $A[X]$. On pose $h = \mathsf{init}(f)$. Soit r un polynôme non nul de $A[X]$ tel que $\mathsf{deg}(r) < \mathsf{deg}(f)$. Soit $r \in J : h^\infty$ non nul tel que $\mathsf{deg}(r) < \mathsf{deg}(f)$. Alors*

$$r \in J : h^\infty \Rightarrow r \in I[X] \ .$$

Preuve. Par hypothèse, il existe un entier δ et un polynôme q tels que $h^\delta r - qf$ appartient à l'idéal engendré par I dans $A[X]$. On a donc

$$\overline{h^\delta}^I \, \overline{r}^I \ = \ \overline{q}^I \, \overline{f}^I \ . \tag{3.1}$$

Si q était non nul modulo I on aurait $\mathsf{deg}(\overline{q}^I \, \overline{f}^I) \geq \mathsf{deg}(f)$. La relation (3.1) serait alors en contradiction avec l'hypothèse $\mathsf{deg}(r) < \mathsf{deg}(f)$. On a donc $\overline{q}^I = 0$ et $\overline{h^\delta}^I \overline{r}^I = 0$. Comme J est régulier, on sait que $\overline{h}^I$ n'est pas un diviseur de zéro. Par conséquent $\overline{r}^I = 0$, ce qu'il fallait prouver. □

Proposition 3.2.9 *Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène régulier de $A[X]$. Les affirmations suivantes sont équivalentes :*

(i) $p \in J : \mathsf{init}(f)^\infty$,

(ii) $\mathsf{prem}(p, f) \in I[X]$.

Preuve. Montrons d'abord que (i) implique (ii). Puisque $f \in J : \mathsf{init}(f)^\infty$, l'hypothèse (i) entraîne $\mathsf{prem}(p, f) \in (I + \langle f \rangle) : \mathsf{init}(f)^\infty$. Le lemme 3.2.8 s'applique alors avec $r = \mathsf{prem}(p, f)$ et on obtient (ii). Prouvons maintenant l'implication réciproque. Il existe un entier $\delta \geq 0$ et $q \in A[X]$ tels que $h^\delta p = qf + \mathsf{prem}(p, f)$. Il résulte de l'hypothèse (ii) que $\mathsf{prem}(p, f) \in J$. Comme on a évidemment $f \in J$ on en conclut que $p \in J : h^\infty$. □

Proposition 3.2.10 *Soit A un anneau noethérien et $J = (I, f)$ un idéal quasi-monogène régulier de $A[X]$. Les affirmations suivantes sont équivalentes :*

(i) $p \in \sqrt{J : \mathsf{init}(f)^\infty}$,

(ii) $(\exists\, l \geq 0) \mid \mathsf{prem}(p^l, f) \in I[X]$,

(iii) $(\exists\, m \geq 0) \mid \mathsf{prem}(p^m, f) \in \sqrt{I[X]}$.

Preuve. L'équivalence $(i) \Leftrightarrow (ii)$ est une conséquence immédiate de la proposition 3.2.9. L'implication $(ii) \Rightarrow (iii)$ est triviale. Il nous suffit donc de montrer $(iii) \Rightarrow (i)$. Le principe est identique à celui de la preuve de la proposition 3.2.9 dont nous reprenons les notations. A partir de la relation $h^\delta p^m = qf + \mathsf{prem}(p^m, f)$, on obtient $h^\delta p^m \in \sqrt{J}$. Selon la proposition A.1.14 on a $\sqrt{J : h^\infty} = \sqrt{J} : h^\infty$ donc $p^m \in \sqrt{J : h^\infty}$. Il en résulte que $p \in \sqrt{J : h^\infty}$. □

La caractérisation du saturé à l'aide de la notion de pseudo-reste dans la proposition 3.2.9 entraîne la propriété suivante à l'aide de laquelle nous pourrons *scinder* des ensembles triangulaires.

Corollaire 3.2.11 *Soit A un anneau noethérien et $f \in A[X] \setminus A$ d'initial h. Soit $I_1, \ldots, I_m$ des idéaux de A et $I = \cap_{\ell=1}^m I_\ell$. On suppose que les idéaux quasi-monogènes $J = (I, f)$ et (I_ℓ, f) $(1 \leq \ell \leq m)$ sont réguliers. Alors*

$$J : h^\infty \;=\; \bigcap_{\ell=1}^{m} \left(\langle I_\ell \cup \{f\} \rangle : h^\infty \right) .$$

Preuve. Soit $p \in A[x]$. Avec les hypothèses et à l'aide la proposition 3.2.9, on a clairement les équivalences suivantes :

$$\begin{aligned} p \in J : h^\infty \quad &\Longleftrightarrow \quad \mathsf{prem}(p, f) \in I[X] \\ &\Longleftrightarrow \quad \mathsf{prem}(p, f) \in \cap_{\ell=1}^m I_\ell[X] \\ &\Longleftrightarrow \quad (\forall \ell \in [1, m]) \;\; p \in \langle I_\ell \cup \{f\} \rangle : h^\infty . \end{aligned}$$

□

Proposition 3.2.12 *Soit A un anneau noethérien et $f \in A[X] \setminus A$ d'initial h. Soit a un élément non nul de A et I' un idéal de A. On note I l'idéal $I = I' : a^\infty$. Si l'idéal quasi-monogène (I, f) est régulier alors*

$$\langle I \cup \{f\} \rangle : h^\infty \;=\; \langle I' \cup \{f\} \rangle : (ah)^\infty .$$

Preuve. On pose $J = (I, f)$. Si $p \in J : h^\infty$ alors $\mathsf{prem}(p, f) \in I[X]$ d'après la proposition 3.2.9, ce qui équivaut à $\mathsf{prem}(p, f) \in I'[X] : a^\infty$ selon la proposition 3.1.5. Par conséquent il existe un entier m tel que $a^m \mathsf{prem}(p, f) \in I'$, c'est-à-dire $\mathsf{prem}(a^m p, f) \in I'$ puisque $a \in A$ (proposition 2.1.16). Il existe un entier δ et un polynôme q tels que $h^\delta a^m p = qf + \mathsf{prem}(a^m p, f)$. On a donc $h^\delta a^m p \in \langle I' \cup \{f\} \rangle$, ce qui montre l'inclusion directe.

Réciproquement, Soit $p \in \langle I' \cup \{f\} \rangle : (ah)^\infty$. Il existe un entier m tel que $a^m p \in \langle I' \cup \{f\} \rangle : h^\infty$. Il est clair qu'on a alors $a^m p \in J : h^\infty$. D'après la proposition 3.2.9 on a $\mathsf{prem}(a^m p, f) \in I$. Puisque a est un élément de A la relation précédente équivaut à $a^m \mathsf{prem}(p, f) \in I$. Il résulte des hypothèses de départ que $I = I : a^\infty$ donc $\mathsf{prem}(p, f) \in I$. Une nouvelle application de la proposition 3.2.9 donne $p \in J : h^\infty$. On a ainsi $\langle I' \cup \{f\} \rangle : (ah)^\infty \subseteq J : h^\infty$ et finalement $\langle I' \cup \{f\} \rangle : (ah)^\infty = J : h^\infty$ □

3.3 Pgcd sur un produit de corps

Nous nous intéressons dans cette section au cas particulier où l'anneau A est un produit fini de corps et examinons comment cette structure algébrique fournit un bon support pour le calcul de pgcd de polynômes. Nous mettons effectivement en évidence plus loin que l'algorithme **ggcd** proposé dans [Kal93] calcule un pgcd sur un produit de corps. Ce fait, qui n'apparaît pas du tout dans les travaux de Kalkbrener, explique l'utilisation d'un processus à la D5 [DDD85] [DD85] dans cet algorithme. Mais ce processus est géré de façon dynamique; il distingue les cas à chaque étape du calcul de pgcd contrairement aux implantations présentées dans [Duv87] et [Gom92], qui produisent des résultats sous forme de distinctions de cas, mais celles-ci ne sont effectuées qu'après des calculs réalisés génériquement sur les polynômes à plusieurs variables. Un principe similaire de gestion dynamique pour le calcul de pgcd sur des tours d'extensions simples est explicité dans [MR95] pour les tours algébriques, puis dans [Mor97](chap. 2 et 4); mais ces méthodes nécessitent de travailler constamment dans la structure de produit de corps sous-jacente. Notre travail met donc en lumière des liens forts entre les algorithmes de calcul de pgcd de [MR95] et [Mor97] d'une part, où la structure de produit de corps intervient clairement du fait qu'elle est associée à un idéal radical, et l'algorithme **ggcd** de [Kal93] d'autre part, où cette structure de produit de corps est cachée. Nous présenterons dans la section 5.1 un nouvel algorithme pour calculer des pgcd modulo un ensemble triangulaire par gestion dynamique de scindage, qui utilise des techniques basées sur les sous-résultants.

Après l'examen de quelques propriétés de la notion de pgcd dans des produits d'anneaux principaux, nous exposons de façon non formelle le principe de base d'une gestion dynamique pour le calcul efficace de pgcd sur un produit de corps.

La notion de pgcd peut être définie de manière très générale sur un anneau quelconque comme suit :

Définition 3.3.1 *Soit a et b deux éléments d'un anneau A. On dit que a divise b s'il existe $c \in A$ tel que $b = ac$. On dit que $d \in A$ est un pgcd de a et b s'il vérifie les deux conditions suivantes :*

- *d divise a et d divise b,*
- *pour tout $d' \in A$, si d' divise a et d' divise b alors d' divise d.*

[BW93](section 1.7) dont nous avons extrait la définition ci-dessus, limite ensuite l'étude du pgcd au cas où A est un anneau intègre, en précisant que c'est dans ce cadre qu'elle présente principalement un intérêt. Un anneau de polynômes sur un produit de corps est un produit d'anneaux principaux et n'est généralement pas intègre (sauf si le produit se limite à un terme). On constatera ci-dessous que l'on dispose néanmoins dans un produit d'anneaux principaux de la plupart des propriétés du pgcd dans un anneau principal.

Proposition 3.3.2 *Le nilradical d'un produit de corps est réduit à $\{0\}$ et tout élément régulier est inversible.*

Preuve. Soit $a = (a_1, \ldots, a_m)$ un élément d'un produit de corps A. Une puissance a^m est nulle si et seulement si chaque a_j^m est nul, ce qui équivaut à chaque a_j est nul puisque a_j est élément d'un corps. Pour la seconde partie de l'affirmation, dire que a est régulier revient à dire qu'aucun des a_j n'est nul. Chaque a_j est donc inversible et ainsi a est inversible dans A. La réciproque est triviale. $\square$

Proposition 3.3.3 *Dans un produit d'anneaux $A = A_1 \times \ldots \times A_s$, les idéaux sont les idéaux $I_1 \times \ldots \times I_s$ où les I_j sont des idéaux de A_j. Les idéaux premiers sont du type $A_1 \times \ldots A_{j-1} \times \mathcal{P}_j \times A_{j+1} \ldots \times A_s$ où $\mathcal{P}_j$ est un idéal premier de A_j*

Preuve. Pour $j \in [1, s]$ on note π_j la projection de A sur l'anneau A_j et ϵ_j l'élément de A tel que $\pi_j(\epsilon_j) = 1$ et $\pi_i(\epsilon_j) = 0$ pour tout $i \neq j$. Si $I_1, \ldots, I_s$ sont des idéaux respectifs de $A_1, \ldots, A_s$, il est immédiat que le produit $I_1 \times \ldots \times I_s$ est un idéal de A. Considérons maintenant un idéal I de A et $j \in [1, s]$. L'image I_j de I par π_j est un idéal de A_j puisque π_j est un morphisme surjectif. On a ainsi $I \subseteq I_1 \times \ldots \times I_s$. Pour l'inclusion réciproque, comme I est un groupe additif il suffit de vérifier que pour tout $a_j \in I_j$ on a $a_j\epsilon_j = (0, \ldots, 0, a_j, 0, \ldots, 0) \in I$. On sait que pour tout $i \neq j$ il existe $b_i \in A_i$ tel que $\alpha = (b_1, \ldots, b_{j-1}, a_j, b_{j+1}, \ldots, b_s) \in I$. Puisque I est un idéal on a $\alpha\epsilon_j \in I$ c'est-à-dire $a_j\epsilon_j \in I$.

Supposons maintenant que I est premier. Par définition I est propre; il existe donc un indice j tel que $I_j \neq A_j$. Montrons que I_j est premier. Si a et b sont deux éléments de A_j tels que $ab \in I_j$ alors $ab\epsilon_j \in I$ donc $a\epsilon_j \in I$ ou $b\epsilon_j \in I$, autrement dit $a \in I_j$ ou $b \in I_j$. Il reste à prouver que pour tout indice $i \neq j$ on a $I_i = A_i$. Supposons le contraire et prenons $i = 1 < j$pour simplifier l'écriture. Pour $a \in I_1$ et $b \in I_j$ on a alors $(1, 0, \ldots, 0, b, 0, \ldots) \notin I$ et $(a, 0, \ldots, 0, 1, 0, \ldots) \notin I$. Le produit de ces deux éléments $(a, 0, \ldots, 0, b, 0, \ldots)$ est dans I, ce qui contredit l'hypothèse que I est premier. $\square$

Proposition 3.3.4 *Dans un produit d'anneaux à idéaux principaux tous les idéaux sont principaux.*

Preuve. En utilisant les notations de la proposition 3.3.3, si $I_j = \langle a_j \rangle$ pour tout $j \in [1, s]$ alors il est clair que $I = \langle a \rangle$ avec $a = (a_1, \ldots, a_s)$. $\square$

Lemme 3.3.5 *Si $I = I_1 \times \ldots \times I_s$ est un idéal dans un produit fini d'anneaux $A_1 \times \ldots \times A_s$, on a $\sqrt{I} = \sqrt{I_1} \times \ldots \times \sqrt{I_s}$. En particulier, I est radical si et seulement si les I_j le sont.*

Preuve. On le montre pour $s = 2$. Le cas général s'en déduit aisément. Soit $a_1 \in A_1$ et $a_2 \in A_2$. Si $(a_1, a_2) \in \sqrt{I}$ alors il existe un entier m tel que $(a_1^m, a_2^m) \in I_1 \times I_2$, donc $(a_1, a_2) \in \sqrt{I_1} \times \sqrt{I_2}$. Réciproquement il existe des entiers m et p tels que $(a_1^m, a_2^p) \in I$. En multipliant par (a_1^p, a_2^m) on a $(a_1, a_2)^{m+p} \in I$ donc $(a_1, a_2) \in \sqrt{I}$. $\square$

Le lemme suivant est trivial.

Lemme 3.3.6 *Soit $A = A_1 \times \ldots \times A_s$ un produit d'anneaux. Alors l'anneau $A[X]$ est isomorphe à $A_1[X] \times \ldots \times A_s[X]$.*

L'intérêt de travailler sur un produit de corps est d'avoir une notion de pgcd dans $A[X]$ similaire à celle dont on a l'habitude sur un corps. En particulier, tout couple d'éléments de $A[X]$ admet un pgcd et on dispose de plus d'une relation de Bezout.

Lemme 3.3.7 *Soit A un produit d'anneaux intègres. Soit a et b deux éléments de A qui admettent un pgcd g. Alors un élément g' de A est un pgcd de a et b si et seulement si g et g' sont associés.*

Preuve. Si g etg' sont deux pgcd de a et b alors g divise g' et g' divise g. On en déduit facilement qu'il existe u et v tels que $g = ug' = uvg$, d'où $(1 - uv)g = 0$. En notant w_i la i-ème composante d'un élément $w \in A$ on a soit $1 - u_i v_i = 0$ et alors $u'_i = u_i$ est inversible dans A_i, soit $g_i = 0$ et alors $g'_i = 0$; dans ce cas on choisit $u'_i = 1$ et on a $g = u'g'$ avec u' inversible, ce qui prouve l'implication directe. La contraposée provient du fait que deux éléments associés satisfont les mêmes relations de divisiblité avec tout élément de A. □

La proposition suivante est une extension d'une propriété bien connue pour les anneaux principaux au cas de produits d'anneaux principaux .

Proposition 3.3.8 *Soit a et b des éléments d'un produit d'anneaux principaux $A = A_1 \times \ldots \times A_s$. Alors a et b admettent un pgcd $g \in A$ tel que $\langle a, b\rangle = \langle g\rangle$. En particulier, il existe s et t dans A tels que $g = sa + tb$.*

Preuve. Pour toute composante A_i de A il existe $g_i \in A_i$ tel que $\langle a_i, b_i\rangle_{A_i} = \langle g_i\rangle_{A_i}$. Il suffit de prendre $g = (g_1, \ldots, g_s)$. □

De plus, si f est un élément de A tel que $\langle a, b\rangle = \langle f\rangle$, on vérifie immédiatement à l'aide de la proposition 3.3.7 que f est un pgcd de a et b.

Dans ce qui suit, la dérivée d'un polynôme $p \in A[X]$ est notée p'.

Proposition 3.3.9 *Soit $A = k_1 \times \ldots \times k_s$ un produit de corps et p un polynôme unitaire de $A[X]$. Si $\langle p, p'\rangle = A[X]$ alors l'idéal engendré par p dans $A[X]$ est radical.*

Preuve. Notons p_j l'image de p modulo k_j. Puisque p est unitaire le degré de p_j est égal au degré de p; en particulier p_j n'est pas nul. Puisque 1 est un pgcd de p et p', alors dans chaque anneau $k_j[X]$ le pgcd de p_j et p'_j est 1. Par conséquent les polynômes p_j sont séparables et les idéaux $\langle p_j\rangle_{k_j[X]}$ sont radicaux. Il résulte du lemme 3.3.5 que l'idéal engendré par p est radical. □

Supposons que $A = k_1 \times \ldots \times k_s$ soit un produit de corps. Nous avons vu que tout couple de polynômes de $A[X]$ admet un pgcd et que $g = (g_1, \ldots, g_s) \in k_1[X] \times \ldots \times k_s[X]$ est un pgcd de $a = (a_1, \ldots, a_s)$ et $b = (b_1, \ldots, b_s)$ si et seulement si pour tout j la composante g_j est un pgcd de a_j et b_j dans $k_j[X]$.

Soit (a, b) un couple d'éléments de $A[X]$. Puisqu'on sait calculer un pgcd de a_j et b_j sur chaque corps k_j, avec l'algorithme d'Euclide par exemple, on peut donc calculer un pgcd de a et b dans $A[X]$. Mais il faut effectuer s calculs de pgcd, ce qui devient lourd quand s grandit. De plus, cela suppose qu'on a la connaissance explicite des différents corps. Or, savoir qu'un anneau est un produit de corps n'implique pas qu'on connaisse tous ces corps. Nous serons confrontés à ce problème majeur plus loin. Bien qu'en ce qui nous concerne les corps puissent être calculés, cela nécessite des factorisations sur des extensions de corps; il est préférable d'éviter ces calculs coûteux.

Le principe introduit dans [DDD85] consiste à calculer sur A comme si c'était un corps tout en effectuant des *scindages* de ce produit de corps uniquement lorsqu'un diviseur de zéro est rencontré. En général A sera associé à un idéal de $\mathbf{P}_{n-1}$ et les polynômes a et b seront représentés par des polynômes de $\mathbf{P}_n$. Sur le plan pratique, on peut calculer le pgcd de a et b sur $\mathbf{P}_{n-1}$ par la technique des sous-résultants, puis remonter dans la suite des sous-résultants calculés pour déceler de possibles diviseurs de zéro en spécialisant. Il est plus efficace de gérer dynamiquement cette distinction de cas à chaque étape du calcul de pgcd. Nous en expliquons le principe ci-dessous sur un calcul de type euclidien pour en faciliter la compréhension.

Notons h l'initial du polynôme b. Effectuons la pseudo-division de a par b dans $A[X]$. Il existe deux polynômes q et r tels que

$$h^m a = bq + r$$

avec r nul ou de degré strictement plus petit que $\mathsf{deg}(b)$. De plus, si h n'est pas diviseur de zéro dans A alors q et r sont uniques (on pourra se référer à [SZ67] p. 30). Dans un produit de corps, cela correspond au cas où aucune composante de h n'est nulle; on sait qu'alors h est inversible dans A donc la relation ci-dessus entraîne que $a \in \langle b, r \rangle$. On a encore $r \in \langle a, b \rangle$, d'où $\langle b, r \rangle = \langle a, b \rangle$.

En réitérant le processus ci-dessus comme on le fait classiquement sur un corps, on obtient un pgcd de a et b. Il suffit donc de savoir gérer le cas où h est diviseur de 0 dans A, c'est-à-dire lorsque l'image de h est nulle dans au moins un corps k_j. Sans perte de généralité on peut supposer que h est nul dans $k_1, \ldots, k_r$ et h non nul dans $k_{r+1}, \ldots, k_s$ avec $r \in [1, s-1]$. On pose alors

$$B = k_1 \times \ldots \times k_r$$

et

$$B' = k_{r+1} \times \ldots \times k_s \ .$$

L'image de h dans $B[X]$ est nulle. On a par conséquent

$$\langle a, b \rangle_{B[X]} = \langle a, \mathsf{tail}(b) \rangle_{B[X]} \ .$$

Par induction on trouve dans $B[X]$ un pgcd g_B de a et $\mathsf{tail}(b)$ tel que

$$\langle a, b \rangle_{B[X]} = \langle g_B \rangle_{B[X]} \ .$$

D'autre part h est inversible dans B'; on se retrouve donc dans le cas étudié au début. Là encore, on pourra déterminer $g_{B'} \in B'[X]$ tel que

$$\langle a, b \rangle_{B'[X]} = \langle g_{B'} \rangle_{B'[X]} \ .$$

L'isomorphisme $A[X] \simeq B[X] \times B'[X]$ permet de définir un polynôme $g \in A[X]$ d'images respectives g_B et $g_{B'}$ dans $B[X]$ et $B'[X]$. Il est clair alors que

$$\langle a, b \rangle_{A[X]} = \langle g \rangle_{A[X]} \ .$$

On a ainsi obtenu un pgcd de a et b dans $A[X]$ sans calculer de pgcd sur chaque corps.

Remarquons que le processus présenté ci-dessus permet en fait de calculer des polynômes $g_1, \ldots, g_r$ et des produits de corps $A_1, \ldots, A_r$ tels que A est isomorphe au produit $A_1 \times \ldots \times A_r$ et g_i est unitaire sur A_i pour tout $i \in [1, r]$. Cette propriété qu'utilisent les algorithmes de calcul de pgcd modulo un ensemble triangulaire permet alors de scinder la résolution d'un système algébrique en plusieurs branches.

Chapitre 4

Propriétés des ensembles triangulaires

Résumé

Les ensembles triangulaires de polynômes apparaissent dans de nombreux articles traitant des systèmes d'équations algébriques. Ritt introduit en 1932 la notion d'ensemble caractéristique pour certains ensembles triangulaires [Rit32] et donne dans [Rit66] un algorithme de décomposition de systèmes algébriques à l'aide de calcul d'ensembles caractéristiques et de factorisation dans des extensions de corps. Plus récemment, l'algorithme présenté par Wu [Wu86] [Wu87] calcule des ensembles caractéristiques (dans un sens différent de celui de Ritt) qui n'engendrent pas forcément un idéal premier. Cette approche a été poursuivie et améliorée par de nombreux auteurs principalement dans [CG90], [CG91], [CG92], [GM90], [GM91], [Wan92b], [Wan93a], [Wan95] .

Un nouveau type d'ensembles triangulaires, appelés *chaînes régulières*, a été introduit d'une part dans [YZ94], et d'autre part dans [Kal93], qui tire parti de propriétés des chaînes régulières pour présenter un algorithme de décomposition de variétés algébriques en variétés équidimensionnelles décrites par des chaînes régulières. La notion d'ensemble triangulaire normalisé séparable est introduite dans [Laz91a], qui propose une méthode décomposant l'ensemble des solutions d'un système algébrique en *zéros réguliers* de tels ensembles triangulaires. Ce travail est prolongé dans [Mor97] qui présente le concept de tour d'extensions simples. Récemment, [Wan98] donne une généralisation de la notion de chaîne régulière à des paires d'ensembles polynomiaux (le premier pour les équations et le second pour les inéquations) dont l'union est un ensemble triangulaire. De telles paires sont appelées *systèmes simples*. Il présente en même temps un algorithme de résolution de systèmes polynomiaux dont les sorties sont des systèmes simples.

Toutes les théories mentionnées ci-dessus sont assez proches les unes des autres. La situation est plutôt confuse car beaucoup de notions légèrement différentes peuvent apparaître d'un article à l'autre sous le même nom (ou au contraire, un nom complètement différent). Avec M. Moreno Maza [AM97], puis avec D. Lazard et M. Moreno Maza [ALM99], nous avons essayé de clarifier cette situation, et d'établir des liens entre les types d'ensembles triangulaires utilisés dans différentes approches. Ce chapitre reprend, corrige et prolonge ce travail.

Certaines preuves sont ici plus simplement obtenues à partir du cadre plus général du chapitre 3. Ce sont en effet les propriétés du concept d'idéal quasi-monogène régulier présenté

dans le chapitre 3 qui sont la base inductive du théorème 4.3.11 et des résultats concernant les idéaux d'élimination d'une chaîne régulière et de ses idéaux premiers associés (théorèmes 4.3.4 et 4.3.6).

Dans la section 1, nous montrons l'équidimensionnalité du saturé d'un ensemble triangulaire consistant et nous nous intéressons à ses idéaux d'élimination. Ce nouveau résultat, plus précis que celui de [CG93] nous permet de valider l'équivalence des notions de chaîne régulière et d'ensemble triangulaire régulier.

La section 2 rappelle ce qui a trait aux ensembles caractéristiques de Ritt et la façon dont Wu les utilise.

Nous introduisons dans la section 3 la notion d'ensemble régulier. Les résultats du chapitre 3 permettent d'obtenir des propriétés fondamentales qui caractérisent les ensembles réguliers. Précisons que nous avons aussi voulu simplifier autant que possible les définitions. Dans cette optique, la définition d'*ensemble triangulaire régulier* (4.3.3) nous paraît assez compacte et claire. La cohérence avec la définition plus lourde employée dans [AM97] et [ALM99] est assurée par les résultats de la section 4.5.

La section 4 rappelle d'abord la façon dont Kalkbrener définit les chaînes régulières et leur *représentation*. Ce fut une de nos premières préoccupations que de préciser ce que recouvraient exactement ces deux notions. Kalkbrener les définit simultanément d'une façon inductive qui présente des inconvénients. Il est difficile de comprendre au premier abord les objets algébriques sur lesquels opéreront les algorithmes; les spécifications de ces derniers sont alors obscures. Or, il faut maîtriser ces points si on veut obtenir une implantation et une optimisation efficaces. Nous montrons ainsi que la représentation d'une chaîne régulière correspond au radical de son saturé (théorème 4.4.11). Grâce au théorème d'équidimensionnalité de la section 1, on en déduit qu'une chaîne régulière peut être définie plus simplement comme un ensemble triangulaire régulier. L'isomorphisme que nous établissons dans le théorème 4.4.14 montre ensuite que la structure algébrique sur laquelle les algorithmes de Kalkbrener travaillent implicitement est un produit de corps. Comme nous l'avons exposé dans la section 3.3, tout couple de polynômes sur un produit de corps admet un pgcd. Nous donnons ainsi une validation mathématique de l'algorithme ggcd de [Kal93]. Ce résultat fait de plus clairement apparaître les similitudes de structures algébriques avec les algorithmes de [Laz91a] et [Mor97] qui travaillent explicitement sur des produits de corps.

Dans la section 5 nous associons à tout ensemble triangulaire une suite d'anneaux de fractions. Nous montrons que si l'ensemble est régulier alors cette suite est une tour d'extensions simples au sens de [Mor97]. Réciproquement, toute tour d'extensions simples peut être associée à un ensemble triangulaire régulier. L'ensemble de cette section nous permet de donner une version corrigée de la preuve du théorème 5.1 de [ALM99] (voir la proposition 4.5.7).

La section 6 présente l'unification de concepts provenant de théories différentes par l'équivalence de plusieurs propriétés dans le théorème 4.6.1. On y trouvera une nouvelle caractérisation d'une chaîne régulière qui n'apparaissait pas dans [ALM99].

Nous terminons par une étude des relations entre ensembles triangulaires et bases de Gröbner où nous obtenons des résultats plus forts que dans [ALM99]. On constate qu'on peut obtenir facilement à partir d'une base de Gröbner lexicographique d'un idéal au moins un ensemble caractéristique de Ritt de cet idéal. Et dans le cas où l'idéal est premier, il est encore plus facile d'extraire de la base de Gröbner un ensemble triangulaire régulier.

4.1 Équidimensionnalité

L'objectif de cette section est de montrer que si T est un ensemble triangulaire de $\mathbf{P}_n$ alors l'idéal $\mathsf{sat}(T)$ est fortement équidimensionnel (voir la définition A.3.6) lorsqu'il ne correspond pas à l'anneau $\mathbf{P}_n$ tout entier. Ce résultat est nouveau et plus précis que celui de [CG93] qui affirme uniquement que $\mathsf{sat}(T)$ est équidimensionnel lorsque c'est un idéal propre. C'est en particulier la clé qui est nécessaire pour donner une preuve correcte de l'équivalence des notions de chaîne régulière (définition 4.4.5) et d'ensemble triangulaire régulier (définition 4.3.3) qui est affirmée dans [AM97], [Mor97] et [ALM99].

L'idée est d'utiliser les propriétés des suites régulières (voir la section A.4) en passant dans un anneau de fractions (voir la section A.2). Dans toute la section on considère un ensemble triangulaire $T = \{f_1, \ldots, f_s\}$ de $\mathbf{P}_n$. Pour tout $j \in [1, s]$, on pose $h_j = \mathsf{init}(f_j)$. On désigne par S la partie multiplicative engendrée par $h_1, \ldots, h_s$, c'est-à-dire l'ensemble des produits finis $h_1^{m_1} \ldots h_s^{m_s}$. On utilisera les notations usuelles d'extension et de contraction introduites dans la section A.2 pour les idéaux de $\mathbf{P}_n$ et $S^{-1}\mathbf{P}_n$.

Lemme 4.1.1 *Avec les hypothèses énoncées ci-dessus, on note I l'idéal engendré par T dans $\mathbf{P}_n$. Alors $I^{ec} = \mathsf{sat}(T)$.*

Preuve. Soit $I = \cap_{i=1}^{s} Q_i$ une décomposition primaire minimale de I. On note $\mathcal{P}_i = \sqrt{Q_i}$ et $h = \prod_{f \in T} \mathsf{init}(f)$. On sait avec la proposition A.2.22 que

$$I^{ec} = \bigcap_{\mathcal{P}_i \cap S = \emptyset} Q_i \ . \tag{4.1}$$

D'autre part, la proposition A.1.20 donne la relation

$$\mathsf{sat}(T) = \bigcap_{h \notin \mathcal{P}_i} Q_i \ . \tag{4.2}$$

Remarquons que $h \in S$. Si $S \cap \mathcal{P}_i = \emptyset$ on a donc $h \notin \mathcal{P}_i$. Supposons maintenant que $h \notin \mathcal{P}_i$. Pour tout $f \in T$ on a alors $\mathsf{init}(f) \notin \mathcal{P}_i$. Il en résulte immédiatement, par construction de S, que pour tout $s \in S$ on a $s \notin \mathcal{P}_i$. Ainsi $h \notin \mathcal{P}_i$ si et seulement si $S \cap \mathcal{P}_i = \emptyset$, d'où l'égalité des décompositions (4.1) et (4.2) ci-dessus. □

Proposition 4.1.2 *Avec les hypothèses ci-dessus, on note $\lambda_S(f)$ l'image dans $S^{-1}\mathbf{P}_n$ d'un polynôme $f \in \mathbf{P}_n$. Si $\mathsf{sat}(T) \neq \mathbf{P}_n$ alors $\lambda_S(f_1), \ldots, \lambda_S(f_s)$ est une suite régulière de $S^{-1}\mathbf{P}_n$.*

Preuve. Soit I l'idéal engendré par T dans $\mathbf{P}_n$. Posons $A = S^{-1}\mathbf{P}_n$. Alors l'idéal engendré par les $\lambda_S(f_j)$ dans A est I^e. Il nous faut d'abord montrer que $I^e \neq A$. Si ce n'était pas le cas, le lemme 4.1.1 entraînerait l'égalité $\mathsf{sat}(T) = I^{ec} = \mathbf{P}_n$, ce qui serait en contradiction avec l'hypothèse. Il reste à prouver que pour tout $j \in [1, s]$, l'image de $\lambda_S(f_j)$ dans $A/\langle \lambda_S(f_1), \ldots, \lambda_S(f_{j-1}) \rangle$ n'est pas un diviseur de zéro. C'est trivial pour $j = 1$. Supposons $j > 1$; il suffit de montrer que $\lambda_S(f_j)$ n'appartient à aucun idéal premier associé à $\langle \lambda_S(f_1), \ldots, \lambda_S(f_{j-1}) \rangle$. Soit $\mathcal{P}$ un idéal premier associé à $\langle f_1, \ldots, f_{j-1} \rangle$ tel que $S \cap \mathcal{P} = \emptyset$. On a ainsi $h_j = \mathsf{init}(f_j) \notin \mathcal{P}$. Notons i_j la variable principale de f_j; en remarquant que $\mathcal{P} = (\mathcal{P} \cap \mathbf{P}_{i_{j-1}})\mathbf{P}_n = (\mathcal{P} \cap \mathbf{P}_{i_j - 1})\mathbf{P}_n$, on en déduit $f_j \notin \mathcal{P}$. La relation entre les idéaux premiers associés à $\langle f_1, \ldots, f_{j-1} \rangle$ et ceux associés à $\langle \lambda_S(f_1), \ldots, \lambda_S(f_{j-1}) \rangle$ (voir corollaire A.2.24) assure alors le résultat. □

La proposition 4.1.3 et le théorème 4.1.4 ci-dessous établissent l'équidimensionnalité pure des saturés pour des ensembles triangulaires consistants. Nous complétons donc le résultat de [CG93] qui affirme que le saturé d'un ensemble triangulaire T est équidimensionnel, autrement dit que le radical de T est équidimensionnel.

Proposition 4.1.3 *Soit $T = \{f_1, \ldots, f_s\}$ un ensemble triangulaire de $\mathbf{P}_n$. Si $\mathsf{sat}(T)$ est un idéal propre de $\mathbf{P}_n$ alors il est purement équidimensionnel de hauteur s.*

Preuve. Soit $\mathcal{P}$ un idéal premier associé à $\mathsf{sat}(T)$. Alors $\mathcal{P}^e$ est un idéal premier associé à $\mathsf{sat}(T)^e$ (voir corollaire A.2.24). En notant I l'idéal engendré par T dans $\mathbf{P}_n$, il résulte de l'égalité du lemme 4.1.1 que $\mathcal{P}^e$ est un idéal premier associé à $I^e = I^{ece}$. Or l'idéal I^e est engendré par la suite régulière $\lambda_S(f_1), \ldots, \lambda_S(f_s)$ de la proposition 4.1.2. En utilisant le fait que $\mathbf{P}_n$ est un anneau de Macaulay et que le passage à un anneau de fractions conserve cette propriété (proposition A.4.11), le théorème A.4.12 assure que la hauteur de $\mathcal{P}^e$ est s. On en conclut que $\mathsf{ht}(\mathcal{P}) = s$ avec la proposition A.3.8. $\square$

Théorème 4.1.4 *Tout ensemble triangulaire consistant $T = \{f_1, \ldots, f_s\}$ de $\mathbf{P}_n$ est fortement équidimensionnel. De plus, pour tout idéal premier $\mathcal{P}$ associé à $\mathsf{sat}(T)$, on a $\mathsf{ht}(\mathcal{P} \cap \mathbf{P}_i) = \mathrm{card}(T \cap \mathbf{P}_i)$ pour tout $i \in [0, n]$.*

Preuve. Soit $\mathcal{P}$ un idéal premier de $\mathsf{sat}(T)$. Pour tout $j \in [0, s]$, on note i_j la variable principale de f_j et on pose $\mathcal{Q}_j = (\mathcal{P} \cap \mathbf{P}_{i_j})[x_{i_j+1}, \ldots, x_n]$. Puisque $\mathcal{Q}_s = \mathcal{P}$, les $\mathcal{Q}_j$ sont des idéaux premiers dont l'intersection avec S est vide. On obtient donc dans $S^{-1}\mathbf{P}_n$ la chaîne suivante d'idéaux premiers

$$\langle 0 \rangle = \mathcal{Q}_0^e \subseteq \mathcal{Q}_1^e \cdots \subseteq \mathcal{Q}_s^e = \mathcal{P}^e \ . \tag{4.3}$$

Nous affirmons que les inclusions de (4.3) sont strictes. En effet, on remarque trivialement d'une part que $\lambda_S(f_j) \in \mathcal{Q}_j^e$ pour tout $j \in [1, s]$. D'autre part $\lambda_S(f_j) \notin \mathcal{Q}_{j-1}^e$ car sinon, on a $f_j \in \mathcal{Q}_{j-1}$ (par la proposition A.2.16) donc $\mathsf{init}(f_j) \in \mathcal{Q}_{j-1} \subseteq \mathcal{P}$, ce qui contredit le fait que $\mathsf{init}(f_j) \in S$.

Étant donné que $\mathsf{ht}(\mathcal{P}^e) = s$, la chaîne d'idéaux (4.3) est maximale. On en conclut facilement que $\mathsf{ht}(\mathcal{Q}_j^e) = j$ puis $\mathsf{ht}(\mathcal{Q}_j) = j$ (proposition A.3.8) pour tout j. Il résulte alors de la proposition 3.1.6 que $\mathsf{ht}(\mathcal{P} \cap \mathbf{P}_{i_j}) = j$ pour tout $j \in [0, s]$. Le résultat se généralise alors aux autres idéaux $\mathcal{P} \cap \mathbf{P}_i$ en utilisant le fait qu'il existe $j \in [0, s]$ tel que

$$\mathcal{Q}_{i_j} \subseteq (\mathcal{P} \cap \mathbf{P}_i)[x_{i+1}, \ldots, x_n] \subseteq \mathcal{Q}_{i_{j+1}} \ .$$

$\square$

Le théorème 4.1.4 a pour conséquence immédiate que $\mathsf{sat}(T) \cap \mathbf{P}_i$ n'a que des composantes primaires isolées (voir la proposition A.3.7). On en déduit sans peine ce qui suit.

Corollaire 4.1.5 *Avec les hypothèses du théorème 4.1.4, on a*

$$\mathsf{ass}(\mathsf{sat}(T) \cap \mathbf{P}_i) = \mathsf{ass}(\sqrt{\mathsf{sat}(T)} \cap \mathbf{P}_i) = \{\mathcal{P} \cap \mathbf{P}_i \ | \ \mathcal{P} \in \mathsf{ass}(\mathsf{sat}(T))\} \ ,$$

où $\mathsf{ass}(I)$ désigne l'ensemble des idéaux premiers associés à un idéal I d'un anneau noethérien (définition A.1.18).

Remarque 4.1.6 Malgré le théorème 4.1.4 on n'est pas pleinement satisfait. On aimerait disposer sur le saturé de propriétés plus fortes du type de celles qu'on trouve avec les bases de Gröbner . On sait par exemple que si G est une base de Gröbner minimale de $\mathbf{P}_n$ alors l'idéal $\langle G\rangle = \mathbf{P}_n$ si et seulement si $G = \{1\}$ ou encore

$$\langle G\rangle \cap \mathbf{P}_i = \langle G \cap \mathbf{P}_i\rangle_{\mathbf{P}_i} \ . \tag{4.4}$$

Or certains ensembles triangulaires ne sont pas consistants. Et lorsqu'ils sont consistants, on n'a pas de relation similaire à (4.4) sur le saturé. On constate par exemple avec l'ensemble triangulaire $T = \{x_1^2 - x_1, x_1x_2 - 1\}$ que

$$\mathsf{sat}_1(T \cap \mathbf{P}_1) = \langle x_1^2 - x_1\rangle$$

ne correspond pas à

$$\mathsf{sat}(T) \cap \mathbf{P}_1 = \langle x_1 - 1\rangle \ .$$

Ce phénomène est à mettre en rapport avec ce qui se passe pour la notion d'idéal quasi-monogène présentée dans le chapitre 3 où il suffit d'ajouter une condition pour bénéficier cette fois de bonnes propriétés. Nous verrons plus bas qu'il en va de même pour les ensembles triangulaires.

4.2 Ensembles caractéristiques

Les ensembles caractéristiques forment une famille particulière d'ensembles triangulaires. [Rit32] a introduit le concept d'ensemble caractéristique d'un ensemble fini ou infini de polynômes différentiels. Un de ses objectifs était de fournir une méthode pour résoudre des systèmes d'équations différentielles. Un sous-produit de ce travail consiste en un algorithme de décomposition de systèmes polynomiaux au moyen d'ensembles triangulaires (voir p. 95 dans [Rit66]). Plus précisément, étant donnée une partie finie F de $\mathbf{P}_n$, cet algorithme calcule des ensembles caractéristiques d'idéaux premiers tels que :

$$\mathbf{V}(F) = \cup_1^\ell \mathbf{W}(T_i).$$

Les ensembles caractéristiques d'idéaux premiers présentent de bonnes propriétés (voir le théorème 4.7.4) mais le processus de Ritt entraîne des factorisations dans des extensions de corps qui peuvent s'avérer coûteuses. Wu a utilisé plus tard les travaux de Ritt pour donner une méthode de résolution de systèmes polynomiaux à l'aide d'ensembles triangulaires qui ne fait pas intervenir de factorisation et nécessite uniquement des calculs de pseudo-divisions. Il obtient ainsi une décomposition du type $\mathbf{V}(F) = \cup_1^\ell \mathbf{W}(T_i)$ mais les ensembles T_i y ont des propriétés plus faibles que dans l'algorithme de décomposition de Ritt. La méthode de Wu est basée sur une procédure nommée CHRST-REM (voir p. 3 dans [Wu87]). Étant donnée une partie finie F de $\mathbf{P}_n$, cette procédure calcule un ensemble caractéristique T d'un sous-ensemble fini G de $\mathbf{P}_n$ vérifiant $\langle F\rangle = \langle G\rangle$. Mais l'ensemble T n'est pas forcément un ensemble caractéristique de l'idéal F. Un inconvénient majeur réside dans le fait que F peut engendrer l'idéal unité de $\mathbf{P}_n$ sans que la procédure CHRST-REM ne le découvre. On pourra aussi obtenir dans la décomposition fournie par la méthode de Wu des composantes superflues. Le lecteur trouvera des illustrations de ces problèmes parmi les exemples du chapitre 7. Mentionnons tout de même que [CG92] montre d'une part que l'algorithme de Wu calcule une décomposition en composantes équidimensionnelles ou vides, et d'autre part on y donne un moyen de supprimer ces composantes vides. Wu a ainsi utilisé la terminologie d'ensemble caractéristique dans une situation plus générale que celle où Ritt l'employait. Mais il n'a pas donné de définition précise en ce qui le concerne; [Wu87] définit un ensemble caractéristique comme le résultat de l'algorithme CHRST-REM. Remarquons que ce résultat dépend de l'ordre dans lequel les polynômes d'entrée sont pris en compte. En prenant en compte la façon dont fonctionne l'algorithme CHRST-REM, nous proposons ci-dessous la définition 4.2.2 pour un ensemble caractéristique au sens de Wu.

Les calculs d'ensembles caractéristiques de Wu sont basés sur l'ordre de Ritt pour les ensembles triangulaires réduits précisé en page 4 de [Rit66]. Dans la définition 4.2.5 nous généralisons cet ordre pour des ensembles triangulaires standards (voir la définition 2.2.14). dans l'optique du théorème 4.6.1 qui précise l'équivalence de plusieurs notions d'ensemble triangulaire. Avec cette modification, nous rappelons la définition d'un ensemble caractéristique au sens de Ritt (définition 4.2.8) et leurs propriétés principales (proposition 4.2.10 et théorème 4.2.11). Le contenu de cette section est classique, mais les résultats généralement donnés pour des ensembles caractéristiques réduits sont ici établis pour des ensembles triangulaires standards.

Notation 4.2.1 *Dans cette section F désigne un sous-ensemble non vide de polynômes non nuls de $\mathbf{P}_n$.*

Définition 4.2.2 *Un sous-ensemble T de $\langle F\rangle$ est un* ensemble caractéristique de Wu *de F si l'une des conditions ci-dessous est satisfaite :*

(i) $T = \{a\}$ *où* $a \in k \setminus \{0\}$,

(ii) T *est un ensemble triangulaire et il existe un sous-ensemble* G *de* $\langle F\rangle$ *tel que* $\langle F\rangle = \langle G\rangle$ *et* $G \subseteq \mathsf{red}_{\mapsto 0}(T)$.

Proposition 4.2.3 *Soit $T = \{t_1, \ldots, t_\ell\}$ un ensemble triangulaire de $\mathbf{P}_n$. On désigne par c_k l'initial de t_k. Si T est un ensemble caractéristique de Wu de F alors on a :*

(i) $\langle F\rangle \subseteq \mathsf{sat}(T)$

(ii) $\overline{\mathbf{W}(T)} \subseteq \mathbf{V}(F) \subseteq \mathbf{V}(T)$

(iii) $\mathbf{V}(F) = \mathbf{W}(T) \cup \cup_{k=1}^{l} \mathbf{V}(F \cup \{c_k\})$

(iv) Si $\langle F\rangle$ *est un idéal premier et si* $\mathbf{W}(T) \neq \emptyset$ *alors* $\mathbf{V}(F) = \overline{\mathbf{W}(T)}$.

Preuve. La propriété (i) se déduit rapidement de la proposition 2.2.18. Par passage aux variétés associées, on obtient $\mathbf{V}(\mathsf{sat}(T)) \subseteq \mathbf{V}(F)$, c'est-à-dire $\overline{\mathbf{W}(T)} \subseteq \mathbf{V}(F)$ (voir théorème 2.2.21). Le point (ii) en résulte immédiatement puisque la seconde inclusion est triviale. On peut alors affirmer que

$$\mathbf{W}(T) \cup \cup_1^l \mathbf{V}(F \cup \{c_k\}) \subseteq \mathbf{V}(F) \,.$$

Réciproquement, soit $\zeta \in \mathbf{V}(F)$. Supposons que ζ n'appartienne pas à $\mathbf{W}(T)$. Puisqu'on a $\mathbf{W}(T) \subseteq \mathbf{V}(F) \subseteq \mathbf{V}(T)$, alors ζ est un zéro de T qui annule un initial c_k. Par conséquent $\zeta \in \mathbf{V}(F \cup \{c_k\})$, ce qui clôt la preuve de (iii). Supposons finalement que F engendre un idéal premier et que $\overline{\mathbf{W}(T)} \neq \emptyset$. Notons V la variété $\cup_1^l \mathbf{V}(F \cup \{c_k\})$. La relation (iii) entraîne $\mathbf{V}(F) = \overline{\mathbf{W}(T)} \cup V$. Soit ζ un zéro régulier de T. Il est clair que V ne contient pas ζ. La variété $\mathbf{V}(F)$ étant par hypothèse irréductible, on en déduit $\mathbf{V}(F) = \overline{\mathbf{W}(T)}$. □

Remarque 4.2.4 Soit F et T définis comme ci-dessus. L'ensemble triangulaire T peut être un ensemble caractéristique de F au sens de Wu même si F engendre l'idéal unité de $\mathbf{P}_n$. Choisissons par exemple $F = \{x_2^2 - x_1, x_1x_3^2 - 2x_2x_3 + 1, (x_2x_3 - 1)x_4 + x_2^2\}$. L'ensemble F est triangulaire. C'est un ensemble caractéristique de Wu de lui-même, mais on a $\langle F \rangle = \langle 1 \rangle$. En effet, puisque tout zéro de F vérifie $x_2^2 = x_1$ on déduit de la deuxième équation que $x_2x_3 - 1 = 0$ puis de la troisième que $x_2 = 0$, ce qui contredit la condition précédente.

Définition 4.2.5 *Soit $T = \{t_1, \ldots, t_\ell\}$ et $S = \{s_1, \ldots, s_k\}$ deux ensembles triangulaires standards de $\mathbf{P}_n$. On dit que T est* plus petit que S pour l'ordre de Ritt*, et on écrit $T \prec_r S$ si l'une des conditions suivantes est vérifiée :*

(i) $(\exists i \in \{1, \ldots, \min(k, \ell)\})\ (\forall j \in \{1, \ldots, i-1\})\ t_j \sim_r s_j \quad \text{et} \quad t_i <_r s_i$

(ii) $\ell > k$ et $(\forall j \in \{1, \ldots, k\})\ t_j \sim_r s_j$

On dit que T est plus grand que S *pour l'ordre de Ritt et on écrit $T \succ_r S$ si $S \prec_r T$. Lorsque ni $T \prec_r S$ ni $T \succ_r S$, on dit que T et S sont* équivalents *pour l'ordre de Ritt; on écrit alors $T \sim_r S$.*

Rappelons que les travaux de Ritt concernaient uniquement des ensembles triangulaires réduits. La définition 4.2.5 ci-dessus est plus générale, mais les propriétés que Ritt a montrées pour les ensembles triangulaires réduits sont conservées pour les ensembles triangulaires standards. Cela est dû essentiellement à la propriété suivante :

Lemme 4.2.6 *Soit I un idéal de $\mathbf{P}_n$ et $T = \{t_1, \ldots, t_\ell\}$ un ensemble triangulaire standard de $\mathbf{P}_n$ contenu dans I. Alors l'ensemble $T' = \{t'_1, \ldots, t'_\ell\}$ défini par $t'_1 = t_1$ et $t'_j =$ $\mathsf{prem}(t_j, \{t'_1, \ldots, t'_{j-1}\})$ pour tout $j \in [2, \ell]$, est un ensemble triangulaire réduit contenu dans I et tel que $T' \sim_r T$.*

Preuve. On le montre par récurrence. Pour $\ell = 1$ c'est évident. Considérons alors $\ell > 1$. Il est clair que l'ensemble T' ainsi construit est réduit. Le fait que T' soit inclus dans I se déduit de la "remainder formula" (proposition 2.2.10) avec l'hypothèse de récurrence. Finalement, puisque T est standard, le corollaire 2.1.18 entraîne que les ensembles T et T' sont équivalents pour l'ordre de Ritt. □

Proposition 4.2.7 *Soit $T = \{t_1, \ldots, t_\ell\}$ et $S = \{s_1, \ldots, s_k\}$ deux ensembles triangulaires standards de $\mathbf{P}_n$. On a alors les affirmations suivantes :*

(i) $T \sim_r S \quad \Longleftrightarrow \quad l = k$ et $(\forall j \in \{1, \ldots, k\})\ t_j \sim_r s_j$

(ii) $(\forall p \in \mathbf{P}_n \setminus k)$ $(\mathsf{red?}(p,T)$ et $x_i = \mathsf{mvar}(p)) \implies T_{x_i}^- \cup \{p\} \prec_r T$

Preuve. Ce sont des conséquences directes des définitions 2.1.6 et 4.2.5. □

Définition 4.2.8 *Un sous-ensemble T de F est un* ensemble caractéristique de Ritt *de F si l'une des conditions suivantes est satisfaite :*

(i) $T = \{a\}$ pour un élément a non nul de k,

(ii) $F \cap k \subseteq \{0\}$ et T est un élément minimal pour $\prec_r$ dans $\mathcal{F}$, où $\mathcal{F}$ est la famille composée de tous les ensembles triangulaires standards contenus dans F.

Remarque 4.2.9 Tout ensemble triangulaire T de $\mathbf{P}_n$ est clairement un ensemble caractéristique au sens de Wu de $\langle T \rangle$. Ce n'est cependant pas forcément un ensemble caractéristique de $\langle T \rangle$ au sens de Ritt, même dans le cas où il n'engendre pas l'anneau $\mathbf{P}_n$ tout entier. L'ensemble $T = \{x_1^2 - x_1, x_1x_2 - 1\}$ donné dans la remarque 2.2.9 illustre ce phénomène. On peut vérifier que l'ensemble triangulaire standard $\{x_1 - 1, x_2 - 1\}$, plus petit que T pour l'ordre $\prec_r$, est une base de Gröbner de $\langle T \rangle$ pour l'ordre lexicographique.

Proposition 4.2.10 *Soit T un ensemble caractéristique de $\langle F \rangle$ au sens de Ritt. Alors T est un ensemble caractéristique de F au sens de Wu. De plus, si T est un ensemble triangulaire alors $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$.*

Preuve. Le cas $T \subset k$ est trivial. Supposons donc que T soit un ensemble triangulaire. On a alors $\langle F \rangle \cap k = \{0\}$. Soit $f \in \langle F \rangle$. Posons $r = \mathsf{prem}(f,T)$. La relation donnée par la proposition 2.2.10 entraîne $r \in \langle F \rangle$. Si on suppose $r \neq 0$ alors on a forcément $r \notin k$. Notons v la variable principale de r. Puisque r est réduit par rapport à T, il résulte de la proposition 4.2.7 que

$$T_v^- \cup \{r\} \prec_r T \ .$$

On aboutit ainsi à une contradiction, et par conséquent $r = 0$ et $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$. □

Théorème 4.2.11 *Soit T un ensemble triangulaire standard contenu dans $\langle F \rangle$. Alors les propriétés suivantes sont équivalentes :*

(i) T est un ensemble caractéristique de $\langle F \rangle$ au sens de Ritt,

(ii) $\langle F \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$.

Preuve. L'implication $(i) \Rightarrow (ii)$ a déjà été prouvée dans la proposition 4.2.10. Il nous reste à montrer que si T n'est pas un ensemble caractéristique de $\langle F \rangle$ alors il existe un polynôme $p \in \langle F \rangle$ tel que $\mathsf{prem}(p,T) \neq 0$. Supposons donc qu'il existe un ensemble triangulaire standard $S \subseteq \langle F \rangle$ tel que $S \prec_r T$. On note $S = \{s_1, \ldots, s_k\}$ et $T = \{t_1, \ldots, t_\ell\}$. En utilisant au besoin le lemme 4.2.6, on peut considérer que S est réduit. On distingue alors deux cas. Premièrement, si $\ell < k$ et si pour tout $j \in \{1, \ldots, \ell\}$ on a $t_j \sim_r s_j$, alors posons $p = s_{\ell+1}$. Remarquons que $\mathsf{red?}(p, \{s_1, \ldots, s_\ell\})$. Comme pour tout $j \in \{1, \ldots, \ell\}$ on a $t_j \sim_r s_j$, alors on a aussi $\mathsf{red?}(p, \{t_1, \ldots, t_\ell\})$. Passons à l'autre possibilité. Supposons qu'il existe $i \in \{1, \ldots, \min(k, \ell)\}$ tel que $s_i \prec_r t_i$ et $t_j \sim_r s_j$ pour tout $j \in \{1, \ldots, i-1\}$. Posons $p = s_i$. Comme ci-dessus, nous avons $\mathsf{red?}(p, \{t_1, \ldots, t_{i-1}\})$. Puisque $p \prec_r t_i$ et puisque pour $j \in \{i+1, \ldots, \ell\}$ on a $\mathsf{mvar}(p) \prec_r \mathsf{mvar}(t_j)$, on obtient $\mathsf{red?}(p, \{t_1, \ldots, t_\ell\})$. Dans les deux cas, nous avons finalement trouvé un polynôme p tel que $\mathsf{prem}(p,T) \neq 0$. □

Remarque 4.2.12 Le calcul d'ensembles caractéristiques de Wu au moyen de la procédure CHRST-REM de Wu s'avère très difficile sur certains exemples. Dans un but d'efficacité, [Wan92b] utilise la notion plus faible d'*ensemble médial* de F. Un ensemble triangulaire contenu dans l'idéal $\langle F\rangle$ est appelé ensemble médial si T n'est plus grand qu'aucun ensemble caractéristique de F pour l'ordre de Ritt. Tout ensemble caractéristique de Wu de F, et donc tout ensemble caractéristique de Ritt de $\langle F\rangle$ est ainsi un ensemble médial de F.

4.3 Ensembles triangulaires réguliers

La notion d'ensemble triangulaire régulier présentée ci-dessous permet d'éviter la définition inductive un peu lourde d'une chaîne régulière et de sa représentation que nous rappellerons et étudierons dans la section 4.4. Elle est plus simple que la définition d'ensemble régulier introduite dans [AM97] qui nécessite aussi une induction dont on peut s'affranchir. Nous pensons que notre définition et le travail que nous avons réalisé dans cette section et la suivante apporte non seulement des nouveaux résultats, mais aussi une vision plus simple et plus claire des concepts et des algorithmes présentés par [Kal91], [Kal93], [Kal95]. Le théorème 4.3.4 est très important et à mettre en rapport avec le comportement des bases de Gröbner pour le passage aux idéaux d'élimination. Nous prouvons même plus loin (section 4.6) que notre résultat caractérise les ensembles triangulaires réguliers. Il est complété par le théorème 4.3.6 concernant les idéaux d'élimination des idéaux premiers associés au saturé d'un ensemble triangulaire régulier. Le théorème 4.3.11 montre que le saturé d'un ensemble triangulaire régulier T et son radical se caractérisent en termes de pseudo-reste. Ces résultats se déduisent récursivement des propriétés des idéaux quasi-monogènes et des extensions d'idéaux dans un anneau polynomial que nous avons présentées dans le chapitre 3. Ils apparaissent sous une forme voisine dans [AM97]. On s'intéresse rapidement à la fin de cette section aux ensembles triangulaires normalisés définis dans [Laz91a] (voir la définition 2.2.5). Nos résultats précédents permettent de montrer aisément que tout ensemble triangulaire normalisé est régulier (proposition 4.3.14).

On exploite d'abord les résultats du chapitre 3 pour exprimer le saturé d'un ensemble triangulaire T de $\mathbf{P}_n$ en fonction du saturé de $T^-_{x_n}$.

Proposition 4.3.1 *Pour tout ensemble triangulaire T de $\mathbf{P}_n$ tel que $x_n \notin \mathsf{algVar}(T)$ on a*

$$\mathsf{sat}(T) \;=\; \mathsf{sat}_{n-1}(T)[x_n] \;.$$

Preuve. C'est une conséquence directe de la proposition 3.1.5. □

Proposition 4.3.2 *Soit T un ensemble triangulaire de $\mathbf{P}_n$ tel que $x_n \in \mathsf{algVar}(T)$ et T_{x_n} n'est pas diviseur de zéro dans l'anneau quotient $\mathbf{P}_{n-1}/\mathsf{sat}_{n-1}(T^-_{x_n})$. On a alors la propriété suivante :*

$$\mathsf{sat}(T) \;=\; \langle \mathsf{sat}_{n-1}(T^-_{x_n}) \cup \{T_{x_n}\}\rangle : (\mathsf{init}(T_{x_n}))^\infty \;.$$

Preuve. Notons $I = \mathsf{sat}_{n-1}(T^-_{x_n})$ et $f = T_{x_n}$. On désigne par h l'initial de f. En posant $a = \prod_{t\in T^-_{x_n}} \mathsf{init}(t)$, on a $I = \langle T^-_{x_n}\rangle : a^\infty$. Comme $\langle I \cup \{f\}\rangle$ est quasi-monogène régulier, la proposition 3.2.12 s'applique et donne la relation

$$\langle I \cup \{f\}\rangle : h^\infty \;=\; \langle \langle T^-_{x_n}\rangle \cup \{f\}\rangle : (ah)^\infty \;. \tag{4.5}$$

On a ainsi prouvé le résultat puisque le membre droit de l'égalité (4.5) est égal à $\mathsf{sat}(T)$. $\square$

Pour obtenir une relation intéressante dans le cas où x_n est algébrique il a fallu ajouter une hypothèse supplémentaire; elle consiste à imposer que l'idéal $\langle \mathsf{sat}_{n-1}(T^-_{x_n}) \cup \{T_{x_n}\}\rangle$ soit un idéal quasi-monogène régulier de $\mathbf{P}_{n-1}[x_n]$ (voir la définition 3.2.3). En ajoutant cette condition pour chaque variable algébrique, on définit simplement une classe d'ensembles triangulaires qui bénéficie de propriétés agréables.

Définition 4.3.3 *Soit T un ensemble triangulaire de $\mathbf{P}_n$. On dit que T est* régulier *si pour toute variable $x_i \in \mathsf{algVar}(T)$, l'initial de T_{x_i} n'est pas diviseur de zéro dans l'anneau quotient $\mathbf{P}_{i-1}/\mathsf{sat}_{i-1}(T^-_{x_i})$.*

On peut dire de manière équivalente que l'initial de T_{x_i} n'appartient à aucun des idéaux premiers associés au saturé de $T^-_{x_i}$.

Nous avons vu dans la section 4.1 que la propriété fondamentale des ensembles triangulaires consistants est de représenter des idéaux fortement équidimensionnels et de permettre une lecture aisée de leur structure géométrique. Le problème est alors de savoir pour un ensemble triangulaire T donné si T est consistant, c'est-à-dire s'il admet des zéros réguliers. En effet, dans l'optique de la résolution de systèmes polynomiaux, le fait d'obtenir éventuellement des sorties inutiles semble gênant. Ce qui suit montre l'avantage d'utiliser des ensembles triangulaires réguliers. Nous prouvons dans le théorème 4.3.4 que tout idéal d'élimination de $\mathsf{sat}(T) \cap \mathbf{P}_i$ s'exprime facilement à l'aide de polynômes de $\mathbf{P}_i$ uniquement. On vérifie alors non seulement que tout ensemble triangulaire régulier est consistant, mais aussi que tout idéal premier du saturé de l'ensemble triangulaire *tronqué* $T \cap \mathbf{P}_i$ est l'idéal d'élimination d'un idéal premier de $\mathsf{sat}(T)$; autrement dit, à partir de tout zéro générique d'une variété irréductible de $\overline{\mathbf{W}(T \cap \mathbf{P}_i)}$ (qui est alors un zéro régulier de $T \cap \mathbf{P}_i$) on peut obtenir un zéro générique d'une variété irréductible de $\overline{\mathbf{W}(T)}$.

Théorème 4.3.4 *Si T est un ensemble triangulaire régulier de $\mathbf{P}_n$ alors pour tout entier $i \in [0, n]$ on a*

$$\mathsf{sat}(T) \cap \mathbf{P}_i = \mathsf{sat}_i(T \cap \mathbf{P}_i) \ .$$

Preuve. La démonstration s'effectue par récurrence sur l'entier n. Si $n = 0$ c'est trivial. Lorsque $n > 0$, il suffit simplement de prouver la relation pour $i = n - 1$. Dans le cas où x_n n'est pas une variable algébrique de T, on a $\mathsf{sat}(T) = \mathsf{sat}_{n-1}(T)[x_n]$ d'après la proposition 4.3.1. L'application de la proposition 3.1.3 fournit alors le résultat. Supposons maintenant que $x_n \in \mathsf{algVar}(T)$ et posons $f = T_{x_n}$. D'après la proposition 4.3.2 on a

$$\mathsf{sat}(T) = \langle \mathsf{sat}_{n-1}(T \cap \mathbf{P}_{n-1}) \cup \{f\}\rangle : (\mathsf{init}(f))^\infty$$

En appliquant le corollaire 3.2.6 avec $I = \mathsf{sat}_{n-1}(T \cap \mathbf{P}_{n-1})$, on obtient bien $\mathsf{sat}_{n-1}(T \cap \mathbf{P}_{n-1}) = \mathsf{sat}(T) \cap \mathbf{P}_{n-1}$. $\square$

Corollaire 4.3.5 *Tout ensemble triangulaire régulier est consistant.*

Preuve. On a $\mathsf{sat}(T) \cap \mathbf{P}_0 = \mathsf{sat}_0(\emptyset) = \{0\}$. Donc 1 n'appartient pas à $\mathsf{sat}(T)$. Or, dire que l'ensemble des zéros réguliers de T est non vide revient à dire que l'idéal $\mathsf{sat}(T)$ est un idéal propre de $\mathbf{P}_{n-1}$ (utiliser le théorème 2.2.21) □

Nous avons vu précédemment que les ensembles triangulaires généraux n'étaient pas forcément consistants, contrairement aux ensembles réguliers. On peut ajouter qu'un ensemble triangulaire général qui est consistant ne satisfait pas forcément à l'égalité du théorème 4.3.4. Un contre-exemple simple est donné avec l'ensemble $T = \{x_1^2 - x_1, x_1x_2 - 1\}$ de la remarque 2.2.9. On a $\mathsf{sat}(T) = \langle x_1 - 1, x_2 - 1\rangle$ donc $\mathsf{sat}(T) \cap \mathbf{P}_1 = \langle x_1 - 1\rangle$, alors que $\mathsf{sat}_1(T \cap \mathbf{P}_1) = \langle x_1^2 - x_1\rangle$.

Théorème 4.3.6 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$. Alors $\mathsf{sat}(T)$ est un idéal fortement équidimensionnel. De plus, la hauteur de $\mathsf{sat}(T) \cap \mathbf{P}_i$ est donnée par le nombre d'éléments de $T \cap \mathbf{P}_i$ et*

$$\mathsf{ass}(\mathsf{sat}_i(T \cap \mathbf{P}_i)) = \{\mathcal{P} \cap \mathbf{P}_i \mid \mathcal{P} \in \mathsf{ass}(\mathsf{sat}(T))\} .$$

Preuve. Sachant que T est consistant, le théorème 4.1.4. s'applique et fournit la première partie de l'énoncé. L'ensemble des idéaux premiers associés à $\mathsf{sat}_i(T \cap \mathbf{P}_i)$ est alors donné par le corollaire 4.1.5 en utilisant le fait que $\mathsf{sat}(T) \cap \mathbf{P}_i = \mathsf{sat}_i(T \cap \mathbf{P}_i)$. □

Illustrons avec l'exemple ci-dessous ce que signifie géométriquement l'équidimensionnalité forte d'un ensemble triangulaire régulier T. Cet exemple montre encore une fois comment le saturé de T se comporte de façon plus satisfaisante que l'idéal engendré par T.

Exemple 4.3.7 On considère l'ensemble triangulaire

$$T = \{x_2^3 - x_2, x_1x_3^2 - x_2\} .$$

L'idéal engendré par T admet la décomposition primaire minimale $\langle T\rangle = Q_1 \cap \ldots \cap Q_4$ avec

$$\begin{aligned} Q_1 &= \langle x_2, x_3^2\rangle \\ Q_2 &= \langle x_2 + 1, x_3^2\, x_1 + 1\rangle \\ Q_3 &= \langle x_2 - 1, x_3^2\, x_1 - 1\rangle \\ Q_4 &= \langle x_1, x_2\rangle . \end{aligned}$$

On constate que l'idéal $\langle T\rangle$ est équidimensionnel mais la composante Q_4 diffère géométriquement des trois autres dans le sens où tout zéro générique de la variété (irréductible) de Q_4 a une première coordonnée algébrique contrairement aux variétés irréductibles associées respectivement à Q_1, Q_2, Q_3 (on pourra consulter la section 16.3 de [vdW91] sur le concept de zéro générique). Par définition le saturé de T correspond à l'idéal $\langle T\rangle : x_1^\infty$. Une décomposition primaire réduite est donc donnée par

$$\mathsf{sat}(T) = Q_1 \cap Q_2 \cap Q_3 .$$

Les variétés irréductibles V_1, V_2, V_3 associées à Q_1, Q_2, Q_3 admettent respectivement comme zéros génériques les éléments de K^n qui s'écrivent $(\zeta, 0, 0, \xi)$, $(\zeta, -1, \sqrt{\frac{-1}{\zeta}}, \xi)$ et $(\zeta, 1, \sqrt{\frac{1}{\zeta}}, \xi)$, où ζ est transcendant sur $\mathbb{C}$ et ξ est transcendant sur $\mathbb{C}(\zeta)$. Ces points ont une caractéristique commune : pour tout zéro générique (a_1, a_2, a_3, a_4) de V_1, V_2 et V_3 le nombre a_1 est transcendant sur k, puis a_2 algébrique sur $k(a_1)$, a_3 algébrique sur $k(a_1, a_2)$, et finalement a_4 est transcendant sur $k(a_1, a_2, a_3)$. Cette propriété est une manière d'exprimer que le saturé de T est fortement équidimensionnel.

Lorsque l'ensemble triangulaire régulier T définit un idéal saturé de dimension zéro, la proposition suivante montre qu'on peut considérer indifféremment l'ensemble des zéros réguliers, sa clôture ou l'ensemble des zéros lui-même, ce qui se révèle bien pratique pour la décomposition de systèmes zéro-dimensionnels.

Proposition 4.3.8 *Si $T = \{f_1, \ldots, f_n\}$ est un ensemble triangulaire régulier de $\mathbf{P}_n$ de cardinal n alors*

(i) $\mathsf{sat}(T) = \langle T \rangle$,

(ii) $\overline{\mathbf{W}(T)} = \mathbf{V}(T)$,

(iii) $\mathbf{W}(T) = \mathbf{V}(T)$.

Preuve. On prouve l'égalité (i) par récurrence sur n. C'est vérifié par convention pour $n = 0$. Supposons $n > 0$. Par hypothèse f_n a pour variable principale x_n. On pose $h = \mathsf{init}(f_n)$ et $I = \mathsf{sat}_{n-1}(T^-_{x_n})$. La relation de la proposition 4.3.2 donne

$$\mathsf{sat}(T) = \langle I \cup \{f_n\}\rangle : h^\infty .$$

Nous affirmons d'abord que si $\mathcal{P}$ est un idéal premier associé à $\langle I \cup \{f_n\}\rangle$ alors $h \notin \mathcal{P}$. En effet, l'idéal $I \cup \{f_n\}$ est par hypothèse un idéal quasi-monogène régulier. Il résulte donc de la proposition 3.2.5 que $\mathcal{P} \cap \mathbf{P}_{n-1}$ est un idéal premier de qui contient I. Il contient par conséquent un idéal premier $\mathcal{Q}$ de $\mathbf{P}_{n-1}$ associé à I. Puisque $\mathcal{Q}$ est de hauteur $n-1$ d'après le théorème 4.3.6, on en déduit que $\mathcal{P} \cap \mathbf{P}_{n-1} = \mathcal{Q}$. Comme T est régulier, on sait que $h \notin \mathcal{Q}$, d'où $h \notin \mathcal{P}$.

La proposition A.1.20 entraîne alors que

$$\mathsf{sat}(T) = \langle I \cup \{f_n\}\rangle .$$

Puisque T' est un ensemble triangulaire régulier de $\mathbf{P}_{n-1}$ de cardinal $n-1$, on a par récurrence $I = \langle T^-_{x_n}\rangle$, et ainsi $\mathsf{sat}(T) = \langle T \rangle$, ce qui clôt la preuve de (i).

L'égalité (ii) est une conséquence directe de (i) par le théorème 2.2.21. Finalement, soit $a \in \mathbf{V}(T)$. C'est donc un zéro d'un idéal premier $\mathcal{P}$ associé à $\langle T \rangle$. On sait avec le point (i) et le théorème 4.3.6 que $\mathcal{P}$ est maximal et que pour tout $i \in [1, n]$ on a $\mathsf{init}(f_i) \notin \mathcal{P}$. On en déduit que

$$\langle \mathcal{P} \cup \{\mathsf{init}(f_i)\}\rangle = \mathbf{P}_n .$$

On en déduit que a ne peut être zéro de $\mathsf{init}(f_i)$. C'est donc un zéro régulier de T. Comme on a trivialement $\mathbf{W}(T) \subseteq \mathbf{V}(T)$ l'égalité (iii) s'ensuit. $\square$

L'exemple ci-dessous illustre que c'est bien le fait que T soit régulier qui est primordial dans les hypothèses de la proposition 4.3.8.

Exemple 4.3.9 Soit T l'ensemble triangulaire de $\mathbf{P}_3$ défini par

$$T = \{x_1^2 - x_1, x_2^2 - x_1, x_1x_3 - x_2\} \ .$$

Il est clair que $T_{x_3}^-$ est un ensemble triangulaire régulier qui vérifie les propriétés de la proposition 4.3.8. Mais T n'est pas régulier car l'initial du polynôme $x_1x_3 - x_2$ est diviseur de zéro modulo $T_{x_3}^-$.

Comme le nombre de polynômes de T correspond au nombre de variables, on pourrait s'attendre à ce que la variété $\mathbf{V}(T)$ soit de dimension zéro. Mais on vérifie facilement que

$$\mathbf{V}(T) = \{(1,1,1)\} \cup \{(1,-1,-1)\} \cup \{(0,0,t), t \in K\}$$

et par suite que $\mathbf{V}(T)$ a un nombre infini de points. Le passage au saturé de T élimine la dernière composante, de dimension trop grande, puisque

$$\begin{aligned} \mathsf{sat}(T) &= \langle x_1 - 1, x_2^2 - x_1, x_1x_3 - x_2\rangle \\ &= \langle x_1 - 1, x_2^2 - 1, x_3 - x_2\rangle \ . \end{aligned}$$

On constate immédiatement que les propriétés de la proposition 4.3.8 ne sont effectivement pas vérifiées.

Les relations des idéaux quasi-monogènes réguliers avec la notion de pseudo-reste établies dans la section 3.2 nous permettent d'établir facilement des propriétés similaires pour les ensembles triangulaires réguliers.

Lemme 4.3.10 *Soit T un ensemble triangulaire non vide de $\mathbf{P}_n$ tel que $x_n \in \mathsf{algVar}(T)$ et $\mathsf{init}(T_{x_n})$ n'est pas diviseur de zéro dans $\mathbf{P}_{n-1}/\mathsf{sat}_{n-1}(T_{x_n}^-)$. Alors pour tout $p \in \mathbf{P}_n$ on a*

$$p \in \mathsf{sat}(T) \iff \mathsf{prem}(p, T_{x_n}) \in \mathsf{sat}_i(T_{x_i}^-) \ .$$

Preuve. On part de l'égalité $\mathsf{sat}(T) = \langle \mathsf{sat}_{n-1}(T_{x_n}^-) \cup \{T_{x_n}\}\rangle : (\mathsf{init}(T_{x_n}))^\infty$ donnée dans la proposition 4.3.2. L'idéal quasi-monogène engendré par $\mathsf{sat}_{n-1}(T_{x_n}^-)$ et T_{x_n} étant régulier, le résultat est alors une application directe de la proposition 3.2.9. □

Théorème 4.3.11 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$. Pour tout polynôme p de $\mathbf{P}_n$ on a les équivalences suivantes :*

(i) $p \in \mathsf{sat}(T) \iff \mathsf{prem}(p, T) = 0$,

(ii) $p \in \sqrt{\mathsf{sat}(T)} \iff (\exists m \geq 0) \mid \mathsf{prem}(p^m, T) = 0$.

Preuve. L'assertion (ii) est en fait une conséquence de (i). Montrons donc l'équivalence (i) par récurrence sur l'entier n. Elle est triviale pour $n = 0$. Soit $n > 0$ et p un polynôme de $\mathbf{P}_n$ de degré d en x_n. On pose $p = \sum_{k=0}^{d} p_k x_n^k$. Dans le cas où x_n est une variable transcendante par rapport à T, on sait que $\mathsf{sat}(T) = \mathsf{sat}_{n-1}(T)[x_n]$. D'après l'hypothèse de récurrence, on a donc

$$p \in \mathsf{sat}(T) \iff (\forall k \in [0, d])\ \mathsf{prem}(p_k, T) = 0\ .$$

On en déduit avec le corollaire 2.1.18 que

$$p \in \mathsf{sat}(T) \iff \mathsf{prem}(p, T) = 0\ .$$

Si x_n est une variable algébrique, le lemme 4.3.10 donne l'équivalence

$$p \in \mathsf{sat}(T) \iff \mathsf{prem}(p, T_{x_n}) \in \mathsf{sat}_n(T_{x_n}^-)\ .$$

Le résultat prouvé pour le cas précédent entraîne

$$p \in \mathsf{sat}(T) \iff \mathsf{prem}(\mathsf{prem}(p, T_{x_n}), T_{x_n}^-) = 0\ ,$$

c'est-à-dire ce qu'on voulait prouver. □

Remarque 4.3.12 Avec le théorème 4.3.11, on vérifie facilement que tout ensemble triangulaire régulier T est un ensemble triangulaire standard. En effet, pour toute variable $v \in \mathsf{algVar}(T)$ l'initial de T_v n'est pas diviseur de zéro modulo T_v^-. Par conséquent il n'appartient pas au saturé de T_v^- et ne peut donc se réduire à zéro par T_v^-.

Nous terminons cette section par l'étude d'une classe importante d'ensembles triangulaires définis dans [Laz91a], à savoir celle des ensembles normalisés.

Lemme 4.3.13 *Soit p un polynôme non nul de $\mathbf{P}_n$ et T un ensemble triangulaire régulier de $\mathbf{P}_n$. Si p est normalisé par rapport à T alors il n'est pas diviseur de zéro dans $\mathbf{P}_n/\mathsf{sat}(T)$.*

Preuve. On raisonne par induction en utilisant l'ordre $\prec_r$ sur les polynômes. Le cas où $p \in k$ est trivial. Considérons donc que $\mathsf{mvar}(p) = x_i$. Soit $\mathcal{P}$ un idéal premier de $\mathsf{sat}(T)$. On note $\mathcal{Q}$ l'idéal $\mathcal{P} \cap \mathbf{P}_i$. Il s'agit de montrer que $p \notin \mathcal{Q}$. Puisque p est normalisé par rapport à T, la variable x_i n'est pas algébrique pour T. D'après la proposition 4.3.2 on a ainsi

$$\mathsf{sat}_i(T \cap \mathbf{P}_i) = \mathsf{sat}_{i-1}(T \cap \mathbf{P}_{i-1})[x_i]\ .$$

Puisque $\mathcal{Q}$ est un idéal premier associé à $\mathsf{sat}_i(T \cap \mathbf{P}_i)$ (théorème 4.3.6), on en déduit que

$$\mathcal{Q} = (\mathcal{P} \cap \mathbf{P}_{i-1})[x_i]\ . \tag{4.6}$$

Le polynôme p étant normalisé par rapport à T, son initial h l'est aussi. Comme $h \prec_r p$ il résulte de l'hypothèse de récurrence que $h \notin \mathcal{P}$, puis de la relation 4.6 que $p \notin \mathcal{Q}$. □

Proposition 4.3.14 *Tout ensemble triangulaire normalisé est régulier.*

Preuve. On obtient facilement le résultat par une induction sur n par application du lemme 4.3.13. □

4.4 Chaînes régulières

Le concept de chaîne régulière est introduit de façon indépendante dans [YZ94] et dans [Kal91]. Les chaînes régulières apparaissent aussi dans [CG92]. Ces ensembles triangulaires standards sont utilisés par ces auteurs pour proposer des algorithmes qui calculent des décompositions équidimensionnelles de variétés algébriques qui ont des propriétés meilleures que les décompositions produites par la méthode de Wu sans nécessiter de factorisation.

La définition originale de Kalkbrener est fondée sur la notion de point pseudo-générique. À toute chaîne régulière T est associée une variété équidimensionnelle V appelée représentation de T (qui n'est pas l'ensemble des zéros de T). L'ensemble des points pseudo-génériques de T est en fait l'ensemble des points génériques des composantes irréductibles de V. Rappelons que toute variété irréductible est définie par l'un quelconque de ses points génériques. [Kal91] définit de façon inductive une chaîne régulière de $\mathbf{P}_n$ en même temps que son ensemble des points pseudo-génériques. Kalkbrener propose alors une méthode pour décomposer l'ensemble des zéros d'un système algébrique en un nombre fini de représentations d'ensembles triangulaires. Toutefois, il n'apparaît pas que la représentation peut en fait être définie simplement de façon globale dans $\mathbf{P}_n$. Or il nous a semblé important dès le début de notre thèse de préciser clairement les spécifications de cette méthode qui ne décompose pas en zéros réguliers d'ensembles triangulaires comme celle de Wu [Wu87] ou celle de Lazard [Laz91a], mais en clôtures de zéros réguliers comme le montre le théorème 4.4.11. Nous prouvons simultanément que la notion de chaîne régulière de Kalkbrener et celle d'ensemble triangulaire régulier de la section 4.3 sont équivalentes. Enfin, le dernier objectif de cette section est de faire apparaître en quoi la représentation d'une chaîne régulière induit une structure de produit de corps adéquate pour les algorithmes présentés dans le chapitre suivant (théorème 4.4.14).

Précisons encore que, contrairement à [Kal91] et [Kal93] où la terminologie est celle des variétés, nous travaillons dans cette section avec des idéaux. Ce cadre nous a paru le mieux adapté à nos objectifs et rejoint en cela l'habilitation de M. Kalkbrener [Kal95] [Kal98]. Il y définit une notion plus générale – les systèmes de représentations – pour étudier le transfert d'algorithmes (calcul de hauteur, radical, décomposition d'idéaux) d'un anneau commutatif noethérien A à l'anneau polynomial $A[X]$. Un système de représentations dans A est composé d'un ensemble S de parties finies de A et d'une application qui, à tout élément de S, associe un idéal radical propre de A (la représentation de S). De plus, pour tout idéal I de A, il doit exister $C_1, \ldots, C_s$ dans S tels que $\sqrt{I} = C_1 \cap \ldots \cap C_s$. Puisque les variétés correspondent à des idéaux radicaux et les points génériques à des idéaux premiers, on peut alors considérer les chaînes régulières dans $\mathbf{P}_n$ comme un cas particulier de système de représentations. Avec ce point de vue, la représentation d'une chaîne régulière correspond à l'idéal de ce que Kalkbrener appelle représentation de T dans [Kal91].

Notation 4.4.1 *Soit I un idéal de A. Pour un polynôme p de $A[x]$ nous notons $\widehat{p}^I$ l'image canonique de p dans* $\mathrm{fr}(A/I)[x]$*, où* $\mathrm{fr}(A/I)$ *désigne l'anneau total des fractions de A/I (voir la définition A.2.3). De plus, si $\mathcal{P}$ est un idéal premier associé à I et $\kappa = \mathrm{fr}(A/\mathcal{P})$, alors on dit que κ est un* corps associé *à I et on écrit $\widehat{p}^\kappa$ pour $\widehat{p}^\mathcal{P}$.*

Remarque 4.4.2 Soit $p \in A[x] \setminus A$. Le polynôme $\widehat{p}^I$ est unitaire dans $\mathrm{fr}(A/I)[x]$ si et seulement si pour tout idéal premier $\mathcal{P}$ associé à I l'initial de p n'appartient pas à $\mathcal{P}$ (voir la proposition A.1.23). En supposant que $\widehat{p}^I$ est unitaire, on a alors clairement $\mathsf{deg}(p, x) = \mathsf{deg}(\widehat{p}^I, x)$. De plus, étant donné un autre polynôme $r \in A[x]$, si $\mathsf{deg}(r, x) < \mathsf{deg}(p, x)$ alors on a $\mathsf{deg}(\widehat{r}^I, x) < \mathsf{deg}(\widehat{p}^I, x)$.

Exemple 4.4.3 Soit k le corps des rationnels $\mathbb{Q}$ et $n = 3$. Soit $T_5 = \{p_1, p_2\}$ où

$$\begin{aligned} p_1 &= x_1^4 - 5\, x_1^2 + 6\ , \\ p_2 &= \left(x_1^2 - 2\right) x_2^2 + \left(-2\, x_1^3 + 4\, x_1\right) x_2 + x_1^4 - 2\, x_1^2\ . \end{aligned}$$

On note I l'idéal engendré par T_5 dans $\mathbf{P}_3$. Cet idéal admet pour décomposition primaire

$$I = \langle x_1^2 - 3,\ (x_2 - x_1)^2\rangle\ \cap\ \langle x_1^2 - 2\rangle.$$

Par conséquent les idéaux premiers associés à I sont

$$\mathcal{P}_1 = \langle x_1^2 - 3,\ (x_2 - x_1)\rangle \quad \text{et} \quad \mathcal{P}_2 = \langle x_1^2 - 2\rangle\ .$$

On a ainsi $\sqrt{I} = \mathcal{P}_1\ \cap\ \mathcal{P}_2$. Les corps associés à I sont

$$\kappa_1 = \mathrm{fr}(\mathbb{Q}[x_1, x_2]/\mathcal{P}_1) = \mathbb{Q}(\sqrt{3}) \quad \text{et} \quad \kappa_2 = \mathrm{fr}(\mathbb{Q}[x_1, x_2]/\mathcal{P}_2) = \mathbb{Q}(\sqrt{2})(x_2)\ .$$

On pose maintenant $p = (x_1^2 - 2)\ x_3^4 + (x_2 - x_1)\ x_3^3 + (1 - x_1)\ x_3 + 1$ et $h = \mathsf{init}(p)$. On vérifie immédiatement que $\widehat{h}^{\kappa_1} = 1$ et $\widehat{h}^{\kappa_2} = 0$. Ainsi, le polynôme $\widehat{p}^I$ n'est pas unitaire dans $\mathrm{fr}(A/I)[x]$.

Notation 4.4.4 *Soit $i \in \{1, \ldots, n\}$ et T un ensemble triangulaire de $\mathbf{P}_i$. Dans ce qui suit, la notation $\mathsf{Rep}_i(T)$ sera utilisée pour désigner un idéal de $\mathbf{P}_i$ qui sera associé à T dans le sens précisé par la définition 4.4.5 ci-dessous. On définit alors $\mathcal{K}_i(T)$ comme l'ensemble de tous les corps $\kappa = \mathrm{fr}(\mathbf{P}_i/\mathcal{P})$, où $\mathcal{P}$ est un idéal premier associé à $\mathsf{Rep}_i(T)$.*

Définition 4.4.5 *Soit T un ensemble triangulaire de $\mathbf{P}_i$. On dit que T est une* chaîne régulière *dans $\mathbf{P}_i$, de* représentation $\mathsf{Rep}_i(T)$*, si l'on a :*

(i) soit $i = 0$, l'ensemble T est vide et $\mathsf{Rep}_0(T) = \{0\}$,

(ii) soit $i > 0$, l'ensemble $T_{x_i}^-$ est une chaîne régulière de $\mathbf{P}_{i-1}$ de représentation $\mathsf{Rep}_{i-1}(T)$ et l'une des conditions suivantes est vérifiée :

(a) $x_i \notin \mathsf{algVar}(T)$ et pour tout $p \in \mathbf{P}_i$ on a :

$$p \in \mathsf{Rep}_i(T) \quad \Longleftrightarrow \quad (\forall \kappa \in \mathcal{K}_{i-1}(T_{x_i}^-))\ \ \widehat{p}^\kappa = 0$$

(b) $x_i \in \mathsf{algVar}(T)$, et pour tout $\kappa \in \mathcal{K}_{i-1}(T_{x_i}^-)$ on a $\widehat{\mathsf{init}(T_{x_i})}^\kappa \neq 0$ et pour tout $p \in \mathbf{P}_i$ on a :

$$p \in \mathsf{Rep}_i(T) \quad \Longleftrightarrow \quad (\forall \kappa \in \mathcal{K}_{i-1}(T_{x_i}^-))\ \ \widehat{p}^\kappa \in \sqrt{\langle \widehat{T_{x_i}}^\kappa \rangle}\ .$$

Exemple 4.4.6 Reprenons l'ensemble triangulaire T_1 défini dans l'exemple 2.2.2. On a $T_1 = \{f_1, f_2, f_3\}$ avec

- $f_1 = x_1 x_2^2 - 3$,
- $f_2 = x_3^2 - 2x_1x_2x_3 + 3x_1$,
- $f_3 = (x_2x_3 + x_2^3)x_4 - 2x_1$.

L'ensemble $\{f_1, f_2\}$ est évidemment une chaîne régulière. Soit I l'idéal engendré par $\{f_1, f_2\}$ dans $\mathbf{P}_3$. Cet idéal est primaire et correspond à l'idéal saturé de l'ensemble triangulaire $\{f_1, f_2\}$. On vérifie que $\mathsf{init}(f_3)$ n'appartient pas au radical de I, ce qui permet de conclure que T_1 est une chaîne régulière.

Considérons maintenant l'ensemble triangulaire $T_1' = \{f_1', f_2, f_3\}$ où $f_1' = x_2\, f_1$. Notons I' l'idéal engendré par $\{f_1', f_2\}$ dans $\mathbf{P}_3$. La décomposition primaire de I' est

$$I' = I \ \cap \ \langle x_2, x_3^2 + 3x_1 \rangle \ .$$

On constate alors que $\mathsf{init}(f_3)$ appartient au radical de $\langle x_2, x_3^2 + 3x_1\rangle$. Par conséquent T_1' n'est pas une chaîne régulière.

Exemple 4.4.7 On vérifie aisément que l'ensemble T_5 de l'exemple 4.4.3 n'est pas une chaîne régulière car $\mathsf{init}(p_2)$ est diviseur de zéro modulo $\langle p_1\rangle$. Par contre, les deux ensembles $C_1 = \{x_1^2 - 3, (x_2 - x_1)^2\}$ et $C_2 = \{x_1^2 - 2\}$ sont des chaînes régulières, de représentations respectives $\mathcal{P}_1$ et $\mathcal{P}_2$. De plus, l'ensemble $C_1 \cup \{p\}$ est aussi une chaîne régulière puisqu'on a $\widehat{h}^{\kappa_1} = 1$, où $h = \mathsf{init}(p)$. Sa représentation est l'idéal $\langle x_1^2 - 3, x_2 - x_1, (x_3^2 - x_1)\ (x_3^2 + 1)\rangle$.

Proposition 4.4.8 *Soit T une chaîne régulière de $\mathbf{P}_i$. Alors on a*

$$x_i \notin \mathsf{algVar}(T) \quad \Longrightarrow \quad \mathsf{Rep}_i(T) \ = \ \sqrt{\mathsf{Rep}_{i-1}(T)}[x_i].$$

Preuve. Soit $p \in \mathbf{P}_i$ et $\kappa \in \mathcal{K}_{i-1}(T_{x_i}^-)$. La relation $\widehat{p}^\kappa = 0$ signifie que chaque coefficient de p, vu comme un polynôme en une variable dans $\mathbf{P}_{i-1}[x_i]$, est nul dans κ. Ainsi $p \in \mathsf{Rep}_i(T)$ signifie que chacun des coefficients de p appartient à tout idéal premier associé à $\mathsf{Rep}_{i-1}(T)$. Puisque $\sqrt{\mathsf{Rep}_{i-1}(T)}$ est l'intersection des idéaux premiers associés à $\mathsf{Rep}_{i-1}(T)$, on obtient le résultat. □

Remarque 4.4.9 Soit T une chaîne régulière de $\mathbf{P}_n$ telle que $x_n \in \mathsf{algVar}(T)$. Il est clair avec la définition 4.4.5 que l'idéal de $\mathbf{P}_n$ engendré par $\mathsf{Rep}_{n-1}(T_{x_n}^-)$ et T_{x_n} est un idéal quasi-monogène régulier.

Proposition 4.4.10 *Soit T une chaîne régulière de $\mathbf{P}_i$. Alors on a*

$$x_i \in \mathsf{algVar}(T) \quad \Longrightarrow \quad \mathsf{Rep}_i(T) = \{p \in \mathbf{P}_i \ \mid \ (\exists m \geq 0)\ \mathsf{prem}(p^m, T_{x_i}) \in \mathsf{Rep}_i(T_{x_i}^-)\}.$$

Preuve. Soit $p \in \mathbf{P}_i$. Définissons $t = T_{x_i}$ et $h = \mathsf{init}(t)$. Soit e un entier positif. On pose $r_e = \mathsf{prem}(p^e, t)$. Il existe un entier positif δ_e et un polynôme q_e de $\mathbf{P}_i$ tels que :

$$h^{\delta_e} p^e = q_e t + r_e \ . \tag{4.7}$$

Supposons d'abord que $p \in \mathsf{Rep}_i(T)$ et prouvons qu'il existe un entier $m \geq 0$ tel que $r_m \in \mathsf{Rep}_i(T^-_{x_i})$. Soit $\kappa \in \mathcal{K}_{i-1}(T^-_{x_i})$. D'après le point (*b*) de la définition 4.4.5 il existe un entier $m \geq 0$ tel que $(\widehat{p}^\kappa)^m$ appartient à l'idéal engendré par $\widehat{t}^\kappa$. En choisissant m assez grand on peut prendre le même entier m pour chaque idéal premier $\mathcal{P}$ associé à $\mathsf{Rep}_{i-1}(T^-_{x_i})$. La relation (4.7) entraîne alors que $\widehat{r_m}^\kappa$ appartient à l'idéal engendré par $\widehat{t}^\kappa$. On en déduit que $\widehat{r_m}^\kappa = 0$ d'après la remarque 4.4.2. De la même manière que dans la preuve de la proposition 4.4.8 on obtient

$$r_m \in \sqrt{\mathsf{Rep}_{i-1}(T^-_{x_i})[x_i]} \ .$$

Cette dernière proposition assure alors que $r_m \in \mathsf{Rep}_i(T^-_{x_i})$. Réciproquement, supposons qu'il existe un entier $m \geq 0$ tel que $r_m \in \mathsf{Rep}_i(T^-_{x_i})$. Soit $\kappa \in \mathcal{K}_{i-1}(T^-_{x_i})$. Puisque $\widehat{r_m}^\kappa = 0$, nous obtenons $\widehat{h^{\delta_m} p^m}^\kappa \in \langle \widehat{t}^\kappa \rangle$ d'après la relation (4.7). Selon le point (*b*) de la définition 4.4.5 l'élément $\widehat{h^{\delta_m}}^\kappa$ est inversible. Il s'ensuit que $\widehat{p}^\kappa$ appartient au radical de $\langle \widehat{t}^\kappa \rangle$. On en conclut que $p \in \mathsf{Rep}_i(T)$. □

Théorème 4.4.11 *Soit T une chaîne régulière de $\mathbf{P}_i$. Alors on a*

$$\mathsf{Rep}_i(T) \ = \ \sqrt{\mathsf{sat}_i(T)}$$

Preuve. On raisonne par récurrence sur i. Pour $i = 0$ on a $T = \emptyset$ et $\mathsf{Rep}_i(T) = \{0\}$ d'après la définition 4.4.5. L'égalité résulte de la convention $\mathsf{sat}_i(\emptyset) = \{0\}$ donnée dans la définition 2.2.16 et du fait que $\mathbf{P}_i$ est un anneau intègre.

Supposons maintenant $i > 0$. Comme $T^-_{x_i}$ est une chaîne régulière de $\mathbf{P}_{i-1}$, on a d'après l'hypothèse de récurrence $\mathsf{Rep}_{i-1}(T^-_{x_i}) = \sqrt{\mathsf{sat}_{i-1}(T^-_{x_i})}$. D'autre part, avec les commutations établies dans la proposition 3.1.5, il résulte de la proposition 4.4.8 que $\mathsf{Rep}_i(T^-_{x_i}) = \sqrt{\mathsf{Rep}_{i-1}(T^-_{x_i})[x_i]}$. On déduit alors immédiatement le résultat de ce qui précède lorsque $x_i \notin \mathsf{algVar}(T)$. Dans le cas où $x_i \in \mathsf{algVar}(T)$ on a selon la proposition 4.4.10 :

$$\mathsf{Rep}_i(T) = \{p \in \mathbf{P}_i \ \mid \ (\exists m \geq 0) \ \mathsf{prem}(p^m, T_{x_i}) \in \mathsf{Rep}_i(T^-_{x_i})\}.$$

Rappelons que l'idéal J engendré par $\mathsf{Rep}_{i-1}(T^-_{x_i})$ et T_{x_i} est quasi-monogène régulier (remarque 4.4.9). Il résulte alors de la proposition 3.2.10 que

$$\mathsf{Rep}_i(T) = \sqrt{(\mathsf{Rep}_{i-1}(T^-_{x_i}) + \langle T_{x_i} \rangle) : h^\infty} \ , \tag{4.8}$$

où h est l'initial de f. Notons h' le produit des initiaux de $T^-_{x_i}$. On a ainsi $\mathsf{Rep}_{i-1}(T^-_{x_i}) = \sqrt{\langle T^-_{x_i} \rangle : h'^\infty}$ en utilisant la proposition A.1.14. L'application de la proposition 3.2.12 sur le membre droit de la relation 4.8 entraîne alors

$$\mathsf{Rep}_i(T) = \sqrt{(\sqrt{\langle T^-_{x_i} \rangle} + \langle T_{x_i} \rangle) : (h'h)^\infty} \ .$$

On en déduit immédiatement le résultat demandé. □

Le saturé d'un ensemble triangulaire étant équidimensionnel, les idéaux premiers associés à $\mathsf{Rep}_i(T)$ sont donc les idéaux premiers associés à $\mathsf{sat}_i(T)$ d'après le corollaire 4.1.5. Il résulte alors clairement des définitions d'une chaîne régulière et d'un ensemble triangulaire régulier ce qui suit.

Proposition 4.4.12 *Un ensemble triangulaire de $\mathbf{P}_n$ est une chaîne régulière si et seulement si c'est un ensemble triangulaire régulier.*

L'équivalence ci-dessus sera complétée dans le théorème 4.6.1 de la section 4.6. En effet, les ensembles triangulaires réguliers (ou si l'on préfère, chaînes régulières) peuvent aussi être caractérisés en termes d'ensembles caractéristiques. La proposition 4.4.12 nous permet dans l'immédiat d'assurer que les sorties des algorithmes de décomposition triangulaire de systèmes polynomiaux proposés par M. Kalkbrener [Kal93] [Kal95] admettent effectivement des zéros réguliers.

Corollaire 4.4.13 *Si T est une chaîne régulière de $\mathbf{P}_i$ alors T est consistant.*

Preuve. C'est simplement une réécriture du corollaire 4.3.5. □

Nous nous intéressons maintenant à la structure algébrique importante que l'on peut associer à toute chaîne régulière. C'est une structure de produit de corps que Kalkbrener ne mentionne pas. Cette propriété permet pourtant de préciser mathématiquement ce que calcule l'algorithme ggcd de [Kal93], à savoir un pgcd de polynômes sur cette structure. Nous montrons ainsi que l'algorithme de décomposition triangulaire de [Kal93] nécessite le même outil de base que l'algorithme de [Laz91a] et [Mor97] qui n'a pourtant pas du tout le même type de spécifications. Ce point commun n'avait rien d'évident jusqu'alors, même pour les auteurs ci-dessus. Il était caché par le manque de clarté de la définition des chaînes que donnait M. Kalkbrener.

Les algorithmes de [Kal93] interprètent en fait implicitement les polynômes comme éléments ou polynômes en une variable sur un anneau du type ci-dessous. Si T est une chaîne régulière de $\mathbf{P}_n$, pour tout $i \in [1, n]$ on pose

$$A_i = \mathrm{fr}(\mathbf{P}_i/\mathsf{Rep}_i(T)) = \mathrm{fr}(\mathbf{P}_i/\sqrt{\mathsf{sat}_i(T \cap \mathbf{P}_i)}) = \mathrm{fr}(\mathbf{P}_i/\sqrt{\mathsf{sat}(T) \cap \mathbf{P}_i}) \ .$$

Chacun des anneaux A_i présente alors la propriété suivante qui est fondamentale pour le développement des algorithmes présentés dans le chapitre 5.

Théorème 4.4.14 *Soit T une chaîne régulière de $\mathbf{P}_n$. Soit $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ l'ensemble des idéaux premiers associés à $\mathsf{sat}(T)$. Alors l'anneau $A_n = \mathrm{fr}(\mathbf{P}_n/\mathsf{Rep}_n(T))$ est un produit fini de corps et*

$$A_n \simeq \mathrm{fr}(\mathbf{P}_n/\mathcal{P}_1) \times \ldots \times \mathrm{fr}(\mathbf{P}_n/\mathcal{P}_m) \ .$$

Preuve. L'anneau noethérien $\mathbf{P}_n/\mathsf{Rep}_n(T)$ est réduit puisqu'un anneau quotient A/I puisqu'un anneau quotient A/I est réduit si et seulement si l'idéal I est radical. La proposition A.2.34 affirme alors que son anneau total des fractions est un produit fini de corps. L'expression de A_n sous forme de produit est obtenue à partir de la même proposition puisque les $\mathcal{P}_j$ correspondent dans $\mathbf{P}_n/\mathsf{Rep}_n(T)$ aux idéaux premiers associés à l'idéal nul. et □

Remarque 4.4.15 De la même façon, on vérifie que chaque anneau A_i défini ci-dessus est un produit de corps du type $\mathrm{fr}(\mathbf{P}_i/\mathcal{P}_j \cap \mathbf{P}_i)$.

4.5 Tours d'extensions simples

Le concept de tour d'extensions simples généralise celui bien connu de tour d'extensions de corps. Il est introduit dans [Mor97] et utilisé dans [ALM99]. Notre présentation est un peu différente et apporte quelques corrections et précisions. Nous montrons dans le théorème 4.5.9) qu'à tout ensemble triangulaire régulier T, on peut associer une tour d'extensions simples dont le dernier élément est l'anneau total des fractions de $\mathbf{P}_n/\mathsf{sat}(T)$. Nous pensons fournir dans cette section une preuve valide de ce résultat qu'utilise [Mor97] et [ALM99]. Nous établissons alors l'équivalence entre la radicalité de T et le fait que la tour d'extensions associée soit *séparable* (proposition 4.5.10). La proposition 4.5.12 vérifie qu'on peut réciproquement construire un ensemble triangulaire régulier dont la tour d'extensions simples est donnée. En fin de section, nous montrons que la représentation d'une chaîne régulière ne définit pas toujours une tour d'extensions simples. La notion de chaîne régulière (ou d'ensemble triangulaire régulier) est ainsi plus générale mais elle est pourtant suffisante pour le développement d'algorithmes de calcul de pgcd modulo un ensemble triangulaire (voir le chapitre 5). Notre travail permet donc de constater qu'il n'est pas nécessaire de disposer d'une tour d'extensions simples séparables pour ce type d'algorithme. Le point fondamental est plutôt l'association d'un produit de corps adéquat à un ensemble triangulaire disposant de propriétés minimales.

Définition 4.5.1 *On dit qu'une suite* $(A_0, A_1, \ldots, A_n)$ *d'anneaux commutatifs est une* tour d'extensions simples *du corps* k *si* $A_0 = k$ *et si pour tout* $i \in [1, n]$ *l'une des conditions suivantes est vérifiée :*

(i) $A_i = \mathrm{fr}(A_{i-1}[x_i])$,

(ii) il existe $f_i \in A_{i-1}[x_i]$ *de degré positif et unitaire tel que* $A_i = \mathrm{fr}(A_{i-1}[x_i]/\langle f_i \rangle)$.

Si, de plus, l'idéal $\langle f_i \rangle$ *est radical chaque fois que la condition* (ii) *est respectée, la tour d'extensions simples est dite* séparable.

La proposition suivante précise l'intérêt des tours séparables.

Proposition 4.5.2 *Soit* $(A_0, \ldots, A_n)$ *une tour d'extensions simples séparable de* k*. Alors pour tout* $i \in [0, n]$*, l'anneau* A_i *est un produit de corps.*

Preuve. Le résultat se montre par récurrence. Pour $i = 0$, c'est trivial. Supposons $i > 0$. Puisque $\mathbf{Nil}(A_{i-1}[x_i]) = \mathbf{Nil}(A_{i-1})[x_i]$ (voir la proposition A.2.31), il résulte de l'hypothèse de récurrence que $A_{i-1}[x_i]$ est un anneau réduit. Dans le cas (ii), l'anneau quotient $A_{i-1}[x_i]/\langle f_i \rangle$ est réduit puisque par hypothèse $\langle f_i \rangle$ est radical. Ainsi, pour les deux cas possibles, la proposition A.2.34 entraîne immédiatement que A_i est un produit fini de corps. □

Considérons un ensemble triangulaire régulier T dans $\mathbf{P}_n$. On pose $A_0 = k$ et

$$A_i = \mathrm{fr}(\mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i))$$

pour tout $i \in [1, n]$. L'homomorphisme canonique de $\mathbf{P}_i$ vers A_i induit un morphisme naturel de $\mathbf{P}_{i+1}$ dans $A_i[x_{i+1}]$ qu'on note F_i. Sa restriction à $\mathbf{P}_i$ présente ainsi les caractéristiques suivantes :

Proposition 4.5.3 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$ et $i \in [0, n]$. Pour tout $p \in \mathbf{P}_i$ on a les équivalences suivantes :*

(i) $F_i(p) = 0 \;\Leftrightarrow\; p \in \mathsf{sat}_i(T \cap \mathbf{P}_i) \;\Leftrightarrow\; p \in \mathsf{sat}(T)$,

(ii) $F_i(p) \in \mathbf{Un}(A_i) \;\Leftrightarrow\; (\forall \mathcal{P} \in \mathsf{ass}(\mathsf{sat}_i(T \cap \mathbf{P}_i)))\, p \notin \mathcal{P} \;\Leftrightarrow\; (\forall \mathcal{P} \in \mathsf{ass}(\mathsf{sat}(T)))\, p \notin \mathcal{P}$.

Preuve. Le morphisme canonique de $\mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i)$ vers son anneau total des fractions A_i est injectif, ce qui justifie la première équivalence de (i). Les éléments de $\mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i)$ dont l'image est inversible par ce morphisme sont exactement les éléments non-diviseurs de zéro. On en déduit la première équivalence de (ii). La seconde équivalence pour chaque point est conséquence respectivement du théorème 4.3.4 et du théorème 4.3.6. □

Remarque 4.5.4 Soit f un polynôme de l'ensemble triangulaire régulier T ayant pour variable principale x_i. Si on note h l'initial de f alors $F_{i-1}(h)$ est un élément inversible de A_{i-1}. En effet, par hypothèse h n'est pas diviseur de zéro dans $\mathbf{P}_{i-1}/\mathsf{sat}_{i-1}(T^-_{x_i})$.

Nous montrons ci-dessous que la suite $(A_0, A_1, \ldots, A_n)$ est une tour d'extensions simples de k. Commençons par établir le lien entre les anneaux A_{i-1} et A_i.

Lemme 4.5.5 *Soit A un anneau et S une partie multiplicative de A. Alors*

$$(S^{-1}A)[X] \simeq S^{-1}(A[X]) \ .$$

Preuve. Posons $B = (S^{-1}A)[X]$. Soit $f : A[X] \to B$ le morphisme naturellement induit par l'homomorphisme canonique de A dans $S^{-1}A$. Vérifions que les trois conditions de la proposition A.2.8 sont satisfaites par f. Pour (i), il est clair que les éléments de $f(S)$ sont des inversibles de B. Soit $p = \sum_{k=1}^{d} a_k X^k$ un élément de $\mathrm{Ker}(f)$. Pour tout $k \in [1, d]$ le coefficient $c_k/1$ est nul dans $S^{-1}A$; il existe donc $s_k \in S$ tel que $s_k c_k = 0$ (remarque A.2.2). En notant s le produit des c_k on alors $sp = 0$, ce qui assure le point (ii). D'autre part, tout élément de B s'écrit $\sum_{k=1}^{d}(a_k/s_k)X^k$ avec $a_k \in A$ et $s_k \in S$. Par une mise en dénominateur commun, on peut l'écrire $f(p)f(s)^{-1}$ avec $p \in A[X]$ et $s \in S$, c'est-à-dire sous la forme demandée dans (iii). □

Lemme 4.5.6 *Soit $S \subseteq \mathbf{reg}(A)$ une partie multiplicative de l'anneau A. Alors on a*

$$\mathrm{fr}(S^{-1}A) \simeq \mathrm{fr}(A) \ .$$

Preuve. il suffit d'appliquer la proposition A.2.9 avec $T = \mathbf{reg}(A)$. □

Proposition 4.5.7 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$. Pour tout $i \in [0, n-1]$ on désigne par J_{i+1} l'extension du saturé de $T \cap \mathbf{P}_{i+1}$ dans $A_i[x_i + 1]$ par l'homomorphisme F_i. Alors on a*

$$A_{i+1} \simeq \mathrm{fr}(A_i[x_{i+1}]/J_{i+1}) \ .$$

Preuve. On désigne par S_i l'ensemble des éléments réguliers de $B_i = \mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i)$. On a ainsi $A_i = {S_i}^{-1}B_i$. En notant $\overline{S}$ l'image de S dans $B_i[x_{i+1}]/(I_{i+1}/I_i)$, on a d'après le lemme 4.5.5 puis la proposition A.2.13

$$\begin{aligned} A_i[x_{i+1}]/J_{i+1} &\simeq {S_i}^{-1}B_i[x_{i+1}]/J_{i+1} \\ &\simeq \overline{S_i}^{-1}B_i[x_{i+1}]/(I_{i+1}/I_i)\ . \end{aligned}$$

On veut utiliser l'isomorphisme donné par le lemme 4.5.6 en prenant $B_i[x_{i+1}]/(I_{i+1}/I_i)$ pour A. Il suffit de s'assurer que $\overline{S_i} \subseteq \mathbf{reg}(B_i[x_{i+1}]/(I_{i+1}/I_i))$, ce qui revient à vérifier que l'intersection de S_i avec tout idéal premier de $B_i[x_{i+1}]$ associé à I_{i+1}/I_i est vide. Soit $\alpha \in S_i$. C'est l'image canonique d'un élément p de $\mathbf{P}_i$ tel que pour tout idéal premier $\mathcal{P}$ de I_i, on a $p \notin \mathcal{P}$. Il résulte du théorème 4.3.6 que si $\mathcal{P}' \in \mathsf{ass}(I_{i+1})$, alors $p \notin \mathcal{P}'$. On en déduit que α n'appartient à aucun idéal premier associé à I_{i+1}/I_i dans $B_i[x_{i+1}]$, ainsi qu'on le désirait. Le lemme 4.5.6 entraîne alors

$$\begin{aligned} \mathrm{fr}(A_i[x_{i+1}]/J_{i+1}) &\simeq \mathrm{fr}(B_i[x_{i+1}]/(I_{i+1}/I_i)) \\ &\simeq \mathrm{fr}((\mathbf{P}_{i+1}/I_i[x_{i+1}])/(I_{i+1}/I_i[x_{i+1}])) \\ &\simeq \mathrm{fr}(\mathbf{P}_{i+1}/I_{i+1})\ , \end{aligned}$$

qui correspond à l'isomorphisme de la proposition. □

Lemme 4.5.8 *Avec les notations ci-dessus, posons $I_i = \mathsf{sat}_i(T \cap \mathbf{P}_i)$. Alors l'idéal J_i engendré par $F_{i-1}(I_i)$ a pour image réciproque I_i lui-même. De plus, si $x_i \in \mathsf{algVar}(T)$ alors $J_i = \langle F_{i-1}(T_{x_i})\rangle$, sinon J_i est réduit à 0.*

Preuve. Notons $B_{i-1} = (\mathbf{P}_{i-1}/I_{i-1})$ et S'_{i-1} l'ensemble des éléments réguliers de B_{i-1}. On désigne par I'_i l'image de I_i dans $B_{i-1}[x_i]$. C'est un idéal de $B_{i-1}[x_i]$ d'image réciproque I_i. De plus, il résulte du théorème 4.3.6 que pour tout idéal premier $\mathcal{P}'$ associé à I'_i on a $\mathcal{P}' \cap S'_{i-1} = \emptyset$. L'idéal J_i étant l'extension de I'_i dans l'anneau ${S'_{i-1}}^{-1}(B_{i-1}[x_i]$, on en déduit avec la proposition A.2.22 que I'_i est le contracté de J_i, et par suite que $I - i$ est l'image réciproque de J_i par $Fi - 1$. On a ainsi prouvé la première partie du lemme.

Supposons maintenant que $x_i \in \mathsf{algVar}(T)$ et notons $f = T_{x_i}$ et $h = \mathsf{init}(f)$. L'idéal engendré par $F_{i-1}(f)$ est évidemment inclus dans J_i. Réciproquement, soit $p \in \mathsf{sat}_i(T \cap \mathbf{P}_i)$. D'après la proposition 4.3.2, il existe m tel que $h^m p \in \mathsf{sat}_i(T \cap \mathbf{P}_{i-1}) + \langle f\rangle_{\mathbf{P}_i}$. On a par conséquent $F_{i-1}(h)^m F_{i-1}(p) \in \langle F_{i-1}(f)\rangle$. L'inversibilité de $F_{i-1}(h)$ (remarque 4.5.4) entraîne $F_{i-1}(p) \in \langle F_{i-1}(f)\rangle$. Il en résulte $J_i \subseteq \langle F_{i-1}(f)\rangle$.

Le cas où x_i est une variable transcendante par rapport à T est immédiat. □

Théorème 4.5.9 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$. Alors la suite d'anneaux $(A_0, A_1, \ldots, A_n)$ définis par $A_i = \mathrm{fr}(\mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i))$ est une tour d'extensions simples du corps k. On dit que c'est la* tour associée *à T.*

Preuve. En appliquant le lemme 4.5.8 dans la relation donnée par la proposition 4.5.7, on obtient selon le cas $A_i \simeq \mathrm{fr}(A_{i-1}[x_i])$ ou bien $A_i \simeq \mathrm{fr}(A_{i-1}[x_i]/\langle F_{i-1}(T_{x_i})\rangle)$. Il résulte de la remarque 4.5.4 que $F_{i-1}(T_{x_i})$ est unitaire donc la suite $(A_0, A_1, \ldots, A_n)$ satisfait aux conditions de la définition. □

On peut ainsi associer à tout ensemble triangulaire régulier une tour d'extensions simples qui, dans le cas où elle est séparable, permet d'obtenir la propriété suivante.

Proposition 4.5.10 *Avec les notations du théorème 4.5.9, la tour $A_0, A_1, \ldots, A_n$ est séparable si et seulement si l'idéal $\mathsf{sat}(T)$ est radical.*

Preuve. On reprend les notations du lemme 4.5.8. Par définition, si la tour est séparable alors J_n est un idéal radical de $A_{n-1}[x_n]$. L'idéal $\mathsf{sat}(T)$ qui est le contracté de J_n par F_{n-1} est donc radical d'après la proposition A.1.4. Réciproquement, supposons que $\mathsf{sat}(T)$ est radical. On a alors encore selon la proposition A.1.4

$$\begin{aligned} F_{n-1}^{-1}(\sqrt{\langle J_{n-1}\rangle}) &= \sqrt{F_{n-1}^{-1}(\langle J_{n-1}\rangle)} \\ &= \sqrt{\mathsf{sat}(T)} \\ &= \mathsf{sat}(T)\ . \end{aligned}$$

On en déduit $\sqrt{\langle J_{n-1}\rangle} = F_{n-1}(\mathsf{sat}(T)) = \langle J_{n-1}\rangle$. □

On introduit ainsi la même terminologie pour les ensembles triangulaires que pour les tours.

Définition 4.5.11 *Un ensemble triangulaire régulier T est dit* séparable *si* $\mathsf{sat}(T)$ *est radical.*

On s'intéresse maintenant au problème réciproque de celui qui est évoqué dans le théorème 4.5.9. Autrement dit, on cherche à associer à une tour d'extensions simples de k un ensemble triangulaire régulier.

Proposition 4.5.12 *Soit $(A_0, A_1, \ldots, A_n)$ une tour d'extensions simples de k. Alors il existe un ensemble triangulaire régulier T de $\mathbf{P}_n$ tel que $(A_0, A_1, \ldots, A_n)$ soit la tour associée à T.*

Preuve. La construction se fait par induction sur n. Pour $n = 0$ il est clair que l'ensemble vide convient pour T. Soit $n > 0$. D'après l'hypothèse de récurrence on peut associer à $A_0, \ldots, A_{n-1}$ un ensemble triangulaire régulier T' de $\mathbf{P}_{n-1}$ tel que $A_{n-1} = \mathrm{fr}(\mathbf{P}_{n-1}/\mathsf{sat}_{n-1}(T'))$. Dans le cas où $A_n = \mathrm{fr}(A_{n-1}[x_n])$ on vérifie immédiatement avec le lemme 4.5.8 et la proposition 4.5.7 que $T = T'$ convient. Supposons maintenant que f est un polynôme de $A_{n-1}[x_n]$ tel que $A_n = \mathrm{fr}(A_{n-1}[x_n]/\langle f\rangle)$. On note S l'ensemble des éléments de $\mathbf{P}_{n-1}$ qui ne sont pas diviseurs de zéro modulo $\mathsf{sat}_{n-1}(T')$. Le polynôme f s'écrit

$$f = \sum_{j=0}^{d} (\overline{a_j}/\overline{s_j}) x_n^j$$

où $\overline{a_j}$ est la classe résiduelle dans $\mathbf{P}_{n-1}/\mathsf{sat}_{n-1}(T')$ d'un élément a_j de $\mathbf{P}_{n-1}$ et $\overline{s_j}$ est la classe d'un élément s_j de S. De plus le coefficient $a_d \in S$ par hypothèse. Puisqu'une mise en dénominateur commun ne modifie pas ces propriétés, on peut supposer que les s_j sont tous identiques; on note alors s cette valeur commune. Le polynôme $g = \sum_{j=0}^{d} (\overline{a_j}/1) x_n^j = (\overline{s}/1) f$ engendre dans $A_{n-1}[x_n]$ le même idéal que f puisque $(\overline{s}/1)$ est inversible. Soit t le polynôme de $\mathbf{P}_n$ défini par $t = \sum_{j=0}^{d} a_j x_n^j$. Alors $T = T' \cup \{t\}$ est un ensemble triangulaire régulier de $\mathbf{P}_n$. Puisque g est l'image de t dans $A_{n-1}[x_n]$, il résulte ici encore du lemme 4.5.8 et de la proposition 4.5.7 que T convient. □

Remarquons qu'il est aussi possible d'associer à un ensemble triangulaire régulier T une autre suite d'anneaux $(A'_0, A'_1, \ldots, A'_n)$, définie par

$$A'_i = \mathrm{fr}(\mathbf{P}_i/\sqrt{\mathsf{sat}_i(T \cap \mathbf{P}_i)})\ .$$

Nous avons vu que chaque anneau A'_i est alors un produit de corps. Disposerait-on avec la suite A'_i d'une tour d'extensions simples séparables ? La réponse est non car A'_i n'est pas même pas forcément une tour d'extensions simples. Considérons par exemple l'ensemble triangulaire régulier T de $\mathbf{P}_2$ suivant :

$$T = \{x_1^2 - x_1, x_2^2 - x_1\}\ .$$

On a

$$A'_1 = \mathrm{fr}(\mathbf{P}_1/\langle x_1^2 - x_1\rangle) \simeq k_1 \times k_2$$

où k_1 est le corps $\mathrm{fr}(\mathbf{P}_1/\langle x_1\rangle)$ et k_2 le corps $\mathrm{fr}(\mathbf{P}_1/\langle x_1 - 1\rangle)$. L'idéal engendré par l'image de $\sqrt{\mathsf{sat}(T)}$ dans l'anneau $A'_1[x_2] = k_1[x_2] \times k_2[x_2]$ est d'après ce qui précède, l'idéal

$$J = \sqrt{\langle F_1(x_2^2 - x_1)\rangle}\ .$$

L'image de $x_2^2 - x_1$ dans $k_1[x_2]$ est $f_1 = x_2^2$ et son image dans $k_2[x_2]$ est $f_2 = x_2^2 - 1$. On vérifie aisément que $\sqrt{\langle f_1\rangle_{k_1[x_2]}} = \langle x_2\rangle_{k_1[x_2]}$ et que l'idéal $\langle f_2\rangle_{k_2[x_2]}$ est radical. D'après le lemme 3.3.5, l'idéal J est donc engendré dans $k_1[x_2] \times k_2[x_2]$ par le couple $(x_2, x_2^2 - 1)$. Ce couple correspond au polynôme $x_1x_2^2 - (x_1 - 1)x_2 + x_1$ de $A_1[x_2]$ qui n'est pas unitaire, donc la condition (ii) de la définition 4.5.1 n'est pas remplie.

4.6 Équivalence de différentes notions

Les différents concepts attachés aux ensembles triangulaires qui ont été introduits dans ce chapitre se retrouvent dans le théorème ci-dessous pour fournir des caractérisations équivalentes d'ensembles triangulaires.

Théorème 4.6.1 *Pour tout ensemble triangulaire T non vide de $\mathbf{P}_n$ les conditions ci-dessous sont équivalentes :*

(i) T est un ensemble triangulaire régulier de $\mathbf{P}_n$,

(ii) T est une chaîne régulière de $\mathbf{P}_n$,

(iii) $\mathsf{red}_{\mapsto 0}(T) = \mathsf{sat}(T)$,

(iv) $\mathsf{sat}(T) \cap \mathbf{P}_i = \mathsf{sat}_i(T \cap \mathbf{P}_i)$ *pour tout* $i \in [0, n]$,

(v) T est un ensemble caractéristique au sens de Ritt de $\mathsf{sat}(T)$,

Preuve. L'équivalence entre les deux premières notions a déjà été donnée dans la proposition 4.4.12. Vérifions maintenant que $(i) \Leftrightarrow (iii)$ et $(i) \Leftrightarrow (iv)$. Si T est régulier, l'égalité (iii) a été établie dans le théorème 4.3.11 et la relation (iv) dans le théorème 4.3.4 Réciproquement, supposons que T ne soit pas régulier. Il existe un indice $i > 0$ tel que l'initial de T_{x_i} soit diviseur de zéro dans $\mathbf{P}_{i-1}/\mathsf{sat}_{i-1}(T_{x_i}^-)$. Posons $h = \mathsf{init}(T_{x_i})$. On dispose ainsi d'un polynôme $p \in \mathbf{P}_{i-1}$ tel que

$$p \notin \mathsf{sat}_{i-1}(T \cap \mathbf{P}_{i-1}) \tag{4.9}$$

et

$$hp \in \mathsf{sat}_{i-1}(T \cap \mathbf{P}_{i-1}) \ . \tag{4.10}$$

A partir de la relation (4.10) on obtient aisément que $p \in \mathsf{sat}_i(T \cap \mathbf{P}_i)$ donc $p \in \mathsf{sat}(T)$. On en déduit conjointement avec la relation (4.9) que $\mathsf{sat}(T) \cap \mathbf{P}_{i-1} \neq \mathsf{sat}_{i-1}(T \cap \mathbf{P}_{i-1})$, ce qui prouve $(iv) \Rightarrow (i)$. De plus, la relation (4.9) entraîne aussi que $\mathsf{prem}(p, T_{x_i}^-) \neq 0$ donc $\mathsf{prem}(p, T) \neq 0$ puisque $p \in \mathbf{P}_{i-1}$. On a par conséquent $\mathsf{red}_{\mapsto 0}(T) \neq \mathsf{sat}(T)$ et ainsi $(iii) \Rightarrow (i)$.

On obtient facilement $(iii) \Leftrightarrow (v)$. En effet, par définition T est un ensemble caractéristique de $\mathsf{sat}(T)$ si et seulement si $\mathsf{sat}(T) \subseteq \mathsf{red}_{\mapsto 0}(T)$. L'équivalence voulue résulte simplement du fait qu'on a toujours $\mathsf{red}_{\mapsto 0}(T) \subseteq \mathsf{sat}(T)$ (proposition 2.2.18). □

4.7 Ensembles triangulaires et bases de Gröbner

Nous étudions dans cette section la construction d'ensembles triangulaires avec des propriétés minimales à partir d'une base de Gröbner lexicographique minimale G d'un idéal I. On montre d'abord que lorsque I est premier, on peut extraire immédiatement de G au moins un ensemble triangulaire régulier T tel que $I = \mathsf{sat}(T)$ (théorème 4.7.4). Lorsque I n'est pas premier on ne dispose pas de propriété aussi forte. Le théorème 4.7.14 précise qu'on peut cependant toujours extraire facilement de G au moins un ensemble caractéristique au sens de Ritt de I qu'on appelle *ensemble médian associé* à I (définition 4.7.6). Ces résultats prolongent ceux de [ALM99] où est introduite la notion d'*ensemble médian* d'un système de générateurs d'un idéal I. Celle-ci correspond à un cas particulier d'ensemble médian associé à I. Notre généralisation montre qu'il y a éventuellement plusieurs ensembles caractéristiques disponibles dans la base de Gröbner G et permet de choisir parmi ceux-ci. Elle fait aussi apparaître le rôle principal des initiaux des polynômes de G dans ces problèmes, et a ainsi l'avantage de limiter les calculs de pseudo-restes sur ces initiaux au lieu de les effectuer sur les polynômes eux-mêmes.

Notation 4.7.1 *Nous supposons dans cette section que I est un idéal propre de $\mathbf{P}_n$. Nous utilisons les notations de l'annexe B présentant les bases de Gröbner. L'ordre lexicographique sur les monômes de $\mathbf{P}_n$, associé à l'ordre de variables $x_1 < \cdots < x_n$, est noté $\prec_{lex}$ (définition B.0.16). Pour cet ordre, le monôme de tête d'un polynôme p de $\mathbf{P}_n$ est noté $\mathsf{lm}(p)$. Toutes les références aux bases de Gröbner dans cette partie seront relatives à cet ordre. On désigne par G la base de Gröbner minimale de I pour l'ordre $\prec_{lex}$. Soit v une variable de $\{x_1, \ldots, x_n\}$. On pose*

$$G_v = \{g \in G \mid \mathsf{mvar}(g) = v\} \quad \text{et} \quad G_v^- = \{g \in G \mid \mathsf{mvar}(g) < v\} \ .$$

Enfin, on note $\mathsf{algVar}(G)$ l'ensemble des variables v telles que $G_v \neq \emptyset$.

Lemme 4.7.2 *Soit G une base de Gröbner minimale pour l'ordre lexicographique. Alors pour tout polynôme $g \in G$ on a $\mathsf{init}(g) \notin \langle G \rangle$.*

Preuve. Posons $h = \mathsf{init}(g)$ et supposons au contraire que $h \in \langle G \rangle$. Alors il existe $g' \in G \setminus \{g\}$ tel que $\mathsf{lm}(h)$ soit divisible par $\mathsf{lm}(g')$. Puisque $\mathsf{lm}(h)$ divise $\mathsf{lm}(g)$ on en déduit alors que $\mathsf{lm}(g')$ divise $\mathsf{lm}(g)$, ce qui contredit le fait que G est une base minimale (voir la définition B.0.18). □

Lemme 4.7.3 *Soit G une base de Gröbner minimale qui engendre un idéal premier de $\mathbf{P}_n$. Pour tout ensemble triangulaire T tel que $T \subseteq G$ on a*

$$\mathsf{sat}(T) \subseteq \langle G \rangle \ .$$

Preuve. Posons $T = \{g_1, \ldots, g_s\}$ et $h_i = \mathsf{init}(g_i)$ pour tout $i \in [1, s]$. On a $\langle T \rangle \subseteq \langle G \rangle$ donc

$$\mathsf{sat}(T) = \langle T \rangle : (h_1 \ldots h_s)^\infty \subseteq \langle G \rangle : (h_1 \ldots h_s)^\infty \ .$$

Puisque par hypothèse $\langle G \rangle$ est premier, il résulte du lemme 4.7.2 que $h_1 \ldots h_s \notin \langle G \rangle$ et par conséquent $\langle G \rangle : (h_1 \ldots h_s)^\infty = \langle G \rangle$ (proposition A.1.15), ce qui permet de conclure. □

Théorème 4.7.4 *Soit I un idéal premier de $\mathbf{P}_n$ et G une base de Gröbner minimale de I. Soit T un ensemble triangulaire extrait de G tel que :*

- $\mathsf{algVar}(T) = \mathsf{algVar}(G)$,
- *pour toute variable $v \in \mathsf{algVar}(T)$ le polynôme T_v est un élément de G_v de degré minimal en v.*

Alors T est un ensemble triangulaire régulier et

$$I = \mathsf{sat}(T) = \mathsf{red}_{\mapsto 0}(T) \ . \tag{4.11}$$

On dira que T est un ensemble triangulaire régulier extrait de G, *ou* associé *à I.*

Preuve. On montre d'abord que $I \subseteq \mathsf{red}_{\mapsto 0}(T)$ par l'absurde. Soit $p \in I$ et $r = \mathsf{prem}(p, T)$. La "remainder formula" (proposition 2.2.10) entraîne $r \in I$ donc il existe $g \in G$ tel que $\mathsf{lm}(g)$ divise $\mathsf{lm}(r)$. Posons $v = \mathsf{mvar}(g)$. Par construction de T, la variable v est algébrique par rapport à T et $\mathsf{mdeg}(T_v) \leq \mathsf{mdeg}(g)$. Supposons $r \neq 0$. Le polynôme r est réduit par rapport à T donc son monôme de tête l'est aussi. Par conséquent $\mathsf{lm}(g)$ est réduit par rapport à T; en particulier on a $\mathsf{mdeg}(g) < \mathsf{mdeg}(T_v)$, en contradiction avec ce qui précède. On en déduit que $r = 0$.

Il résulte ensuite de la proposition 2.2.18 que

$$I \subseteq \mathsf{red}_{\mapsto 0}(T) \subseteq \mathsf{sat}(T) \ .$$

Puisque le lemme 4.7.3 assure que $\mathsf{sat}(T) \subseteq I$, on en déduit les égalités (4.11). Le fait que T soit régulier est conséquence directe du point (iii) du théorème 4.6.1. □

Exemple 4.7.5 Soit $n = 4$. On considère les polynômes suivants :

$$\begin{aligned} p_1 &= x_2x_3 - x_1 \\ p_2 &= x_1x_4 - x_2 \\ p_3 &= x_3x_4 - 1 \end{aligned}$$

L'ensemble $G = \{p_1, p_2, p_3\}$ est une base de Gröbner minimale d'un idéal premier. Il existe deux ensembles triangulaires réguliers extraits de G qui sont $T_1 = \{p_1, p_2\}$ et $T_2 = \{p_1, p_3\}$. On a ainsi $\langle G\rangle = \mathsf{sat}(T_1) = \mathsf{sat}(T_2)$. Les zéros de G forment la variété irréductible

$$V = \{(t_1, t_2, t_1/t_2, t_2/t_1) \mid t_1, t_2 \in \mathbb{C} \setminus \{0\}\} .$$

Bien que $p_2 \prec_{lex} p_3$, l'ensemble T_2 peut se révéler plus intéressant que l'ensemble T_1 car on a aussi $\langle G\rangle = \langle T_2\rangle$ alors que $\mathbf{V}(T_1) = V \cup \{(0, 0, t_3, t_4) \mid t_3, t_4 \in \mathbb{C}\}$.

Remarquons cependant qu'on ne peut pas toujours trouver un ensemble triangulaire régulier T extrait de G tel que $\langle G\rangle = T$. Soit $T = \{x_2^2x_3 - x_1^2, x_1x_4 - x_2\}$ et $I = \mathsf{sat}(T)$. L'idéal I admet pour base de Gröbner minimale

$$G = \{x_2^2x_3 - x_1^2, x_1x_4 - x_2, x_2x_3x_4 - x1, x_3x_4^2 - 1\} .$$

On vérifie facilement que l'idéal I est premier. Les ensembles triangulaires réguliers associés à I sont T et $T' = \{x_2^2x_3 - x_1^2, x_2x_3x_4 - x_1\}$ mais le calcul des bases de Gröbner des idéaux $\langle T\rangle$ et $\langle T'\rangle$ montrent que ceux-ci sont strictement inclus dans I.

Dans le cas général où I n'est pas premier, on ne peut plus extraire aussi facilement que dans le théorème 4.7.14, un ensemble triangulaire qui ait des propriétés minimales de la base de Gröbner lexicographique de I. La construction inductive de la définition 4.7.6 ci-dessous, qui ne demande qu'un simple calcul de pseudo-reste sur les initiaux de polynômes de G, permet quand même d'exhiber au moins un ensemble caractéristique de Ritt de I.

Définition 4.7.6 *Soit I un idéal propre de $\mathbf{P}_n$ et G une base de Gröbner minimale de I. On appelle* ensemble médian extrait *de G, ou* ensemble médian associé *à I, tout ensemble triangulaire T de $\mathbf{P}_n$ qui vérifie les conditions suivantes :*

(i) si $n = 0$ alors $T = \emptyset$

(ii) si $n > 0$ alors $T' = T^-_{x_n}$ est un ensemble médian extrait de $G^-_{x_n}$ et on distingue deux cas :

- *(a) si $\{\mathsf{init}(g) \mid g \in G_{x_n}\} \subseteq \mathsf{red}_{\mapsto 0}(T')$ alors $T = T'$*
- *(b) sinon $T = T' \cup \{f\}$ où f est un polynôme de G_{x_n} de degré minimal en x_n parmi les éléments $g \in G_{x_n}$ vérifiant $\mathsf{prem}(\mathsf{init}(g), T') \neq 0$.*

Tout idéal propre de $\mathbf{P}_n$ admet au moins un ensemble médian associé. La proposition suivante montre que la définition 4.7.6 généralise le cas où I est un idéal premier que nous avons étudié plus haut.

Proposition 4.7.7 *Soit I un idéal premier de $\mathbf{P}_n$ et T un ensemble triangulaire. Alors T est un ensemble triangulaire régulier associé à I si et seulement si T est un ensemble médian associé à I.*

Preuve. On le vérifie par induction sur l'entier n. C'est trivial pour le cas $n = 0$ qui correspond à $I = \{0\}$. Supposons $n > 0$. Soit G la base de Gröbner minimale de I. Le cas $G_{x_n} = \emptyset$ est immédiat. Dans le cas contraire tout polynôme $g \in G_{x_n}$ est tel que $\mathsf{init}(g) \notin I \cap \mathbf{P}_{n-1}$ (lemme 4.7.2). Puisque par induction $T^-_{x_n}$ est régulier et $I \cap \mathbf{P}_{n-1} = \mathsf{sat}(T^-_{x_n})$, on a $\mathsf{prem}(\mathsf{init}(g), T^-_{x_n}) \neq 0$ selon le théorème 4.3.11. Par conséquent les éléments de G_{x_n} de degré minimal en x_n sont exactement ceux qui vérifient la condition (b) de la définition 4.7.6, ce qui entraîne l'équivalence voulue. □

Revenons au cas général des ensembles médians pour lequel nous donnons quelques exemples. Nous en dégagons ensuite les propriétés principales.

Exemple 4.7.8 Soit $n = 4$ et $F = \{x_1x_2, x_2x_3, x_3x_4\}$. On pose $I = \langle F \rangle$. Alors on a $G = F$ et le seul ensemble médian associé à I est $\{x_1x_2, x_3x_4\}$.

Exemple 4.7.9 Soit $n = 5$ et $T = \{x_2^2 - x_1, x_3^2 - x_2x_3, (x_3 + x_2)x_4, (x_3 - x_2)x_5\}$. La base de Gröbner minimale de l'idéal I engendré par T est $G = F \cup \{x_1x_4, x_2x_4x_5\}$. On trouve ici deux ensembles médians extraits de G. Le premier est T lui-même et le second est $T' = \{x_2^2 - x_1, x_3^2 - x_2x_3, x_1x_4, (x_3 - x_2)x_5\}$.

Exemple 4.7.10 Soit $n = 4$. On pose $F = \{x_2^2 - x_1, x_3^2 - 2x_2x_3 + x1, (x_3 - x_2)x_4\}$. L'idéal $I = \langle F \rangle$ admet F comme base de Gröbner minimale. L'unique ensemble médian extrait de F est F lui-même. Notons que $\mathbf{W}(F) = \emptyset$ puisque $(x_3 - x_2)$ appartient au radical de $F^-_{x_4}$. Contrairement au cas où I est un idéal premier, il n'est donc pas possible d'assurer qu'un ensemble médian associé à I soit consistant.

Remarque 4.7.11 Même dans le cas où I est radical, les ensembles médians associés à I peuvent être inconsistants. Avec $n = 4$, prenons $T = \{x_1^2 - 2, x_2^2 - 2, (x_1 - x_2)x_3, (x_1 + x_2)x_4\}$ et $I = \langle T \rangle$. On a alors $G = T \cup \{x_3x_4\}$. Le seul ensemble médian extrait de G est T car $\mathsf{prem}(x_3x_4, T_{x_3}) = 0$. On vérifie sans peine que le produit des initiaux de T_{x_3} et T_{x_4} appartient à l'idéal engendré par $T^-_{x_3}$ donc $\mathbf{W}(T) = \emptyset$.

Proposition 4.7.12 *Tout ensemble médian associé à un idéal propre non nul de $\mathbf{P}_n$ est un ensemble triangulaire standard.*

Preuve. La construction de T donnée dans la définition 4.7.6 ci-dessus entraîne immédiatement que T satisfait les conditions de la définition 2.2.14. □

Proposition 4.7.13 *Soit I un idéal propre de $\mathbf{P}_n$. Tout ensemble médian T associé à I est tel que*

$$T \subseteq I \subseteq \mathsf{red}_{\mapsto 0}(T) .$$

Preuve. La première inclusion est triviale. Passons à la seconde. On note G la base de Gröbner minimale de I. Soit $p \in I$ et $r = \mathsf{prem}(p, T)$. Puisque $T \subseteq I$ on a $r \in I$. Il existe donc $g \in G$ tel que $\mathsf{lm}(r)$ est multiple de $\mathsf{lm}(g)$ (proposition B.0.20). Supposons que r est non nul. Puisque $\mathsf{red?}(r, T)$ on a aussi $\mathsf{red?}(\mathsf{lm}(r), T)$ et

$$\mathsf{red?}(\mathsf{lm}(g), T) . \tag{4.12}$$

Posons $v = \mathsf{mvar}(g)$. Si v est algébrique par rapport à T on a donc $\mathsf{mdeg}(g) < \mathsf{mdeg}(T_v)$ (voir la remarque 2.2.12). Il résulte alors de la définition 4.7.6 que $\mathsf{prem}(\mathsf{init}(g), T_v^-) = 0$. Et on a clairement la même relation lorsque v est transcendante par rapport à T. La proposition 2.2.13 implique alors que $\mathsf{lm}(g)$ n'est pas réduit par rapport à T, ce qui contredit (4.12). On en conclut que r est nul. □

Théorème 4.7.14 *Soit I un idéal propre de $\mathbf{P}_n$. Tout ensemble médian associé à I est un ensemble caractéristique de Ritt de I.*

Preuve. Cette affirmation est une conséquence directe des propositions 4.7.13 et 4.7.12 et du théorème 4.2.11. □

Les propriétés des ensembles médians sont bien moins fortes en général que dans le cas d'un idéal premier. Le théorème 4.7.14 montre cependant que tout idéal I de $\mathbf{P}_n$ possède un ensemble caractéristique de Ritt et qu'un tel ensemble n'est pas plus difficile à calculer qu'une base de Gröbner lexicographique de I.

Remarque 4.7.15 Si on dispose d'un ensemble médian T associé à I alors on peut aisément tester si un sous-ensemble C de I est un ensemble caractéristique de Ritt de I. Il suffit de vérifier que C est un ensemble triangulaire standard tel que $C \sim_r T$.

Nous distinguons dans la définition suivante l'un des ensembles médians extraits d'une base de Gröbner. Celui-ci a comme propriété supplémentaire d'être initialement réduit. Cette définition permet aussi de faire finalement le lien avec la définition d'ensemble médian de [ALM99].

Définition 4.7.16 *Soit I un idéal propre de $\mathbf{P}_n$ et G la base de Gröbner minimale de I. L'*ensemble médian *de I, noté $\mathcal{M}(I)$, est l'ensemble triangulaire défini de manière unique par*

(i) si $n = 0$ alors $T = \emptyset$

(ii) si $n > 0$ alors $T' = T_{x_n}^-$ est l'ensemble médian de $I \cap \mathbf{P}_{n-1}$ et on distingue deux cas :

- *(a) si $\{\mathsf{init}(g) \mid g \in G_{x_n}\} \subseteq \mathsf{red}_{\mapsto 0}(T')$ alors $T = T'$*
- *(b) sinon $T = T' \cup \{g\}$ où g est le plus petit polynôme de G_{x_n} par rapport à l'ordre $\prec_{lex}$ tel que $\mathsf{prem}(\mathsf{init}(g), T') \neq 0$.*

Proposition 4.7.17 *L'ensemble médian $\mathcal{M}(I)$ est initialement réduit.*

Preuve. Soit G la base de Gröbner minimale de I. On prouve la proposition par l'absurde. Supposons que $T = \mathcal{M}(I)$ ne soit pas initialement réduit. Il existe alors une variable $v \in \mathsf{algVar}(T)$ telle que $g = T_v$ ne soit pas initialement réduit par rapport à T_v^-. Posons $p = \mathsf{prem}(g, T_v^-)$. On a ainsi $p \prec_{lex} g$ et $p \in I$.

Puisque T est un ensemble triangulaire standard on a $\mathsf{prem}(\mathsf{init}(g), T_v^-) \neq 0$ et il résulte de la proposition 2.1.17 que $\mathsf{deg}(p, v) = \mathsf{mdeg}(g)$. On sait avec la proposition 4.7.13 que $p \notin \langle G_v^- \rangle$ car $\mathsf{prem}(p, T_v^-) = p \neq 0$. Par conséquent le monôme de tête de p est divisible par le monôme de tête d'un polynôme $g' \in G_v$ tel que $g' \prec_{lex} g$. On en conclut que $\mathsf{prem}(g', T_v^-) = 0$ et donc que $\mathsf{lm}(g')$ n'est pas réduit par rapport à T_v^- d'après la proposition 2.2.13. On aboutit ainsi à une contradiction puisque par construction p est réduit par rapport à T_v^-. □

La proposition 4.7.18 ci-dessous montre que si $T = \mathcal{M}(I)$ et $v \in \mathsf{algVar}(T)$ alors T_v est aussi le plus petit polynôme g de G_v pour l'ordre de Ritt qui vérifie $\mathsf{prem}(g, T_v^-) \neq 0$.

Proposition 4.7.18 *Soit I un idéal propre non nul de $\mathbf{P}_n$ et G sa base de Gröbner minimale. Soit $g \in \mathcal{M}(I)$ tel que $\mathsf{mvar}(g) = v$. Alors pour tout $g' \in G$ tel que $g' \prec_{lex} g$ on a $\mathsf{prem}(g', T_v^-) = 0$.*

Preuve. Posons $T = \mathcal{M}(I)$. Si $\mathsf{deg}(g', v) < \mathsf{mdeg}(g)$ alors $\mathsf{prem}(g', T_v^-) = \mathsf{prem}(g', T) = 0$ d'après la proposition 4.7.13. Supposons maintenant que g' a pour variable principale v et que $\mathsf{mdeg}(g') = \mathsf{mdeg}(g)$. Il résulte de la construction de l'ensemble médian de I que $\mathsf{prem}(\mathsf{init}(g'), T_v^-) = 0$. On en déduit avec la proposition 2.1.17 que $\mathsf{prem}(g', T_v^-) = \mathsf{prem}(\mathsf{tail}(g'), T_v^-)$. On est ainsi ramené au cas précédent, d'où $\mathsf{prem}(g', T_v^-) = 0$. □

La proposition suivante permet de constater que la distinction des cas (a) et (b) dans la définition 4.7.16 peut se faire indifféremment en calculant les pseudo-restes des polynômes de G_{x_n} par rapport à T' ou en ne calculant que les pseudo-restes de leurs initiaux.

Proposition 4.7.19 *Soit G une base de Gröbner lexicographique minimale de $\mathbf{P}_n$ et T un ensemble médian extrait de $G_{x_n}^-$. On a*

$$G_{x_n} \subseteq \mathsf{red}_{\mapsto 0}(T) \iff \{\mathsf{init}(g) \mid g \in G_{x_n}\} \subseteq \mathsf{red}_{\mapsto 0}(T) \ .$$

Preuve. L'implication directe est immédiate avec le corollaire 2.1.18. Réciproquement, si $\{\mathsf{init}(g) \mid g \in G_{x_n}\} \subseteq \mathsf{red}_{\mapsto 0}(T)$ alors par définition T est un ensemble médian de $\langle G \rangle$. La proposition 4.7.13 affirme alors que $\langle G \rangle \subseteq \mathsf{red}_{\mapsto 0}(T)$, et en particulier $G_{x_n} \subseteq \mathsf{red}_{\mapsto 0}(T)$. □

Remarque 4.7.20 La définition de l'ensemble médian d'un idéal I dans [ALM99] correspond à la définition 4.7.16 donnée plus haut où les termes $\mathsf{init}(g)$ sont à remplacer par g. Les propositions 4.7.18 et 4.7.19 montrent par conséquent que les deux définitions sont en fait équivalentes.

Chapitre 5

Calcul modulo un ensemble triangulaire et décomposition triangulaire

Résumé

Ce chapitre présente les algorithmes qui permettent de calculer *modulo un ensemble triangulaire régulier* T, ce qui ici, signifie effectuer des calculs avec des polynômes en une variable à coefficients dans le produit de corps $\mathcal{A}(T) = \mathrm{fr}(\mathbf{P}_n/\sqrt{\mathsf{sat}(T)})$ défini par T. Ces algorithmes permettent ensuite de construire des algorithmes de décomposition triangulaire de systèmes de polynômes. Ils utilisent le principe de scindage dynamique que nous avons exposé dans la section 3.3.

On peut de manière similaire à [Laz91a] et [Mor97] les utiliser pour calculer une décomposition des zéros du système de départ en zéros réguliers d'ensembles triangulaires. Pour notre part, nous nous sommes investi dans le calcul de décompositions en clôtures de zéros réguliers d'ensembles triangulaires dont l'idée apparaît dans [Kal93].

Nous présentons d'abord le problème du scindage d'un ensemble triangulaire qui correspond à celui évoqué dans le chapitre 3 pour scinder un produit de corps afin de calculer des pgcd sur des produits de corps. Nous verrons qu'un algorithme de scindage de $\mathcal{A}(T)$ permet de définir un algorithme de calcul de pgcd *modulo* T, qui lui-même servira à résoudre notre problème de scindage. C'est sur ce principe que fonctionnent les algorithmes split et ggcd introduits par M. Kalkbrener [Kal93]. Notre présentation est différente et il nous semble qu'elle permet avec les résultats du chapitre 4 de mieux comprendre le travail qu'effectuent ces algorithmes. De plus, nous présentons un nouvel algorithme de calcul de pgcd modulo un ensemble triangulaire qui utilise la technique des sous-résultants pour plus d'efficacité. Notons que nous avons encore amélioré récemment cet algorithme par l'adaptation des techniques proposées par [Duc96].

Notre travail de validation mathématique de l'algorithme de calcul de pgcd de Kalkbrener nous a permis d'aller plus loin que lui. Nous utilisons le principe dynamique de son algorithme pour développer des algorithmes de calcul de partie sans facteur carré d'un polynôme et d'inversion modulo une chaîne régulière (sections 5.2 et 5.3).

Nous rappelons ensuite l'algorithme de décomposition triangulaire de [Kal95]. Les algorithmes de calcul de partie sans facteur carré et d'inversion cités ci-dessus nous permettent de modifier cet algorithme de décomposition pour obtenir des décompositions triangulaires avec des spécifications plus fortes.

Mentionnons pour finir que l'idée de calculer des parties sans facteur carré et d'inverser apparaît dans [Laz91a] pour calculer des décompositions triangulaires en zéros réguliers. Une mise en œuvre est proposée dans [MR95] puis [Mor97] où ces calculs et les calculs de pgcd au-dessus d'une tour d'extensions simples sont effectués de manière dynamique comme dans nos algorithmes, mais nécessitent l'inversion des initiaux des polynômes tout au long du calcul. Il nous a semblé préférable d'utiliser la normalisation uniquement dans le processus de construction d'un ensemble triangulaire. Nos décompositions triangulaires ne la font donc intervenir que dans le cas où on désire obtenir en sortie des ensembles triangulaires normalisés. En effet, nous nous sommes rendus compte que le calcul des coefficients de Bezout pouvait rendre le calcul de pgcd beaucoup plus coûteux. Les performances de nos implantations ont montré que notre choix était justifié.

Notation 5.0.21 *Dans ce chapitre T désigne un ensemble triangulaire régulier de $\mathbf{P}_n$. Nous avons montré dans la section 4.5 que l'anneau $\mathrm{fr}(\mathbf{P}_n/\sqrt{\mathsf{sat}(T)})$ est un produit de corps. Nous le désignerons désormais par $\mathcal{A}_n(T)$ ou simplement $\mathcal{A}(T)$ et nous utiliserons la notation $\mathsf{Rep}(T) = \sqrt{\mathsf{sat}(T)}$ introduite pour les chaînes régulières.*

Si $\{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ est l'ensemble des idéaux premiers associés à $\mathsf{sat}(T)$, on a d'après le théorème 4.4.14

$$\mathcal{A}(T) = \mathrm{fr}(\mathbf{P}_n/\mathcal{P}_1) \times \ldots \times \mathrm{fr}(\mathbf{P}_n/\mathcal{P}_r)\ .$$

On notera $\mathcal{K}(T)$ l'ensemble des corps associés à T, c'est-à-dire les $\mathrm{fr}(\mathbf{P}_n/\mathcal{P}_j)$ où $j \in [1, r]$.

Pour travailler avec les notations ci-dessus qui évitent les indices, nous introduisons une nouvelle variable x_{n+1} plus grande que x_n. Rappelons que si κ est un corps associé à T et p un polynôme de $\mathbf{P}_{n+1}$ on note $\widehat{p}^{\kappa}$ l'image canonique de p dans $\mathrm{fr}(\mathbf{P}_n/\mathcal{P})[x_{n+1}]$ (notation 4.4.1). On désignera de plus l'image de p dans $\mathcal{A}(T)$ par $\widehat{p}^{T}$.

5.1 Scindage et pgcd modulo un ensemble triangulaire

Nous avons vu dans le chapitre 3 que tout couple de polynômes en une variable à coefficients dans un produit de corps admet un pgcd. Le problème est alors de déterminer effectivement un tel pgcd. Disposant d'un ensemble triangulaire régulier T, nous ne connaissons pas explicitement les corps associés à T. Un aperçu de la stratégie à la D5 sur laquelle nous nous appuyons pour le calcul d'un pgcd sur $\mathcal{A}(T)$ est présenté dans le chapitre 3. Cela nécessite de pouvoir distinguer pour un élément a donné dans $\mathcal{A}(T)$, les corps de $\mathcal{K}(T)$ dans lesquels l'image de a est nulle des autres, autrement dit ceux dans lesquels l'image de a est inversible. Il faut donc pouvoir *scinder* l'ensemble $\mathcal{K}(T)$. Nous verrons ci-dessous que ce problème du scindage et celui du pgcd se résolvent mutuellement dans le cadre des ensembles triangulaires réguliers et qu'on dispose alors d'outils pour résoudre des systèmes polynomiaux.

Bien que les travaux de Kalkbrener ne mentionnent pas la structure de produit de corps $\mathcal{A}(T)$ et ne dégagent pas une notion mathématique de pgcd comme la définition 5.1.3, on trouvera dans [Kal95] une étude complète dans le cadre des *systèmes de représentations* du problème du scindage d'un idéal radical où intervient un algorithme dont les principes sont à la base de l'algorithme de calcul de pgcd présenté plus bas. Les algorithmes split et gcd reprennent les idées de [Kal93]. Nous avons ajouté un algorithme monicPolynomial pour des raisons pratiques et un algorithme subResGcd qui remplace le processus euclidien de calcul de l'algorithme ggcd de Kalkbrener par un processus basé sur l'utilisation des sous-résultants et dont la gestion permet de plus d'éviter de répéter certains calculs. On obtient de cette manière une meilleure efficacité.

Commençons par définir plus précisément ce que nous entendons lorsque nous parlons de *scindage*.

Définition 5.1.1 *Soient $T, T_1, \ldots, T_m$ des ensembles triangulaires réguliers de $\mathbf{P}_n$. On dit que l'ensemble $\{T_1, \ldots, T_m\}$ est un T-*scindage *si les ensembles $\mathcal{K}(T_j)$ sont deux à deux* *disjoints et*

$$\mathcal{K}(T) = \bigcup_{j=1}^{m} \mathcal{K}(T_j)\ .$$

On peut dire de manière équivalente que $T_1, \ldots, T_m$ est un T-scindage si les idéaux premiers associés aux saturés des T_j sont tous distincts et que

$$\mathsf{ass}(\mathsf{sat}(T)) \ = \ \bigcup_{j=1}^{m} \mathsf{ass}(\mathsf{sat}(T_j))\ .$$

Nous avons mentionné plus haut que dans l'optique d'un calcul de pgcd, le fait intéressant était la capacité de séparer les corps $\mathrm{fr}(\mathbf{P}_n/\mathcal{P}_j)$ pour lesquels la composante d'un élément a de $\mathcal{A}(T)$ était nulle de ceux pour lesquels elle était non nulle. Nous introduisons dans ce but la définition suivante.

Définition 5.1.2 *Soit T un ensemble triangulaire régulier et $p \in \mathbf{P}_n$. On dit qu'un couple $N = \{T_1, \ldots, T_l\}$ et $I = \{T'_1, \ldots, T'_m\}$ de familles d'ensembles triangulaires réguliers est un* scindage *de T suivant p si $N \cup I$ est un T-scindage et si*

- $(\forall \kappa \in \mathcal{K}(N))\ \widehat{p}^{\kappa} = 0$,
- $(\forall \kappa \in \mathcal{K}(I))\ \widehat{p}^{\kappa} \neq 0$.

Lorsque $\mathrm{card}(\mathrm{N} \cup \mathrm{I}) = 1$ *on dit que T ne se scinde pas suivant p.*

Nous donnons en fin de section un algorithme $\mathsf{split}(T, p)$ qui calcule un scindage de T suivant un polynôme p. Cet algorithme utilise un calcul de pgcd modulo un ensemble triangulaire. Nous allons donc d'abord préciser ce que nous entendons par là.

Remarquons tout d'abord que tout couple (P_1, P_2) d'éléments de $\mathcal{A}(T)[x_{n+1}]$ admet un pgcd qui est l'image d'un polynôme de $\mathbf{P}_{n+1}$ par l'homomorphisme canonique. En effet, on dispose d'un pgcd G dans $\mathcal{A}(T)[x_{n+1}]$; il suffit alors de mettre tous les coefficients de G au même dénominateur puis de multiplier par ce dénominateur. On obtient ainsi clairement l'image d'un polynôme de $\mathbf{P}_{n+1}$ qui est un associé de G dans $\mathcal{A}(T)[x_{n+1}]$ donc un pgcd de (P_1, P_2) d'après le lemme 3.3.7.

Si $p_1, p_2 \in \mathbf{P}_{n+1}$, il existe donc un polynôme $g \in \mathbf{P}_{n+1}$ tel que $\widehat{g}^T$ est un pgcd de $\widehat{p_1}^T$ et $\widehat{p_2}^T$ dans $\mathcal{A}(T)[x_{n+1}]$. Un tel pgcd n'est pas généralement unitaire dans $\mathcal{A}(T)[x_{n+1}]$, c'est-à-dire que son coefficient de tête en x_{n+1} peut être nul dans certaines composantes du produit de corps $\mathcal{A}(T)$. De plus, tel que nous l'avons présenté, le calcul d'un pgcd dans $\mathcal{A}(T)[x_{n+1}]$ peut entraîner plusieurs branches de calcul et fournir en fait la valeur du pgcd sur des sous-produits de corps de $\mathcal{A}(T)[x_{n+1}]$. En vue de décomposer des systèmes il est alors préférable de remplacer $\mathcal{A}(T)[x_{n+1}]$ par les sous-produits de corps obtenus, qui seront représentés par des ensembles triangulaires réguliers. Cela permettra en même temps d'obtenir des pgcds unitaires qui seront plus aisément manipulables. On aboutit ainsi à la définition ci-dessous.

Définition 5.1.3 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$ et deux polynômes p_1 et p_2 de $\mathbf{P}_{n+1}$. On dit que $g \in \mathbf{P}_{n+1}$ est un* pgcd de p_1 et p_2 modulo T *si $\widehat{g}^T$ est nul ou* *unitaire dans $\mathcal{A}(T)[x_{n+1}]$ et si $\widehat{g}^T$ est un pgcd de $\widehat{p_1}^T$ et $\widehat{p_2}^T$. Plus généralement, on dit que $\{(g_1, T_1), \ldots, (g_m, T_m)\}$ est un* pgcd de p_1 et p_2 modulo T *si les conditions suivantes sont réalisées :*

(i) $\{T_1, \ldots, T_m\}$ *est un T-scindage,*

(ii) $\widehat{g_j}^{T_j}$ *est nul ou unitaire dans $\mathcal{A}(T_j)$ pour tout $j \in [1, m]$,*

(iii) $\widehat{g_j}^{T_j}$ *est un pgcd de $\widehat{p_1}^{T_j}$ et $\widehat{p_2}^{T_j}$ pour tout $j \in [1, m]$.*

Supposons que pour tout $i \in [0, n-1]$ on dispose d'un algorithme $\mathsf{gcd}_i(p_1, p_2, T)$ qui calcule pour tout ensemble triangulaire régulier T de $\mathbf{P}_i$ et tous $p_1, p_2 \in \mathbf{P}_{i+1}$ un pgcd de p_1 et p_2 modulo T. Remarquons qu'un tel algorithme existe pour $i = 0$ puisqu'on retrouve alors la notion de pgcd sur le corps k. Nous allons construire un algorithme $\mathsf{monicPolynomial}(p, T)$ qui, à partir d'un polynôme $p \in \mathbf{P}_{n+1}$, scinde l'ensemble triangulaire T si l'image de p modulo $\mathcal{A}(T)$ n'est pas unitaire. Ce nouvel algorithme permet alors de construire un algorithme $\mathsf{gcd}_n(p_1, p_2, T)$. Précisons que dans les boucles des algorithmes qui suivent, *itérer* signifie que le reste du corps de la boucle est ignorée et qu'on passe directement à l'itération suivante.

Proposition 5.1.4 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$ et $p \in \mathbf{P}_{n+1}$. Alors l'algorithme* $\mathsf{monicPolynomial}(p, T)$ *ci-dessous calcule une famille de couples $\{(p_1, T_1), \ldots, (p_m, T_m)\}$ telle que $\{T_1, \ldots, T_m\}$ est un T-scindage et $p_1, \ldots, p_m$ sont des polynômes de $\mathbf{P}_{n+1}$ tels que pour tout $j \in [1, m]$ on a*

(i) $\widehat{p_j}^{T_j}$ *est nul ou unitaire dans $\mathcal{A}(T_j)$,*

(ii) $\widehat{p}^{T_j} = \widehat{p_j}^{T_j}$.

- $\mathsf{monicPolynomial}(p, T) ==$
  - si $p \in k$ alors retourner $\{(p, T)\}$
  - $\Phi := \emptyset$
  - $x_i := \mathsf{mvar}(p)$
  - si $x_i \in \mathsf{algVar}(T)$ alors
    - pour $(g, U) \in \mathsf{gcd}_{i-1}(p, T_{x_i}, T^-_{x_i})$ faire
      - si $g \in \mathbf{P}_{i-1}$ alors $\Phi := \Phi \cup \{(p, U \cup \{T_{x_i}\})\}$, itérer
      - $\Phi := \Phi \cup \{(0, U \cup \{g\})\}$
      - si $\mathsf{mdeg}(g) < \mathsf{mdeg}(T_{x_i})$ alors
        - $q := \mathsf{pquo}(T_{x_i}, g)$
        - $\Phi := \Phi \cup \mathsf{monicPolynomial}(p, U \cup \{q\})$
  - sinon
    - pour $(h, U) \in \mathsf{monicPolynomial}(\mathsf{init}(p), T^-_{x_i})$ faire
      - si $h \neq 0$ alors
        - $\Phi := \Phi \cup \{(p, U)\}$
      - sinon
        - $\Phi := \Phi \cup \mathsf{monicPolynomial}(\mathsf{tail}(p), U)$
  - retourner $\{(p, U \cup T^+_{x_i}) \mid (p, U) \in \Phi\}$.

Alors pour tout ensemble triangulaire régulier T, si p_1 et p_2 sont des polynômes de $\mathbf{P}_{n+1}$, l'algorithme $\mathsf{gcd}_n(p_1, p_2, T)$ ci-dessous calcule un pgcd de p_1 et p_2 modulo T. On dispose ainsi par induction des algorithmes monicPolynomial et gcd pour tout entier n.

- $\mathsf{gcd}_n(p_1, p_2, T) ==$
  - si $p_1 \prec_r p_2$ alors échanger p_1 et p_2
  - $\Theta := \emptyset$
  - pour $(p, U) \in \mathsf{monicPolynomial}(p_2, T)$ faire
    - si $p = 0$ alors $\Theta := \Theta \cup \mathsf{monicPolynomial}(p_1, U)$ et itérer
    - si $p \in \mathbf{P}_n$ alors $\Theta := \Theta \cup \{(p_2, U)\}$
    - sinon $\Theta := \Theta \cup \mathsf{gcd}_n(\mathsf{prem}(p_1, p), p, U)$
  - retourner Θ.

[Kal95] présente un algorithme pour calculer des pgcds d'un ensemble de polynômes *modulo une chaîne régulière*. L'algorithme gcd ci-dessus effectue le même travail pour deux polynômes que celui donné dans [Kal95]. Nous précisons de plus ici quel sens mathématique il faut donner au terme de *pgcd* employé par Kalkbrener, alors que l'auteur s'est principalement appuyé pour cette appellation de pgcd sur la similarité de structure de son algorithme avec celle de l'algorithme d'Euclide classique sur un corps.

Il est bien connu que l'utilisation de l'algorithme des sous-résultants ([Loo82]) pour le calcul de résultant ou de pgcd de polynômes sur un anneau intègre permet d'éviter une croissance exponentielle des coefficients des polynômes intermédiaires. Pour une implantation plus efficace du calcul de pgcd modulo un ensemble triangulaire, l'utilisation de techniques basées sur les sous-résultants semble alors naturelle.

Les spécifications sont les mêmes que pour l'algorithme ci-dessus, mais on suppose de plus que $\widehat{p_2}^T$ est unitaire et que $p_2 \prec_r p_1$ avec $\mathsf{mvar}(p_2) = x_{n+1}$. On l'utilise donc en pratique à l'intérieur de l'algorithme gcd précédent à la place de l'appel récursif. L'actualisation des coefficients δ, ψ, β en fin d'algorithme se fait exactement de la même manière que dans l'algorithme de base du calcul de pgcd avec les sous-résultants.

- $\mathsf{subResGcd}_n(p_1, p_2, T) ==$
  - $\delta := \mathsf{mdeg}(p_1) - \mathsf{mdeg}(p_2)$
  - $\psi :=$ -1; $\beta := (-1)^{\delta+1}$
  - $lts := [T]$
  - $\Theta := \emptyset$
  - Tant que lts non vide faire
    - $p := \mathsf{prem}(p_1, p_2)/\beta$
    - $lmp := \bigcup_{T' \in lts} \mathsf{monicPolynomial}(p, T')$
    - $lts := \emptyset$
    - Pour $(q, U) \in lmp$ faire
      - si $q = 0$ alors $\Theta := \Theta \cup \{(p_2, U)\}$ et itérer
      - si $q \in \mathbf{P}_n$ alors $\Theta := \Theta \cup \{(p, U)\}$ et itérer
      - si $\mathsf{mdeg}(q) < \mathsf{mdeg}(p)$ alors
        - réduire p_2 et q par rapport à U
        - $\Theta := \Theta \cup \mathsf{subResGcd}_n(p_2, q, U)$

itérer
$lts := lts \cup \{U\}$
$(p_1, p_2) := (p_2, q)$
actualiser (δ, ψ, β)
retourner Θ

Les algorithmes précédents permettent de disposer d'un algorithme de scindage d'un ensemble triangulaire régulier suivant un polynôme.

Proposition 5.1.5 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$ et $p \in \mathbf{P}_n$. L'algorithme* $\mathsf{split}_n(T, p)$ *ci-dessous calcule un scindage (N, I) de T suivant p.*

Il est possible qu'il suffise dans certains cas de ne calculer que l'ensemble N, qui représente les composantes de $\mathcal{A}(T)$ sur lesquelles p est nul, ou l'ensemble S regroupant les composantes sur lesquelles p est inversible. A partir de $\mathsf{split}_n(T, p)$, on dispose trivialement pour ces tâches respectives d'algorithmes qu'on nomme $\mathsf{nullComp}_n(T, p)$ et $\mathsf{invComp}_n(T, p)$.

- $\mathsf{split}_n(T, p) ==$
  si $p = 0$ alors retourner $(\{T\}, \emptyset)$
  si $p \in k$ alors retourner $(\emptyset, \{T\})$
  si $T \subseteq \mathbf{P}_{n-1}$
  alors
  si $p \in \mathbf{P}_{n-1}$ alors retourner $\mathsf{split}_{n-1}(T, p)$
  $N := \emptyset$
  $(N_0, I) := \mathsf{split}_{n-1}(T, \mathsf{init}(p))$
  pour $T' \in N_0$ faire
  $(N', I') := \mathsf{split}_n(T', \mathsf{tail}(p))$
  $N := N \cup N'$
  $I := I \cup I'$
  sinon
  $U := T \cap \mathbf{P}_{n-1}$
  $f := T_{x_n}$
  $\{(g_1, U_1), \ldots, (g_m, U_m)\} := \mathsf{gcd}_{n-1}(p, f, U)$
  $I := \{U_j \cup \{f\} \mid g_j \in \mathbf{P}_{n-1}\}$ (1)
  $N := \{U_j \cup \{g_j\} \mid g_j \notin \mathbf{P}_{n-1}\}$ (2)
  $J := \{j \in [1, m] \mid g_j \notin \mathbf{P}_{n-1}$ et $\mathsf{mdeg}(g_j) < \mathsf{mdeg}(f)\}$
  pour tout $j \in J$ faire
  $q := \mathsf{pquo}(f, g_j)$
  $I := I \cup \mathsf{invComp}_n(U_j \cup \{q\}, p)$ (3)
  retourner (N, I).

Le lecteur pourra se référer à [Kal93] ou [Kal95] pour la preuve de l'algorithme. Essayons d'en dégager les principes pour T non inclus dans $\mathbf{P}_{n-1}$. On peut vérifier aisément que la proposition 4.5.7 est valide lorsqu'on considère le radical du saturé de T au lieu du saturé lui-même. On a ainsi dans notre situation

$$\mathcal{A}_n(T) \simeq \mathrm{fr}(\mathcal{A}_{n-1}(U)[x_n]/\sqrt{\langle \widehat{f}^U \rangle}) \; .$$

Le fait que $\mathcal{A}_{n-1}(U)$ soit un produit de corps permet de se ramener par scindage au cas où $\mathcal{A}_{n-1}(U)$ est simplement un corps. Le calcul de pgcd consiste alors à rechercher les facteurs de $\widehat{f}^U$ qui sont communs avec $\widehat{p}^U$ et qui induisent des corps sur lesquels p est nul (ligne (2) de l'algorithme). Lorsque le pgcd est un élément de $\mathcal{A}_{n-1}(U)$, les polynômes $\widehat{f}^U$ et $\widehat{p}^U$ sont premiers entre eux et p est donc inversible dans $\mathcal{A}(U \cup \{f\})$ (ligne (1)). Mais si le pgcd g a pour variable principale x_n alors le pseudo-quotient de f par g ne fournit pas forcément des facteurs premiers avec p sur $\mathcal{A}_{n-1}(U)$. En effet, l'élément $\widehat{f}^U$ n'est pas à priori sans facteur carré. Pour être sûr d'isoler les facteurs premiers avec $\widehat{p}^U$ on doit relancer la recherche de scindage sur le pseudo-quotient comme l'exprime la ligne (3).

Remarque 5.1.6 Dans l'algorithme split et dans l'algorithme monicPolynomial la recherche récursive de scindages dûe au fait que les polynômes de l'ensemble triangulaire T ne sont pas sans facteur carré modulo le saturé des éléments de T de variable principale inférieure ne nous a pas semblé satisfaisante. En remarquant que nous avions ci-dessus les outils nécessaires pour effectuer d'autres opérations sur des polynômes en une variable sur un anneau $\mathcal{A}(T)$ il devenait possible d'éviter ce travail récursif dans l'algorithme split. Nous présentons en effet dans la section suivante un algorithme qui calcule, pour $p \in \mathbf{P}_{n+1}$ et $T \subset \mathbf{P}_n$, la partie sans facteur carré de $\widehat{p}^T$. Avec un tel algorithme on peut construire des ensembles triangulaires réguliers qui sont radicaux et considérer par conséquent simplement le saturé d'un ensemble triangulaire régulier T au lieu de son radical $\mathsf{Rep}(T)$.

5.2 Partie sans facteur carré

On suppose dans cette section que k est de caractéristique nulle. Nous présentons dans cette section un nouvel algorithme de calcul de partie sans facteur carré modulo un ensemble triangulaire régulier. Kalkbrener n'a pas utilisé ses algorithmes de pgcd et de scindage pour obtenir un tel algorithme alors que cela est simple. Il mentionne l'intérêt de pouvoir effectuer ce type de calcul dans la section 6 de [Kal95]. L'importance d'un tel algorithme apparaît dans [Laz91a] et [Mor97] car on peut alors construire des ensembles triangulaires séparables, c'est-à-dire dont le saturé est radical (proposition 5.2.2). Dans ce qui suit, pour tout polynôme p on note p' sa dérivée par rapport à la variable principale de p.

Proposition 5.2.1 *Soit T un ensemble triangulaire régulier de $\mathbf{P}_n$ et $p \in \mathbf{P}_{n+1}$. On suppose que $\mathsf{mvar}(p) = x_{n+1}$ et $\widehat{p}^T$ est unitaire. Alors l'algorithme $\mathsf{squareFreePart}_n(p, T)$ ci-dessous calcule une famille de couples $\{(p_1, T_1), \ldots, (p_m, T_m)\}$ telle que $\{T_1, \ldots, T_m\}$ est un T-scindage et $p_1, \ldots, p_m$ sont des polynômes de $\mathbf{P}_{n+1}$ vérifiant les propriétés suivantes :*

– $\widehat{p_j}^{T_j}$ *est unitaire dans* $\mathcal{A}(T_j)$,

– $\langle \widehat{p_j}^{T_j}, \widehat{p_j'}^{T_j} \rangle = \langle 1 \rangle$.

• $\mathsf{squareFreePart}_n(p, T) ==$
  si $\mathsf{mdeg}(p) = 1$ alors retourner $\{(p, T)\}$
  $\Phi := \emptyset$
  pour $(g, T) \in \mathsf{gcd}_n(p, p', T)$ faire

si $g \in \mathbf{P}_n$ alors $\Phi := \Phi \cup \{(p, T)\}$ et itérer
$\Phi := \Phi \cup \{(\mathsf{pquo}(p, g), T)\}$
retourner Φ

En utilisant l'algorithme ci-dessus on construit alors des ensembles triangulaires séparables comme l'indique la proposition suivante.

Proposition 5.2.2 *Soit T un ensemble triangulaire régulier séparable de $\mathbf{P}_n$ et $p \in \mathbf{P}_{n+1}$ tel que*

- $\mathsf{mvar}(p) = x_{n+1}$
- $\widehat{p}^T$ *est unitaire*
- $\langle \widehat{p_j}^{T_j}, \widehat{p_j'}^{T_j} \rangle = \langle 1 \rangle$.

Alors $\mathsf{sat}(T \cup \{p\})$ *est un ensemble triangulaire régulier séparable de* $\mathbf{P}_{n+1}$.

Preuve. Cela résulte facilement des propositions 4.5.10 et 3.3.9. □

L'utilisation de cet algorithme dans la construction d'ensembles triangulaires au cours d'une décomposition introduit une étape supplémentaire. Néanmoins, cela permet de supprimer des branches récursives dans les algorithmes monicPolynomial et split comme nous l'avons mentionné dans la remarque 5.1.6 et de simplifier ainsi ces algorithmes. Lorsque la tour T est séparable l'algorithme monicPolynomial présenté dans la section précédente devient

- $\mathsf{monicPolynomial}(p, T) ==$

  si $p \in k$ alors retourner $\{(p, T)\}$
  $\Phi := \emptyset$
  $x_i := \mathsf{mvar}(p)$
  si $x_i \in \mathsf{algVar}(T)$ alors
  pour $(g, U) \in \mathsf{gcd}_{i-1}(p, T_{x_i}, T_{x_i}^-)$ faire
  si $g \in \mathbf{P}_{i-1}$ alors $\Phi := \Phi \cup \{(p, U \cup \{T_{x_i}\})\}$, itérer
  $\Phi := \Phi \cup \{(0, U \cup \{g\})\}$
  si $\mathsf{mdeg}(g) < \mathsf{mdeg}(T_{x_i})$ alors
  $q := \mathsf{pquo}(T_{x_i}, g)$
  $\Phi := \Phi \cup \{(p, U \cup \{q\})\}$
  sinon
  pour $(h, U) \in \mathsf{monicPolynomial}(\mathsf{init}(p), T_{x_i}^-)$ faire
  si $h \neq 0$ alors
  $\Phi := \Phi \cup \{(p, U)\}$
  sinon
  $\Phi := \Phi \cup \mathsf{monicPolynomial}(\mathsf{tail}(p), U)$
  retourner $\{(p, U \cup T_{x_i}^+) \mid (p, U) \in \Phi\}$

5.3 Inversion

Définition 5.3.1 *Soit T un ensemble triangulaire régulier et $p \in \mathbf{P}_n$. On dit que (q, n) est un* inverse *de p modulo T si*

- *n est normalisé par rapport à T,*
- $\widehat{p}^T \widehat{q}^T = \widehat{n}^T$.

On dira que n est le normalisé *de p modulo T, ou le normalisé de p dans $\mathcal{A}(T)$.*

Lorsque $p \in \mathbf{P}_{n+1}$ de variable principale x_{n+1}, et que $\widehat{p}^T$ est unitaire alors il existe un polynôme $q \in \mathbf{P}_n$ et $n \in \mathbf{P}_{n+1}$ de même degré principal que p tels que (q, n) est un inverse de p modulo T. On a alors $\mathsf{sat}(T \cup \{p\}) = \mathsf{sat}(T \cup \{n\})$. On peut, grâce à cet algorithme, effectuer des décompositions de variétés en clôtures d'ensembles triangulaires normalisés.

À partir d'un polynôme p unitaire sur $\mathcal{A}(T)$, l'algorithme $\mathsf{recip}(p, T)$ suivant calcule un inverse de p modulo T. La fonction $\mathsf{halfExtendedResultant}(p, f, U)$ utilisée dans cet algorithme retourne un couple (g, c) tel que g est un pgcd de p et f modulo U, et c est le coefficient de Bezout associé à p. Il existe ainsi un polynôme c' tel que $\widehat{g}^U = \widehat{c}^U \widehat{p}^U + \widehat{c'}^U \widehat{f}^U$. Le couple (g, c) s'obtient de façon classique à partir d'un calcul de pgcd étendu classique.

- $\mathsf{recip}(p, T) ==$

  si p normalisé par rapport à T alors retourner $(1, p)$
  $v := \mathsf{mvar}(p)$
  si $v \in \mathsf{algVar}(T)$ alors
      $(g, c) := \mathsf{halfExtendedResultant}(p, T_v, T_v^-)$
      $(q, n) := \mathsf{recip}(g, T)$
      retourner $(q\,c, n)$
  sinon
      $(q, n) := \mathsf{recip}(\mathsf{init}(p), T)$
      $r := n\ \mathsf{mvar}(p)^{\mathsf{mdeg}(p)} + q\ \mathsf{tail}(p)$
      $r := \mathsf{prem}(p, T)$
      retourner (q, r)

5.4 Algorithme de Kalkbrener

Définition 5.4.1 *Soit F une partie finie de $\mathbf{P}_n$. Un famille $\{T_1, \ldots, T_m\}$ d'ensembles triangulaires réguliers de $\mathbf{P}_n$ est une* décomposition triangulaire de F au sens des saturés *si on a*

$$\sqrt{F} = \bigcup_{j=1}^{m} \sqrt{\mathsf{sat}(T_j)}\ .$$

On dira aussi que c'est une décomposition triangulaire au sens des clôtures *puisque cela équivaut à*

$$\mathbf{V}_F(K) = \bigcup_{j=1}^{m} \overline{\mathbf{W}(T_j)}\ .$$

Puisque les ensembles triangulaires d'une telle décomposition sont réguliers, chaque sortie représente un ensemble de zéros qui n'est pas vide (voir le corollaire 4.3.5). On évite ainsi l'un des écueils de la méthode originale de Wu puisque celle-ci peut fournir des sorties non consistantes (nous avons constaté régulièrement ce phénomène dans les exemples traités dans le chapitre 7).

[Kal95] montre que le fait de pouvoir calculer modulo des ensembles triangulaires réguliers permet d'obtenir l'algorithme $\mathsf{decompose}(F)$ suivant qui calcule, à partir d'un ensemble fini F de polynômes, une décomposition triangulaire de F au sens des saturés.

- $\mathsf{decompose}_n(F) ==$
  - $F := F \setminus \{0\}$
  - si $F = \emptyset$ alors retourner $\{\emptyset\}$
  - si $F \cap k \neq \emptyset$ alors retourner $\emptyset$
  - $\Theta := \emptyset$
  - $F' := F \cap \mathbf{P}_{n-1}$
  - $\Delta := \mathsf{decompose}_{n-1}(F')$
  - pour $U \in \Delta$ répéter
    - $\Gamma := \mathsf{gcd}_n(F \setminus F', U)$
    - pour $(U_j, g_j) \in \Gamma$ répéter
      - si $g_j = 0$ alors $\Theta := \Theta \cup \{U_j\}$ et itérer
      - si $\mathsf{mvar}(g_j) < x_n$ alors $\Theta := \Theta \cup \mathsf{decompose}_n(F \cup \{g_j\})$ et itérer
      - $\Theta := \Theta \cup \{U_j \cup \{g_j\}\} \cup \mathsf{decompose}_n(F \cup \mathsf{init}(g_j))$
  - retourner Θ

La décomposition triangulaire calculée par l'algorithme $\mathsf{decompose}(F)$ permet de répondre immédiatement à la question de l'existence de solutions (dans K) au système F. Notons que la décomposition n'est pas forcément *réduite* dans le sens où on peut avoir $\overline{\mathbf{W}(T_{j_1})} \subseteq \overline{\mathbf{W}(T_{j_2})}$ pour deux indices j_1 et j_2 de $[1, m]$.

5.5 De nouvelles spécifications

Les algorithmes recip et $\mathsf{squareFreePart}$ des sections précédentes permettent d'obtenir des sorties normalisées ou (et) séparables.

Pour obtenir des sorties séparables l'algorithme de décomposition devient

- $\mathsf{decompose}_n(F) ==$
  - $F := F \setminus \{0\}$
  - si $F = \emptyset$ alors retourner $\{\emptyset\}$
  - si $F \cap k \neq \emptyset$ alors retourner $\emptyset$
  - $\Theta := \emptyset$
  - $F' := F \cap \mathbf{P}_{n-1}$
  - $\Delta := \mathsf{decompose}_{n-1}(F')$
    - $\Gamma := \mathsf{gcd}_n(F \setminus F', U)$
    - pour $(U_j, g_j) \in \Gamma$ répéter
      - si $g_j = 0$ alors $\Theta := \Theta \cup \{U_j\}$ et itérer

si $\mathsf{mvar}(g_j) < x_n$ alors $\Theta := \Theta \cup \mathsf{decompose}_n(F \cup \{g_j\})$ et itérer
pour $(g', U') \in \mathsf{squareFreePart}_n(g_j, U_j)$ faire
$\Theta := \Theta \cup \{U' \cup \{g'\}\}$
$\Theta := \Theta \cup \mathsf{decompose}_n(F \cup \mathsf{init}(g_j))$
retourner Θ

Pour obtenir des sorties normalisées il suffit dans l'algorithme ci-dessus de remplacer la partie

pour $(g', U') \in \mathsf{squareFreePart}_n(g_j, U_j)$ faire
$\Theta := \Theta \cup \{U' \cup \{g'\}\}$

simplement par

$(q_j, n_j) := \mathsf{recip}(g_j, U_j)$
$\Theta := \Theta \cup \{U_j \cup \{n_j\}\}$

Les deux possibilités peuvent être combinées pour fournir en sortie des ensembles triangulaires normalisés séparables.

Chapitre 6

Théorie de Galois et ensembles triangulaires

Résumé

Ce chapitre peut être lu de façon indépendante. Son objet principal n'est pas la résolution de systèmes polynomiaux. Nous nous y intéressons à la théorie de Galois et étudions des idéaux, que nous appelons idéaux de Galois, qui apparaissent dans le cadre de cette théorie. C'est un travail réalisé en collaboration avec A. Valibouze et présenté à la conférence internationale MEGA'98 [AV98]. La notion d'idéal de Galois est introduite dans [Val97]. Elle généralise les notions d'idéal des relations et d'idéal des relations symétriques. Pour un polynôme f de $k[X]$ séparable, il est bien connu que l'idéal des relations associé à f est engendré par un ensemble triangulaire de polynômes normalisé séparable puisque c'est un idéal maximal. Il en est de même pour l'idéal des relations symétriques engendré par l'ensemble triangulaire composé des modules de Cauchy de f. Nous donnons ici une généralisation de cette propriété aux idéaux de Galois.

Cette propriété géométrique que nous dégageons semble importante pour le développement de méthodes symboliques en théorie de Galois. Elle peut effectivement être exploitée pour optimiser des algorithmes existants. Nous montrons dans ce chapitre que ce résultat permet de dégager aussi de nouveaux algorithmes.

Un algorithme pour calculer algébriquement les résolvantes relatives est ainsi présenté dans la section 6.7. Il fonctionne pour tout type d'invariant et peut être utilisé dans diverses méthodes de calcul du groupe de Galois d'un polynôme. C'est par exemple un outil de base de la méthode décrite dans [Val97]. Il permet encore de calculer des résolvantes relatives de préférence à des résolvantes absolues dans la méthode des matrices de partition (voir [AV96]). En effet, les résolvantes relatives sont des facteurs sur le corps de base des résolvantes absolues dont le calcul devient inabordable lorsque le degré de f grandit.

Conjointement nous donnons une manière de calculer un ensemble triangulaire qui engendre un idéal de Galois donné. Il est ainsi possible de trouver l'idéal des relations entre les racines de f et de travailler ensuite dans le corps de décomposition de f.

6.1 Introduction

Let k be a perfect field and $\bar{k}$ an algebraic closure of k. Let f be a univariate polynomial of $k[X]$ supposed separable with degree n, and Ω be an ordered set of the n roots of f in $\bar{k}^n$. In [Val97] is introduced the notion of ideal of Ω-relations invariant by a subset L of the symmetric group of degree n. It generalizes the notion of *ideal of relations* and the notion of *ideal of symmetric relations*. We call them *Galois ideals*.

This paper presents two important results. First, we prove in Theorem 6.5.4 that a Galois ideal associated with a group L which contains the Galois group of f is generated by a *separable triangular set* of polynomials which forms a reduced Gröbner basis of this ideal for lexicographical order. We think that the knowledge of such a property may simplify some problems, and thus it may be a basic tool to construct more efficient algorithms in Galois theory. This remark may be taken into account when one is concerned with optimal implementation issues. Moreover, it may lead to new algorithms in Galois theory. The second major result of this paper illustrates this assertion since we give here an algebraic method for computing *relative resolvents* (see Section 6.7). We also specify (see Remark 6.7.11) that when the Galois group of the polynomial f is known, our algorithms may be employed for computing the ideal of relations among the roots of f and consequently for computing in the decomposition field of f.

The *resolvent* is the fundamental tool, introduced by J.L. Lagrange [Lag70], in the constructive Galois theory. Later, R.P. Stauduhar [Sta73] has extended the definition of J.L. Lagrange. Let us recall that the resolvents relative to the symmetric group $\mathfrak{S}_n$, called *absolute resolvents*, can be computed with many algorithms (see [Lag70], [MS85], [Soi81] and [Val89]). However, for computing resolvents relative to some proper subgroup L of $\mathfrak{S}_n$, there exists only a numerical method (see [Eic96] or [Sta73]) and a linear method which requires hard generic computation (see [Arn76] and [Col95]); the reader can see also [Yok96] for computing linear factors of resolvents. The numerical method is generally efficient but is not adapted for the problems which require high precision; and it may be used only in a particular algorithm for computing Galois groups. On the contrary our algebraic method is general. Furthermore, it works with any kind of invariant.

The interest of the computation of relative resolvents follows from complexity considerations. Indeed, the degree of the resolvents increases with the order of the group L; since these resolvents have to be factorized for extracting informations on the Galois group of f, absolute resolvents may be harder to handle than relative resolvents. For example, by the method of partition matrices (see [AV96]) it is possible to compute the Galois group of a polynomial with resolvents relative to a group which contains this Galois group. The symmetric group always satisfies this requirement but, as explained above, it is preferable to use resolvents relative to smaller groups. Moreover, these relative resolvents may avoid some degenerated cases with non-separable absolute resolvents.

Our algorithm requires only the triangular Gröbner basis of the Galois ideal associated with the group L. Due to the particular structure of some considered Galois ideals I, our method is in fact easily obtained from a natural algorithm for computing characteristic polynomial of the multiplication by a polynomial inside the finite quotient algebra $k[x_1, \ldots, x_n]/I$ (see Section 6.6).

The complexity of our method depends essentially on the complexity of lexicographical Gröbner bases. The average arithmetic cost for the computation of Gröbner bases in the zero dimensional case is $d^{O(n)}$, where n is the number of variables and d is the maximum degree of input polynomials (see [Laz91b]). Practically, some efficient implementations are available for the computations of Gröbner bases (see [Fau97]). Note that this part of the computation in our method decreases when the polynomial f is reducible over k. In this case the computation splits into several computations of Gröbner bases with less variables. This point will be developed in a future paper.

The chapter is structured as follows. Section 6.2 introduces our terminology and notations. The third section contains some lemmas of commutative algebra; further proofs will refer to them. In Section 6.4, we introduce the concept of *equiprojectable* variety and we show that it gives a geometrical characterization of the ideals of $k[x_1, \ldots, x_n]$ generated by a separable triangular set. In Section 6.5, this characterization is exploited to prove the main property for Galois ideals that we mentioned above. Section 6.6 presents the algorithm for computing the characteristic polynomial of the multiplication by a polynomial inside $k[x_1, \ldots, x_n]/I$ in the particular case where the ideal I admits a separable triangular set of generators. The former results are exploited in Section 6.7 to give a method for computing relative resolvents in Galois theory. An explicit way of computing a triangular set of polynomials which generates a Galois ideal is simultaneously presented. Finally an explicit example illustrates our method.

6.2 Definitions, notations

Throughout the chapter, k is a perfect field and $\bar{k}$ is an algebraic closure of k. Let f be a univariate polynomial of $k[X]$ supposed separable, with degree n. Let $\Omega = (\alpha_1, \ldots, \alpha_n)$ be a tuple of the n roots of the polynomial f in $\bar{k}^n$ with some fixed order. Let $x_1 < \ldots < x_n$ be n ordered variables which are algebraically independent over k. For $P \in k[x_1, \ldots, x_n]$, the evaluation of P in Ω is denoted by $P(\Omega)$. We denote by $\mathfrak{S}_n$ the symmetric group of degree n. For $\sigma \in \mathfrak{S}_n$ the action of σ on Ω, denoted by $\sigma.\Omega$ is defined by $\sigma.\Omega = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

The following definition has been introduced in [Val97] and generalizes the well-known notions of *ideal of relations* and *ideal of symmetric relations*.

Definition 6.2.1 *Let L be a subset of the symmetric group $\mathfrak{S}_n$. The* Galois (L,Ω)-ideal *is the ideal I_Ω^L of $k[x_1, \ldots, x_n]$ formed by the Ω-relations invariant by L:*

$$I_\Omega^L = \{R \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in L)\ (\sigma.R)(\Omega) = 0\}\ ,$$

where $(\sigma.R)(x_1, \ldots, x_n) = R(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Since the tuple Ω is fixed throughout the chapter, the ideal I_Ω^L will also be called the Galois ideal associated with L.

Definition 6.2.2 *The ideal $I_\Omega^{\mathfrak{S}_n}$ is called the* ideal of symmetric relations *of f. The ideal $I_\Omega^{\{Id\}}$ is called the* ideal of relations *of f and is simply denoted by I_Ω.*

Let us recall the definition of the Galois group.

Definition 6.2.3 *The* Galois group of Ω *over* k*, denoted by* G_Ω*, is the subgroup of* $\mathfrak{S}_n$ *defined by*

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid (\forall P \in I_\Omega)\ \sigma.P(\Omega) = 0\}\ .$$

Usually G_Ω *is also called the Galois group of* f *over* k*.*

Remark 6.2.4 From the definition of the Galois group, it follows directly that $I_\Omega^{G_\Omega} = I_\Omega$.

For $i \in [1, n]$ and $E \subset k[x_1, \ldots, x_i]$ we denote by $Z_{\bar{k}^i}(E)$ the set of zeros of E in $\bar{k}^i$, and by $V(E)$ the k-variety $Z_{\bar{k}^n}(E)$.

For a k-variety V in $\bar{k}^n$ we denote $\mathcal{J}(V)$ the radical ideal of $k[x_1, \ldots, x_n]$ composed by the polynomials of $k[x_1, \ldots, x_n]$ which cancel on V.

Notation 6.2.5 *Let* i *and* j *be two integers such that* $1 \leq i \leq j \leq n$*. Let* V *be a subset of* $\bar{k}^j$*. We denote by* $\pi_{j,i}$ *the natural projection map from* $\bar{k}^j$ *to* $\bar{k}^i$*, which sends* $(a_1, \ldots, a_j)$ *to* $(a_1, \ldots, a_i)$*. Moreover, we set* $V_i = \pi_{j,i}(V)$*.*

In this chapter we only need to deal with zero-dimensional ideals; For simplicity we will say *triangular set* for a normalized triangular set of $k[x_1, \ldots, x_n]$. Thus, in this chapter, a triangular set of $k[x_1, \ldots, x_n]$ is a triangular set such that each initial lies in the field k. For a triangular set T in $k[x_1, \ldots, x_n]$, we will always use the notation $T = \{f_1, \ldots, f_n\}$, where f_i is the unique polynomial of T with x_i as greatest variable. It is clear that the ideal generated by a triangular set is zero-dimensional. The notion of *separable triangular set* that we use in this chapter is defined as follows:

Definition 6.2.6 *We say that a triangular set* $T = \{f_1, \ldots, f_n\}$ *of* $k[x_1, \ldots, x_n]$ *is a* separable triangular set *if each polynomial* f_i *satisfies the following condition:*

$\forall \beta = (\beta_1, \ldots, \beta_{i-1}) \in V_{i-1}$*, the univariate polynomial* $f_i(\beta_1, \ldots, \beta_{i-1}, x_i)$ *is separable, i.e. it has no multiple root in* $\bar{k}[x_i]$*.*

We say that an ideal of $k[x_1, \ldots, x_n]$ *is a* triangular ideal *if it admits a separable triangular set of generators.*

Remark 6.2.7 If T is a triangular set, it is a triangular reduced Gröbner basis of the ideal $\langle T \rangle$. for lexicographical ordering (see proposition 4 p.103 in [CLO92])

Remark 6.2.8 Generally a zero-dimensional k-variety V cannot be expressed as zeros of a single separable triangular set, as shown in [Laz92] with the following simple example:

$$V \ = \ V(x_1, x_2)\ \cup\ V(x_1, x_2 + 1)\ \cup\ V(x_1 + 1, x_2)\ .$$

However, it can always be decomposed into a finite family of varieties defined by separable triangular sets (see [AM99] and [Laz92]).

6.3 Commutative algebra preliminaries

In this section we give some basic properties that we will use in the proofs of the next section. For a subset E of a ring S, we write $\langle S\rangle_E$ or ES for the ideal generated in S by E.

Lemma 6.3.1 *Let $\phi : R \to S$ be a surjective homomorphism of commutative rings. Let I be an ideal in R such that $Ker(\phi) \subseteq I$. We denote by J the ideal $\phi(I)$. Then I is the contraction of J to R under ϕ, that is:*

$$\phi^{-1}(J) = \{r \in R \mid \phi(r) \in J\} = I \ .$$

Proof. Note that J is an ideal of S since the homomorphism ϕ is surjective. Let $r \in \phi^{-1}(J)$. Then there exists an element p in I such that $\phi(r) = \phi(p)$. It follows easily from the hypothesis that $r \in I$. Therefore $\phi^{-1}(J) \subseteq I$. The inverse inclusion is obvious. $\square$

Corollary 6.3.2 *With the hypothesis of Lemma 6.3.1, I is a radical ideal of R iff $\phi(I)$ is a radical ideal of S.*

Proof. We set $J = \phi(I)$. By Lemma 6.3.1 we have $I = \phi^{-1}(J)$. It is known that $\phi^{-1}(\sqrt{J}) = \sqrt{\phi^{-1}(J)}$ (see [SZ67], p. 218). Hence if J is radical then I is clearly radical. Conversely, assume that I is radical. Since $\phi^{-1}(\sqrt{J}) = \sqrt{I} = I$, an application of the homomorphism ϕ gives $\sqrt{J} = \phi(I) = J$. $\square$

Proposition 6.3.3 *Let $\mathcal{M}$ be a maximal ideal of a commutative ring R and I a proper ideal of $R[x]$ such that $\mathcal{M} \subseteq I$. If $I \neq \mathcal{M}R[x]$ then there exists a monic polynomial $g \in R[x] \setminus R$ such that $I = \langle \mathcal{M} \cup \{g\}\rangle_{R[x]}$.*

Proof. The natural homomorphism from R to $R/\mathcal{M}$ induces a surjective homomorphism $\phi : \ R[x] \longrightarrow (R/\mathcal{M})[x]$ defined by $\phi(\sum c_k \ x^k) = \sum \overline{c_k}^{\mathcal{M}} \ x^k$.

By assumption the ideal $J = \phi(I)$ is not the zero ideal of the principal ideal domain $(R/\mathcal{M})[x]$. Therefore J is generated by a monic univariate polynomial of $(R/\mathcal{M})[x]$. Thus, there exists $g \in R[x]$ – which can be chosen with a monic leading coefficient in x – such that J is generated by $\phi(g)$. It is clear that $\phi^{-1}(J) = \langle \mathcal{M} \cup \{g\}\rangle_{R[x]}$. Hence it follows from Lemma 6.3.1 that $I = \langle \mathcal{M} \cup \{g\}\rangle_{R[x]}$. $\square$

Proposition 6.3.4 *Let k be a perfect field. Let $\mathcal{M}$ be a maximal ideal of $k[x_1, \ldots, x_{n-1}]$ and $g \in k[x_1, \ldots, x_n]$ such that* degree$(g, x_n) > 0$ *and g is monic w.r.t. the variable x_n. Then the following are equivalent:*

(i) the ideal $\langle \mathcal{M} \cup \{g\}\rangle$ is radical;

(ii) $\forall \beta = (\beta_1, \ldots, \beta_{n-1}) \in V(\mathcal{M})$, $g(\beta_1, \ldots, \beta_{n-1}, x_n)$ is a separable polynomial.

Proof. Let $\beta \in V(\mathcal{M})$. From the isomorphism between the field $K = k(\beta_1, \ldots, \beta_{n-1})$ and $k[x_1, \ldots, x_{n-1}]/\mathcal{M}$ we deduce the following surjective homomorphism:

$$\begin{array}{rcl} \phi: \ k[x_1, \ldots, x_n] & \longrightarrow & K[x_n] \\ p = \sum c_k(x_1, \ldots, x_{n-1})\ x_n^k & \longmapsto & \sum c_k(\beta_1, \ldots, \beta_{n-1})\ x_n^k \end{array}$$

The ideal $\phi(\langle \mathcal{M} \cup \{g\} \rangle)$ is generated in $K[x_n]$ by the image of g. Since the field k is perfect the algebraic extension K is also perfect. Thus $\langle g(\beta_1, \ldots, \beta_{n-1}, x_n) \rangle_{K[x_n]}$ is radical if and only if the univariate polynomial $g(\beta_1, \ldots, \beta_{n-1}, x_n)$ is separable. Then the assertion follows from Corollary 6.3.2. □

The following variant of Chinese remainder Theorem appears implicitly in [Laz92]. Its proof is easily deduced from the proof of the standard version of the Chinese remainder Theorem.

Lemma 6.3.5 *Let $I_1, \ldots, I_m$ be pairwise comaximal ideals in a commutative ring R and $I = \cap_{j=1}^m I_j$. Let $p_1, \ldots, p_m$ be monic polynomials of the same positive degree d in $R[X]$. Then there exists a monic polynomial $p \in R[X]$ of degree d such that*

$$(\forall j \in [1, m]) \quad p \equiv p_j \pmod{I_j R[X]}\ . \tag{6.1}$$

Moreover, we have

$$\langle I \cup \{p\} \rangle_{R[X]} \ = \ \cap_{j=1}^m \langle I_j \cup \{p_j\} \rangle_{R[X]}\ . \tag{6.2}$$

Finally let us recall some properties on zero-dimensional varieties and triangular sets.

Proposition 6.3.6 *Let V be a zero-dimensional k-variety in $\bar{k}^n$ and $I = \mathcal{J}(V)$. Then the following hold:*

(i) The ideal I contains a non-constant univariate polynomial in each of the variables in $\{x_1, \ldots, x_n\}$, and the elimination ideal $I \cap k[x_1, \ldots, x_{n-1}]$ is a zero-dimensional ideal of $k[x_1, \ldots, x_{n-1}]$;

(ii) For each i in $[1, n]$, the projection V_i is a zero-dimensional k-variety in $\bar{k}^i$ and $V_i = Z_{\bar{k}^i}(I \cap k[x_1, \ldots, x_i])$;

(iii) The ideal of V_i in $k[x_1, \ldots, x_i]$ equals $I \cap k[x_1, \ldots, x_i]$;

(iv) If G is a Gröbner basis of I then the ideal $I \cap k[x_1, \ldots, x_i]$ is generated by $G \cap k[x_1, \ldots, x_i]$.

Proof. See Lemma 6.50 in [BW93] for the first point. We obtain assertion 2 by induction from the first point and Corollary 4 in p.124 of [CLO92]. The third assertion obviously follows from the relation $V_i = Z_{\bar{k}^i}(I \cap k[x_1, \ldots, x_i])$ and the fact that I is radical. The last property is classic in Gröbner bases theory. □

Remark 6.3.7 For an integer i in $[1, n]$ and a triangular set $T = \{f_1, \ldots, f_n\}$ it follows clearly from the above proposition that $\pi_{n,i}(V(T)) = Z_{\bar{k}^i}(f_1(x_1), \ldots, f_i(x_1, \ldots, x_i))$.

Proposition 6.3.8 *Let $n > 0$ and T be a separable triangular set of $k[x_1, \ldots, x_n]$. Then $\langle T \rangle$ is radical.*

Proof. It is obvious for $n = 1$. By induction, we assume that the ideal generated by $\{f_1, \ldots, f_{n-1}\}$ in $k[x_1, \ldots, x_{n-1}]$ is the intersection of maximal ideals. The result is then obtained for n by applying Lemma 6.3.5 (with f_n for each p_j) and Proposition 6.3.4. $\square$

6.4 A characterization of zero-dimensional triangular ideals

This section introduces the concept of *equiprojectable* variety. This concept characterizes the zero-dimensional k-varieties which can be expressed as $V(T)$ where T is a separable triangular set. It follows that the ideal of the equiprojectable k-variety is the ideal generated by T. Our geometrical characterization of triangular ideals provides a tool to prove the triangular structure of Galois ideals in Section 6.5.

Definition 6.4.1 *Let $1 \leq i \leq j \leq n$ and V be a finite subset of $\bar{k}^j$. The set V is said* equiprojectable *on V_i, its projection on $\bar{k}^i$, if there exists an integer c such that for each point M in V_i, we have*

$$\mathrm{card}(\pi_{j,i}^{-1}(M)) = c .$$

The positive integer c will be denoted by $c_i(V)$.

Definition 6.4.2 *With the notations of Definition 6.4.1, we say that V is* equiprojectable *if V is equiprojectable on V_i for each $i \in [1, j]$.*

An equiprojectable subset of $\bar{k}^n$ may be characterized by induction. This equivalence will be useful for further proofs.

Proposition 6.4.3 *Let V be a finite subset of $\bar{k}^n$. Then V is equiprojectable iff V_{i+1} is equiprojectable on V_i for each $i \in [1, n-1]$.*

Proof. Let $1 \leq i < j \leq n$ and M be a point of V_i. Clearly we have the following disjoint union:

$$\pi_{n,i}^{-1}(M) = \cup_{M' \in \pi_{j,i}^{-1}(M)} \pi_{n,j}^{-1}(M') , \tag{6.3}$$

Let us assume that V is equiprojectable on V_i for each $i \in [1, n]$. Let $i \in [1, n-1]$. For some point M in V_i, it follows from relation (6.3) above, that

$$c_i(V) = \mathrm{card}(\pi_{i+1,i}^{-1}(M)) \ c_{i+1}(V) . \tag{6.4}$$

Therefore $\mathrm{card}(\pi_{i+1,i}^{-1}(M))$ does not depend on the choice of the point M of V_i.

Conversely, assume that V_{i+1} is equiprojectable on V_i for each $i \in [1, n-1]$. If $i \in [1, n-1]$ and M is a point of V_i, then an easy induction shows that

$$\mathrm{card}(\pi_{n,i}^{-1}(M)) = \prod_{i \leq j < n} c_j(V_{j+1}) \ . \tag{6.5}$$

It follows that V is equiprojectable on V_i. □

Before giving the main theorem of this section, we study in the following proposition the case where V is a k-variety such that V_{n-1} is irreducible. We will refer to this particular case in Theorem 6.4.5 by splitting V_{n-1} into irreducible components and recombining results with Chinese remainders.

Proposition 6.4.4 *Let $n > 1$ and V be a zero-dimensional k-variety in $\bar{k}^n$ such that V_{n-1} is irreducible over k. Let us denote by $I = \mathcal{J}(V)$ the ideal of V, and $\mathcal{M}$ the ideal of V_{n-1} in $k[x_1, \ldots, x_{n-1}]$. Then V is equiprojectable on V_{n-1} and there exists a polynomial g in $k[x_1, \ldots, x_n]$ of degree d in x_n such that*

(i) $c_{n-1}(V) = d$;

(ii) $I = \langle \mathcal{M} \cup \{g\} \rangle$;

(iii) the polynomial g is monic in x_n;

(iv) $g(\beta_1, \ldots, \beta_{n-1}, x_n)$ is a separable polynomial for each $(\beta_1, \ldots, \beta_{n-1})$ in V_{n-1}.

Proof. By Proposition 6.3.3 there exists g in $k[x_1, \ldots, x_n]$ for which properties (ii) and (iii) hold. Since the ideal I is radical, property (iv) follows from Proposition 6.3.4.

Now we prove relation (i) and consequently that V is equiprojectable on V_{n-1}. Let $M = (\beta_1, \ldots, \beta_{n-1})$ be a point of V_{n-1} and $P = (\beta_1, \ldots, \beta_{n-1}, \beta_n)$ with $\beta_n \in \bar{k}$. We have:

$$\begin{aligned} P \in \pi_{n,n-1}^{-1}(M) \quad &\Longleftrightarrow \quad (\forall f \in \langle \mathcal{M} \cup \{g\} \rangle) \quad f(\beta_1, \ldots, \beta_n) = 0 \\ &\Longleftrightarrow \quad g(\beta_1, \ldots, \beta_n) = 0 \ . \end{aligned}$$

Thus $P \in \pi_{n,n-1}^{-1}(M)$ iff β_n is a root of $g(\beta_1, \ldots, \beta_{n-1}, x_n)$. Since this latter polynomial is separable we have $\mathrm{card}(\pi_{n,n-1}^{-1}(M)) = \mathrm{degree}(g, x_n) = d$. Relation (i) clearly follows. □

Theorem 6.4.5 *Let V be a zero-dimensional k-variety in $\bar{k}^n$. Then the following statements are equivalent:*

(1) there exists a separable triangular set $T = \{f_1, \ldots, f_n\}$ such that $\mathcal{J}(V) = \langle T \rangle$;

(2) V is equiprojectable.

Furthermore we have $c_i(V_{i+1}) = \mathrm{degree}(f_{i+1}, x_{i+1})$ and $c_i(V) = \prod_{j=i+1}^{n} \mathrm{degree}(f_j, x_j)$.

Proof. First, we assume (1). Let $T = \{f_1, \ldots, f_n\}$ and $d_j = \text{degree}(f_j, x_j)$. Let $i \in [1, n-1]$ and $M = (\beta_1, \ldots, \beta_i)$ a point of V_i. By hypothesis the polynomial $f_{i+1}(\beta_1, \ldots, \beta_i, x_{i+1})$ has exactly d_{i+1} distinct roots. Since $V_{i+1} = Z_{\bar{k}^{i+1}}(f_1, \ldots, f_{i+1})$ by Remark 6.3.7, it is clear that the cardinal of $\pi_{i+1,i}^{-1}(M)$ equals d_{i+1}. Therefore V_{i+1} is equiprojectable on V_i and V is equiprojectable (Proposition 6.4.3).

Remark that we also have shown that $\text{degree}(f_{i+1}, x_{i+1}) = c_i(V_{i+1})$. Moreover the equality concerning $c_i(V)$ in the theorem is obtained by relation (6.5) above. Hence the last part of the theorem is proved.

Reciprocally, let V be an equiprojectable k-variety. We show by induction on n that $\mathcal{J}(V)$ is a triangular ideal.

For $n = 1$, the result follows from the fact that k is perfect. Let $n > 1$ and let $V_{n-1} = W_1 \cup \ldots \cup W_r$ be the decomposition of the k-variety V_{n-1} into irreducible components. If we denote $\pi_{n,n-1}^{-1}(W_j) = \cup_{M \in W_j} \pi_{n,n-1}^{-1}(M)$, then we have

$$V = \pi_{n,n-1}^{-1}(W_1) \cup \ldots \cup \pi_{n,n-1}^{-1}(W_r) \ . \tag{6.6}$$

Let us denote by $\mathcal{M}_j$ the ideal of W_j in $k[x_1, \ldots, x_{n-1}]$; The ideal $\mathcal{M}_j$ is maximal. If I' is the ideal of V_{n-1} in $k[x_1, \ldots, x_{n-1}]$, then

$$I' = \mathcal{M}_1 \cap \ldots \cap \mathcal{M}_r \ .$$

Each $\pi_{n,n-1}^{-1}(W_j)$ is a k-variety (since it is the inverse image by an homomorphism of a closed set of $\bar{k}^n$ in the Zariski topology) which satisfies the hypothesis of Proposition 6.4.4. Hence there exist r polynomials $g_1, \ldots, g_r$ of $k[x_1, \ldots, x_n]$ such that for each $j \in [1, r]$

(*i*) $\text{degree}(g_j, x_n) = \text{card}(\pi_{n,n-1}^{-1}(M))$ where M is a point of W_j;

(*ii*) $\mathcal{J}(\pi_{n,n-1}^{-1}(W_j)) = \langle \mathcal{M}_j \cup \{g_j\} \rangle$;

(*iii*) g_j is monic as univariate in x_n;

(*iv*) $g_j(\beta_1, \ldots, \beta_{n-1}, x_n)$ is a separable polynomial for each $(\beta_1, \ldots, \beta_{n-1})$ in W_j.

Besides, the k-variety V_{n-1} in $\bar{k}^{n-1}$ is clearly equiprojectable. According to the induction hypothesis, its ideal I' is therefore generated by a separable triangular set T'. Now, the equiprojectability of V on V_{n-1} will allow us to combine results (*i*) to (*iv*) in order to exhibit a convenient polynomial g with greatest variable x_n to *extend* T' into a triangular set of $k[x_1, \ldots, x_n]$. We set $d = c_{n-1}(V)$. By assertion (*i*), each g_j has degree d relatively to x_n. By Lemma 6.3.5, there exists a polynomial $g \in k[x_1, \ldots, x_n]$, monic w.r.t. the variable x_n with $\text{degree}(g, x_n) = d$, such that

$$(\forall j \in [1, r]) \quad g \equiv g_j \pmod{\langle \mathcal{M}_j \rangle} \ , \tag{6.7}$$

and

$$\langle I' \cup \{g\} \rangle = \cap_{j=1}^{m} \langle \mathcal{M}_j \cup \{g_j\} \rangle \ .$$

It follows from identity (*ii*) and relation (6.6) that

$$\mathcal{J}(V) = \langle T' \cup \{g\} \rangle \ .$$

Finally it suffices to check that the triangular set $T = T' \cup \{g\}$ is separable. This is easily done with relation (6.7) and assertion (*iv*). □

6.5 Galois ideals: a fundamental property

This section states a main result. It is shown that if a group of permutations L contains the Galois group of Ω (see Definition 6.2.3) then the Galois ideal I_Ω^L (see Definition 6.2.1) is triangular. This remark may simplify some problems in Galois theory and provides an essential information for some implementation issues. The triangular structure of Galois ideals will be exploited in section 6.7 to give a new algebraic algorithm for computing relative resolvents.

Notation 6.5.1 *Let L be a subgroup of $\mathfrak{S}_n$. For each $i \in [1, n]$ we denote by $L_{(i)}$ the stabilizer of $\{1, \ldots, i\}$ under the natural action of L:*

$$L_{(i)} = \{\tau \in L \mid \forall k \in [1, i],\ \tau(k) = k\}\ .$$

We set $L_{(0)} = L$. Thus we obtain this chain of subgroups of L:

$$\{Id\} = L_{(n)} < L_{(n-1)} \ldots < L_{(1)} < L_{(0)} = L\ .$$

Now let us study the left classes of L modulo $L_{(i)}$, that is, the classes of the equivalence relation $\sim_i$, defined by $\tau \sim_i \tau'$ if and only if $\tau^{-1}\tau' \in L_{(i)}$. We can characterize these classes as follows:

Lemma 6.5.2 *Let L be a subgroup of $\mathfrak{S}_n$ and $(\tau, \tau') \in L^2$. Then*

$$\tau \sim_i \tau' \iff \forall k \in [1, i],\ \tau(k) = \tau'(k)$$

and each equivalence class in $L/\sim_i$ has cardinality $\mathrm{card}(L_{(i)})$.

Proof. We easily have the following equivalences:

$$\begin{aligned} \tau \sim_i \tau' &\iff \tau^{-1}\tau' \in L_{(i)} \\ &\iff (\forall k \in [1, i]) \quad \tau^{-1}\tau'(k) = k \\ &\iff (\forall k \in [1, i]) \quad \tau'(k) = \tau(k). \end{aligned}$$

The second part of this lemma is a basic result on the left classes of a group L modulo a subgroup of L. □

Lemma 6.5.2 applies to a particular family of subsets of $\bar{k}^n$ defined from subgroups of $\mathfrak{S}_n$ as follows:

Proposition 6.5.3 *Let f be a separable polynomial of $k[X]$ and $\Omega = (\alpha_1, \ldots, \alpha_n)$ be the n roots of f in $\bar{k}^n$ with some fixed order. If L is a subgroup of $\mathfrak{S}_n$ then the subset V of $\bar{k}^n$ defined by*

$$V = \{\sigma.\Omega \mid \sigma \in L\}$$

is equiprojectable.

Proof. Let $i \in [1, n]$ and $M \in V_i$. It is sufficient to show that the cardinality of $\pi_{n,i}^{-1}(M)$ is independent from the choice of the point M.

It follows from the definition of V that there exists a permutation τ in L such that $M = (\alpha_{\tau(1)}, \ldots, \alpha_{\tau(i)})$. Then the inverse image of M by $\pi_{n,i}$ may be defined by

$$\pi_{n,i}^{-1}(M) = \{\sigma.\Omega \mid \sigma \in L \text{ and } (\forall k \in [1, i]) \;\; \sigma(k) = \tau(k)\}$$

Since the points of V are all distinct we have

$$\operatorname{card}(\pi_{n,i}^{-1}(M)) = \operatorname{card}(\{\sigma \in L \mid \sigma \sim_i \tau\}) = \operatorname{card}(L_{(i)}) \; . \tag{6.8}$$

Thus the assertion is proved. □

In general, the set V defined in Proposition 6.5.3 is not a variety over k. However it is a k-variety when L contains the Galois group of f. In this case, Galois ideals have the following basic property:

Theorem 6.5.4 *Let Ω be an ordered set of roots of a univariate polynomial f supposed separable and G_Ω be the Galois group of f. Let L be a subgroup of $\mathfrak{S}_n$ which contains G_Ω. Then there exists a separable triangular set $T = \{f_1, \ldots, f_n\}$ such that*

$$I_\Omega^L = \langle T \rangle \; .$$

Moreover, the degree of each f_i in x_i is given by

$$\operatorname{degree}(f_i, x_i) = \operatorname{card}(L_{(i-1)})/\operatorname{card}(L_{(i)}) \; .$$

Proof. If L contains the Galois group of Ω, it is known that $V(I_\Omega^L) = \{\sigma.\Omega \mid \sigma \in L\}$ (see [Val97]). Besides it is easy to verify that I_Ω^L is radical; thus $I_\Omega^L = \mathcal{J}(V(I_\Omega^L))$. Then the result follows immediately from Proposition 6.5.3 and Theorem 6.4.5. The degree of f_i with respect to x_i is easily obtained from relations (6.8) and (6.4). □

The above result specifies the structure of Galois ideals. Therefore it may be exploited to develop and optimize algorithms in Galois theory. The knowledge of the degrees of the polynomials in T may also be useful to improve the efficiency of some techniques.

Remark 6.5.5 The above result is well known when L is the group $\mathfrak{S}_n$. Let us recall that $I_\Omega^{\mathfrak{S}_n}$ is generated by the separable triangular set $\{f_1, \ldots, f_n\}$ of *Cauchy moduli* of f, defined by induction as follows:

$$\begin{aligned} f_1(x_1) &= f(x_1) \\ f_i(x_1, \ldots, x_i) &= \frac{f_{i-1}(x_1, \ldots, x_{i-2}, x_i) - f_{i-1}(x_1, \ldots, x_{i-2}, x_{i-1})}{x_i - x_{i-1}} \; . \end{aligned}$$

6.6 An algorithm for computing some characteristic polynomials

In this section I is a radical zero dimensional ideal of $k[x_1,\dots,x_n]$ and Θ is a polynomial of $k[x_1,\dots,x_n]$. The finite quotient algebra $k[x_1,\dots,x_n]/I$ is denoted by A_I and the class of Θ in A_I is denoted by $\overline{\Theta}$. When I is a triangular ideal a natural algorithm works for computing the characteristic polynomial of the multiplication by $\overline{\Theta}$ in A_I. This algorithm is presented in this section and will be exploited with Galois ideals for computing relative resolvents (see Section 6.7).

Let us denote by $\hat{\Theta}$ the following endomorphism of the quotient ring A_I:

$$\begin{array}{rccc}\hat{\Theta}: & A_I & \longrightarrow & A_I\\ & P & \mapsto & \overline{\Theta}.P\end{array}$$

and by $C_{\Theta,I}$ the characteristic polynomial of $\hat{\Theta}$. The coefficients of $C_{\Theta,I}$ lie in the field k like those of the matrix of the endomorphism $\hat{\Theta}$. Since I is a radical ideal, the classical theorem of Stickelberger says that:

$$C_{\Theta,I}(X) = \prod_{\beta\in V(I)} (X-\Theta(\beta)) \ . \tag{6.9}$$

Let K be an extension of the field k such that $K\cap k[x_1,\dots,x_n]=k$. For two polynomials p and q in $K[x_1,\dots,x_n]$ and for $i\in[1,n]$, we denote by $\mathrm{Res}_{x_i}(p,q)$ the resultant of the polynomials p and q relatively to the variable x_i.

The following lemma presents an algorithm which eliminates the variables $x_1,\dots,x_n$ from a polynomial Ψ in $K[x_1,\dots,x_n]$ and a separable triangular set of $k[x_1,\dots,x_n]$. It will be exploited in Theorem 6.6.2 for computing the characteristic polynomial $C_{\Theta,I}$ when I is a triangular ideal.

Lemma 6.6.1 *Let $T=\{f_1,\dots,f_n\}$ be a separable triangular set of $k[x_1,\dots,x_n]$. Let $\Psi\in K[x_1,\dots,x_n]$. We define inductively the $n+1$ polynomials $\Psi_0,\Psi_1,\dots,\Psi_n$ relatively to T as follows:*

$$\begin{array}{rcl}\Psi_n & := & \Psi\in K[x_1,\dots,x_n]\\ \Psi_{i-1} & := & \mathrm{Res}_{x_i}(f_i(x_1,\dots,x_i),\Psi_i(x_1,\dots,x_i))\in K[x_1,\dots,x_{i-1}]\ ,\end{array}$$

Then the element Ψ_0 of K is given by:

$$\Psi_0=\prod_{\beta\in V(T)}\Psi(\beta)\ .$$

Proof. At the beginning, $\Psi_0 = \mathrm{Res}_{x_1}(f_1(x_1),\Psi_1(x_1))=\prod_{\beta_1\in V_1}\Psi_1(\beta_1)$. Let us denote by V the variety $V(T)$. By induction, we prove that for each $j\in[1,n]$

$$\Psi_0=\prod_{\{\beta_1,\dots,\beta_j\}\in V_j}\Psi_j(\beta_1,\dots,\beta_j)\ .$$

Supposing that our assertion is valid for $j = i - 1$, we have

$$\Psi_0 = \prod_{\{\beta_1,\ldots,\beta_{i-1}\}\in V_{i-1}} \Psi_{i-1}(\beta_1,\ldots,\beta_{i-1}) \ . \tag{6.10}$$

By definition of Ψ_{i-1}, the identity (6.10) becomes

$$\Psi_0 = \prod_{\{\beta_1,\ldots,\beta_{i-1}\}\in V_{i-1}} \mathrm{Res}_{x_i}(f_i(\beta_1,\ldots,\beta_{i-1},x_i), \Psi_i(\beta_1,\ldots,\beta_{i-1},x_i)) \ .$$

Then the result follows from Remark 6.3.7 and the fact that, by assumption, the univariate polynomial $f_i(\beta_1,\ldots,\beta_{i-1},x_i)$ is monic and separable in $\bar{k}[x_i]$. □

Theorem 6.6.2 *Let I be a triangular ideal of $k[x_1,\ldots,x_n]$ generated by a separable triangular set T. Let Θ be a polynomial in $k[x_1,\ldots,x_n]$. Then the characteristic polynomial $C_{\Theta,I}(X)$ of $k[X]$ is computable by the algorithm* $\mathsf{CharPol}(T,\Theta)$ *below.*

```
CharPol(T, Θ) ==
    Ψ := X − Θ
    for i from n to 1 repeat
        f := the only polynomial in T with greatest variable x_i
        Ψ := Res_{x_i}(f, Ψ)
    output(Ψ)
```

Proof. It suffices to apply Lemma 6.6.1 with the set T and the polynomial $\Psi = (X - \Theta)$ of $k[X][x_1,\ldots,x_n]$. By Proposition 6.3.8 the ideal I is radical. Hence relation (6.9) applies and we obtain

$$C_{\Theta,I}(X) \quad = \quad \prod_{\beta\in V(T)} (X - \Theta(\beta)) = \Psi_0 \ .$$

□

6.7 Algebraic computation of relative resolvents

Let L be a subgroup of $\mathfrak{S}_n$ which contains the Galois group of Ω (see 6.2.3). In this section we define the L-relative resolvent by a polynomial Θ, and specify the obvious connection with the characteristic polynomial C_{Θ,I_Ω^L}. We deduce an algorithm for computing relative resolvents from the algorithm of Section 6.6.

The idea appears in [RV99] for the algebraic computation of absolute resolvents. Indeed it is based on the triangular structure of the Cauchy moduli. We show here that a similar method is convenient for computing relative resolvents, and that the efficient improvements presented in [Leh97] and [RV99] for absolute resolvents are also available for our algorithm. The crucial point is that the ideal I_Ω^L is triangular.

Our algorithm depends on the computation of triangular sets of generators of Galois ideals. But we show that reciprocally, it is possible to obtain these triangular sets by using our algorithm (see Theorem 6.7.10 and Remark 6.7.11). Thus, we present also in this section an algorithm for computing the generators of Galois ideals which is based on a recent result presented in [Val97] (see Lemma 6.7.7).

6.7.1 Resolvent and characteristic polynomial

From now on we denote by G_Ω the Galois group of the polynomial f.

Definition 6.7.1 *Let L be a subgroup of $\mathfrak{S}_n$ which contains G_Ω. Let $\Theta \in k[x_1, \ldots, x_n]$. The* L-relative resolvent of Ω by Θ, *denoted by $\mathcal{L}_{\Theta, I_\Omega^L}$, is the following polynomial of $k[X]$:*

$$\mathcal{L}_{\Theta, I_\Omega^L}(X) = \prod_{\Phi \in L.\Theta} (X - \Phi(\Omega)) ,$$

where $L.\Theta$ is the natural orbit of the polynomial Θ under the action of the group L. When $L = \mathfrak{S}_n$ the resolvent $\mathcal{L}_{\Theta, I_\Omega^{\mathfrak{S}_n}}$ is called the absolute resolvent *of f by Θ.*

Remark 6.7.2 In the literature the polynomial $\mathcal{L}_{\Theta, I_\Omega^L}$ is usually called an L-relative resolvent of f by Θ. The fact that the coefficients of $\mathcal{L}_{\Theta, I_\Omega^L}$ lie in k follows easily from Galois theory.

Definition 6.7.3 *Let H be a subgroup of L and $\Theta \in k[x_1, \ldots, x_n]$. The polynomial Θ is an* L-primitive H-invariant *if*

$$H = \{\sigma \in L \mid \sigma.\Theta = \Theta\} .$$

It is called an L-primitive H-invariant separable *if $H = \{\sigma \in L \mid \sigma.\Theta(\Omega) = \Theta(\Omega)\}$.*

The following results are well-known.

Lemma 6.7.4 *Let L and H be two subgroups of $\mathfrak{S}_n$ such that $G_\Omega < L$ and $H < L$. Let Θ be an L-primitive H-invariant and $d = \mathrm{card}(H)$. Then the degree of $\mathcal{L}_{\Theta, I_\Omega^L}(X)$ is the index of H in L and*

$$C_{\Theta, I_\Omega^L} = (\mathcal{L}_{\Theta, I_\Omega^L})^d . \tag{6.11}$$

Since k is a perfect field, the above lemma gives another proof that the coefficients of the L-relative resolvent of Ω by Θ belongs to k and when this resolvent is separable, it is exactly the minimal polynomial of the endomorphism $\hat{\Theta}$.

6.7.2 Some algorithms

Since the characteristic polynomial is a power of the resolvent it is possible to obtain a resolvent from a characteristic polynomial by a n-th root computation. Let p be a monic polynomial in $k[X]$ and $q = p^d$ where d is an integer. Let us call $\mathsf{nthRoot}(q, d)$ a function which returns the polynomial p; it is based on the work of P. Henrici [Hen56] and F. Lehobey [Leh97]. Based on the fact that the considered Galois ideals are triangular, an algorithm for computing relative resolvents is easily obtained from the algorithm $\mathsf{CharPol}$ of Section 6.6.

Theorem 6.7.5 *Let L be a subgroup of $\mathfrak{S}_n$ such that $G_\Omega < L$. Let $T_L = \{f_1, \ldots, f_n\}$ be a separable triangular set which generates the ideal I^L_Ω. Let H be a subgroup of L and Θ be an L-primitive H-invariant. Then the algorithm* $\mathsf{Resolvent}(L, T_L, H, \Theta)$ *presented below computes the L-relative resolvent $\mathcal{L}_{\Theta, I^L_\Omega}$ of Ω by Θ.*

$\mathsf{Resolvent}(L, T_L, H, \Theta) ==$
$d := \mathrm{card}(H)$
$C := \mathsf{CharPol}(T_L, \Theta)$
$\mathrm{output}(\mathsf{nthRoot}(C, d))$

Proof. It follows immediately from Theorem 6.6.2 and formula (6.11). □

Remark 6.7.6 The above algorithm gives the main idea for the computation of L-relative resolvents. For an efficient implementation, the power d has to be eliminated during the successive computations of resultants in the algorithm charPol. This can be realized by a direct extension of the results in [Leh97].

The other drawback is the growth of the number of terms. The computation may be performed modulo the ideal I^L_Ω as described in [RV99] for the particular case where $L = \mathfrak{S}_n$. Thus the growth of coefficients is controlled and some variables may be eliminated before the computation of the corresponding resultant. But the following degenerated case may occur with the computation modulo the ideal I^L_Ω: the resolvent is not the result of the computation but a power of the result (see [RV99]). However, since its degree is known, the resolvent is then immediately obtained from the result of the computation as illustrated in Example 6.7.14 of Section 7. A detailed review of these techniques could not take place here; their adaptation consists mainly in replacing the Cauchy moduli by a triangular set which generates I^L_Ω in the proofs of the original papers.

In order to compute practically the resolvent we need the triangular set T_L. Of course it suffices to know any system of generators of the ideal I^L_Ω to obtain T_L by a Gröbner basis computation. The following lemma is of prime importance to obtain a system of generators of I^L_Ω. The reader can refer to [Val97] for the proof.

Lemma 6.7.7 *Let M and L be two subgroups of $\mathfrak{S}_n$ such that $G_\Omega < M$ and $G_\Omega L$ is a group. Let Θ be an M-primitive L-invariant. We set $\theta = \Theta(\Omega)$. Let $\mathrm{Min}_{\theta,k}$ be the minimal polynomial of θ over k. If θ is a simple root of the resolvent $\mathcal{L}_{\Theta, I^M_\Omega}$ then*

$$I^L_\Omega = I^M_\Omega + \langle \mathrm{Min}_{\theta,k}(\Theta) \rangle \ .$$

Remark 6.7.8 The fact that θ must be a simple root of the resolvent in Lemma 6.7.7 is not really restrictive. Indeed it is known that if k is infinite then there exists an L-primitive H-invariant Θ such that $\mathcal{L}_{\Theta, I^L_\Omega}$ is separable (see [AV96]).

From now on, we assume that k is infinite. We thus consider that we always may compute separable invariants. Let us denote by $\mathsf{Groebner}(PS)$ a function which computes a reduced lexicographical Gröbner basis of the ideal generated by a finite subset PS of $k[x_1, \ldots, x_n]$. We show below that the algorithm Resolvent is a convenient tool to compute triangular Galois ideals.

Theorem 6.7.9 *Let M and L be two subgroups of $\mathfrak{S}_n$ such that $G_\Omega < L < M$. Let T_M be a separable triangular set of generators of the Galois ideal I_Ω^M. Then algorithm* TriangSet(L, M, T_M) *given below computes a separable triangular set of generators of I_Ω^L.*

TriangSet(L, M, T_M) ==
  $\Theta :=$ an M-primitive L-invariant separable for Ω
  $\mathcal{L} :=$ Resolvent(M, T_M, L, Θ)
  factorize $\mathcal{L}$
  $\theta :=$ the root of a linear factor of $\mathcal{L}$
  output(Groebner$(T_M \cup \{\Theta - \theta\})$)

Proof. Let $\theta = \Theta(\Omega)$. The polynomial Θ is invariant by the Galois group of Ω since Θ is an M-primitive L-invariant. Therefore we have $\theta \in k$ and $\mathrm{Min}_{\theta,k} = X - \theta$. Besides, θ is a simple root of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$. It follows that the value of θ is provided by the factorization of L. Finally the output is a reduced lexicographical Gröbner basis of I_Ω^L by Lemma 6.7.7. It is a triangular set by Theorem 6.5.4 and Remark 6.2.7. □

With the notations of Theorem 6.7.9, we always can choose $\mathfrak{S}_n$ for M and the Cauchy moduli of f for T_M. Hence the Galois ideal I_Ω^L is always computable by the algorithm TriangSet. The following theorem is obviously deduced:

Theorem 6.7.10 *Let L and be a subgroup of $\mathfrak{S}_n$ which contains G_Ω. Let H be a subgroup of L and Θ be an L-primitive H-invariant. Then the relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ is computed by the algorithm* RelativeResolvent(L, H, Θ) *below.*

RelativeResolvent(L, H, Θ) ==
  $T :=$ the Cauchy moduli of f
  $T_L :=$ TriangSet$(L, \mathfrak{S}_n, T)$
  output(Resolvent(L, T_L, H, Θ))

Remark 6.7.11 If we want to avoid computing resolvents with high degrees, the computation of $\mathcal{L}_{\Theta, I_\Omega^L}$ (and those of I_Ω^L) can be performed by several steps with intermediate computations of relative resolvents and Galois ideals. Actually, let

$$L = L_e < \ldots < L_0 = \mathfrak{S}_n$$

be a chain of subgroups of $\mathfrak{S}_n$ with $G_\Omega < L$. For each $j \in [0, e]$ we denote by T_j the triangular set which generates L_j. By repeating the algorithm TriangSet(L_{j+1}, L_j, T_j) for j in $[0, e-1]$, we obtain $T_L = T_e$; then the algorithm Resolvent(L, T_L, H, Θ) computes the relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$. Note that if $L = G_\Omega$ then the last triangular set T_e computed by the algorithm TriangSet generates the ideal of relations I_Ω.

Remark 6.7.12 Our algorithm is adapted for the computation of relative resolvents which are involved by the incremental method presented in [Val97] for computing the Galois group and the ideal of relations of a polynomial f. It also may be easily inserted in a method for computing Galois group by using partition and group matrices (see [Val95]).

6.7.3 Explicit examples

Our method for computing relative resolvents is not yet fully implemented but the necessary tools are available in the AXIOM computer algebra system. The two examples presented below give the idea of the implementation which may be realized. In these examples we consider the polynomial $f = x^6+2$, irreducible over $\mathbb{Q}$, whose Galois group is a transitive subgroup of $\mathfrak{S}_6$.

Example 6.7.13 Let L =PGL$(2,5)$ be the transitive maximal subgroup of $\mathfrak{S}_6$ of degree 120 and H be the dihedral group $\mathcal{D}_6$. We have $H < L$. The polynomial $\Theta_1 = x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1$ is a primitive $\mathcal{D}_6$-invariant, and a fortiori a PGL$(2,5)$-primitive $\mathcal{D}_6$-invariant. We compute below the PGL$(2,5)$-relative resolvent of f by Θ_1, which has degree $10 = [L : H]$.

First, we need the triangular set of generators T_L of I_Ω^L. In this step it will be also verified that G_Ω is a subgroup of L. The only way to obtain T_L consists in applying the algorithm $\mathsf{TriangSet}(L, M, T_M)$ with $\mathfrak{S}_6$ as M and the Cauchy moduli of f as T_M. We have:

$$\begin{aligned}
T_{\mathfrak{S}_6} \;=\; & \{x_1^6+2,\\
& x_2^5 + x_1x_2^4 + x_1^2x_2^3 + x_1^3x_2^2 + x_1^4x_2 + x_1^5,\\
& x_3^4 + x_2x_3^3 + x_1x_3^3 + x_2^2x_3^2 + x_1x_2x_3^2 + x_1^2x_3^2 + x_2^3x_3 + x_1x_2^2x_3 + x_1^2x_2x_3\\
& +x_1^3x_3 + x_2^4 + x_1x_2^3 + x_1^2x_2^2 + x_1^3x_2 + x_1^4,\\
& x_4^3 + x_3x_4^2 + x_2x_4^2 + x_1x_4^2 + x_3^2x_4 + x_2x_3x_4 + x_1x_3x_4 + x_2^2x_4 + x_1x_2x_4 + x_1^2x_4\\
& +x_3^3 + x_2x_3^2 + x_1x_3^2 + x_2^2x_3 + x_1x_2x_3 + x_1^2x_3 + x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3,\\
& x_5^2 + x_4x_5 + x_3x_5 + x_2x_5 + x_1x_5 + x_4^2 + x_3x_4 + x_2x_4 + x_1x_4 + x_3^2 + x_2x_3\\
& +x_1x_3 + x_2^2 + x_1x_2 + x_1^2,\\
& x_6 + x_5 + x_4 + x_3 + x_2 + x_1\}\ .
\end{aligned}$$

We denote by Θ_L the primitive L-invariant given in [Gir87] (we do not give the explicit expression of this very big invariant). The computation of the separable absolute resolvent of f by Θ_L is realized by an implementation of the method given in [RV99] for which the present work is a generalization. Its factorization over $\mathbb{Q}$ is the following:

$$\mathcal{L}_{\Theta_L, I_f^{\mathfrak{S}_6}}(X) = (X-42)(X-24)^2(X+6)^3\ .$$

It gives a simple linear factor $(X-42)$ which proves that $G_\Omega <$ PGL$(2,5)$. As specified in our algorithm, we deduce that I_Ω^L is generated by the union of the ideal $I_\Omega^{\mathfrak{S}_6}$ and the ideal $< \Theta_L - 42 >$. The computation of the reduced Gröbner basis for the lexicographical ordering of I_Ω^L provides T_L:

$$\begin{aligned}
T_{\mathrm{PGL}(2,5)} \;=\; & \{x_1^6+2,\\
& x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5,\\
& x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 + x_3x_2^3 + x_3x_2^2x_1 + x_3x_2x_1^2
\end{aligned}$$

$$
\begin{aligned}
&+x_3x_1^3+x_2^4+x_2^3x_1+x_2^2x_1^2+x_2x_1^3+x_1^4,\\
&24x_4+5x_3^3x_2^4+6x_3^3x_2^3x_1+8x_3^3x_2^2x_1^2+x_3^3x_2x_1^3+8x_3^2x_2^4x_1+4x_3^2x_2^3x_1^2\\
&+8x_3^2x_2^2x_1^3+12x_3x_2^4x_1^2+10x_3x_2^3x_1^3+4x_3x_2^2x_1^4+4x_3x_2x_1^5+4x_3+5x_2^4x_1^3\\
&+14x_2+12x_1,\\
&24x_5-5x_3^3x_2^4-7x_3^3x_2^3x_1-16x_3^3x_2^2x_1^2-7x_3^3x_2x_1^3-5x_3^3x_1^4-8x_3^2x_2^4x_1\\
&-12x_3^2x_2^3x_1^2-12x_3^2x_2^2x_1^3-8x_3^2x_2x_1^4-12x_3x_2^4x_1^2-16x_3x_2^3x_1^3-12x_3x_2^2x_1^4\\
&+8x_3-5x_2^4x_1^3-5x_2^3x_1^4-2x_2-2x_1,\\
&24x_6+x_3^3x_2^3x_1+8x_3^3x_2^2x_1^2+6x_3^3x_2x_1^3+5x_3^3x_1^4+8x_3^2x_2^3x_1^2+4x_3^2x_2^2x_1^3\\
&+8x_3^2x_2x_1^4+6x_3x_2^3x_1^3+8x_3x_2^2x_1^4-4x_3x_2x_1^5+12x_3+5x_2^3x_1^4+12x_2+14x_1\} \ .
\end{aligned}
$$

Now, it is possible to compute the L-relative resolvent of f by Θ_1 with the algorithm $\mathsf{Resolvent}(L, T_L, H, \Theta_1)$. As explained in Remark 6.7.6, its computation may also be performed modulo the ideal $I_\Omega^{\mathrm{PGL}(2,5)}$ as follows:

- Let $R_0(X, x_1, \ldots, x_6) = X - \Theta_1$. The reduction of R_0 modulo the ideal I_Ω^L (given by successive Euclidean divisions) eliminates the variables x_6, x_5 and x_4. Let $W_0(X, x_1, x_2, x_3)$ be the result of this reduction.

- We set $R_1(X, x_1, x_2) = \mathrm{Res}_{x_3}(f_3, W_0)$. The reduction of R_1 modulo the ideal I_Ω^L does not eliminate the variables x_1 and x_2 of respective degrees 32 and 28 in R_1, but produces a new polynomial W_1 of degree 4 in each variables x_1 and x_2.

- The elimination of the variable x_2 is given by $R_2(X, x_1) = \mathrm{Res}_{x_2}(f_2, W_1)$. The reduction of R_2 modulo the ideal I_Ω^L produces a univariate polynomial of degree 20 whose factorization is the following:

$$X^2(X^3-2)^2(X^3+2)^4 \ .$$

- Since the PGL(2, 5)-relative resolvent of Ω by Θ_1 has degree $10 = [L : H]$, we obtain the following factorization over $\mathbb{Q}$:

$$\mathcal{L}_{\Theta_1, I_\Omega^{\mathrm{PGL}(2,5)}}(X) = X(X^3-2)(X^3+2)^2 \ .$$

  For this example the extraneous power appears only at the last step, for the computation of the polynomial R_2. Hence we did not have to eliminate some extraneous power and use the function $\mathsf{nthRoot}$ during the process.

Example 6.7.14 Let $\Theta_2 = x_4x_5^2 + x_3x_6^2 + x_5x_2^2 + x_2x_3^2 + x_6x_1^2 + x_1x_4^2$. The polynomial Θ_2 is a $\mathcal{D}_6$-primitive $\mathcal{C}_6$-invariant, where $\mathcal{C}_6$ is the cyclic group of order 6. We compute below the $\mathcal{D}_6$-relative resolvent of f by Θ_2.

Remark that the factorization of $\mathcal{L}_{\Theta_1, I_\Omega^{\mathrm{PGL}(2,5)}}$, given in Example 6.7.13, provides a simple linear factor over $\mathbb{Q}$. This implies that $\mathcal{D}_6$ contains actually the Galois group G_Ω.

The first step consists in computing the Galois ideal $I_\Omega^{\mathcal{D}_6}$. It can be efficiently performed with the algorithm $\mathsf{TriangSet}(\mathcal{D}_6, \mathrm{PGL}(2,5), T_{\mathrm{PGL}(2,5)})$ instead of using $\mathfrak{S}_6$ and the Cauchy moduli of f.

We only have to compute a Gröbner basis if we use the computation of the resolvent in Example 6.7.13 and its factorization. The ideal fixed by $\mathcal{D}_6$ is given by:

$$I_\Omega^{\mathcal{D}_6} = I_\Omega^{\mathrm{PGL}(2,5)} + \langle \Theta_1 - 0 \rangle \ ,$$

where 0 is the value given by the simple linear factor over $\mathbb{Q}$ of the resolvent $\mathcal{L}_{\Theta_1, I_\Omega^{\mathrm{PGL}(2,5)}}$.

In the same way as for the ideal fixed by $\mathrm{PGL}(2,5)$, we compute from Θ_1 and the polynomials of $T_{\mathrm{PGL}(2,5)}$ the following triangular Gröbner basis of the Galois ideal $I_\Omega^{\mathcal{D}_6}$:

$$T_{\mathcal{D}_6} = \{x_1^6 + 2, x_2 + x_1, x_3^2 + x_1x_3 + x_1^2, x_4 + x_3, x_5 + x_3 + x_1, x_6 - x_3 - x_1\} \ .$$

Then we perform the computation of $\mathsf{Resolvent}(\mathcal{D}_6, T_{\mathcal{D}_6}, \mathcal{C}_6, \Theta_2)$ modulo the ideal $I_\Omega^{\mathcal{D}_6}$. The reduction of Θ_2 modulo the ideal $I_\Omega^{\mathcal{D}_6}$ produces the value 0. Therefore the result of our computation is immediately the polynomial X. But the degree of a $\mathcal{D}_6$-relative resolvent is 2, the index of $\mathcal{C}_6$ in $\mathcal{D}_6$. We are in the degenerated case mentioned in Remark 6.7.6, where the resolvent is a power of the result of the computation. We thus deduce that the resolvent is

$$\mathcal{L}_{\Theta_2, I_\Omega^{\mathcal{D}_6}}(X) = X^2 \ .$$

Remark 6.7.15 We used the very powerful Gröbner engine FGb (see [Fau97]) developed by J.C. Faugère to obtain our Gröbner basis quickly.

Chapitre 7

Une comparaison de plusieurs méthodes

Résumé

Ce chapitre consiste en une comparaison expérimentale de plusieurs méthodes de décomposition triangulaire. C'est un travail réalisé en collaboration avec M. Moreno Maza dans lequel nous avons cherché à comparer l'efficacité et les sorties de quatres méthodes de décomposition triangulaires, celles de [Wu87], [Laz91a], [Kal95] et [Wan93b]. Sachant qu'il est difficile de comparer expérimentalement des algorithmes puisque la manière de les implanter est primordiale, nous avons cherché à limiter le plus possible les différences qui proviennent de l'implantation.

Nous présentons le cadre de ce travail dans la section 1. Nous donnons ensuite dans la section 2 un aperçu des trois méthodes qui ne sont pas détaillées dans cet ouvrage, en particulier leurs spécifications. À cette occasion nous présentons une version récursive de l'algorithme de [Wan93b] que nous avons implanté et qui nous semble intéressante pour la compréhension de cette méthode. Nous développons dans la section 3 les exigences qui ont guidé notre travail et présentons notre implantation commune dans le système de calcul formel AXIOM. La section 4 contient des données expérimentales obtenues sur un ensemble d'exemples tests dont beaucoup sont classiques et proviennent de la base du projet Européen PoSSo [Com92]. Ils sont disponibles par ftp dans `ftp://www-calfor.lip6.fr/pub/papers/TriangularSets`. Nous étudions plus en détail certains de ces exemples. Dans la section 5 nous considérons des résultats expérimentaux publiés antérieurement, qui peuvent être en relation avec d'autres approches de la décomposition triangulaire de systèmes algébriques. Nous présentons finalement quelques conclusions que nous avons pu tirer de notre travail dans la dernière partie.

7.1 Introduction

We are concerned here with the following problem: given a finite family F of multivariate polynomials over a field k with ordered variables $x_1 < x_2 < \cdots < x_n$, we want to describe the affine variety $\mathbf{V}(F)$ Such a description is usually provided by a finite family $\{T_1, \ldots, T_r\}$ of polynomial sets with particular properties, a relation between the T_i and F, and an algorithm to compute the T_i from F. A well-developed method since [Buc65] is the following: given an ordering on the monomials, choose for T_1 the Gröbner basis of the ideal generated by F and compute it by the Buchberger's algorithm.

Following the work of Ritt [Rit32] [Rit66], Wu Wen-Tsün [Wu86] introduced another way of solving algebraic systems which is the one we are concerned with. In that case each T_i is a polynomial set such that two distinct polynomials in T_i have distinct greatest variables. Such a T_i is called a triangular set. A point $\zeta \in \mathbf{V}(T_i)$ is called regular if for every $p \in T_i$ the point ζ does not cancel the initial of p (that is the leading coefficient of p regarded as a univariate polynomial in its greatest variable). Then, in Wu's method, the variety $\mathbf{V}(F)$ is the union of the regular zeros of the T_i and this decomposition can be computed by Wu's CHRST-REM algorithm [Wu87]. This method has been investigated in many papers. Among them: [Cho88, CG90, CG92, GM90, Wan92a, Wan92b]. Wu's method is efficient for geometric problems where the degenerate solutions are not interesting. For general problems it seems to be difficult to obtain an efficient implementation and this method may produce superfluous triangular sets. Wu's algorithm, like Buchberger's, depends on many choices; moreover its result is not uniquely defined.

Lazard [Laz91a] proposed a new method to obtain Wu-like decompositions for affine varieties. However in that case the definition of triangular sets has been strengthened in order to guarantee non-redundant and more canonical decompositions. Some details and proofs were not given in detail, especially on the subject of gcd computation, which is the main tool of the method. In [Mor97], these questions are treated and a first implementation of Lazard's method is described and shown to be efficient.

Kalkbrener [Kal91] introduced another type of triangular sets called regular chains (Definition 4.4.5) together with another relation between F and the T_i. In that case $\mathbf{V}(F)$ is the union of the closures (w.r.t. Zarisky topology) of the regular zeros of the T_i.

Wang [Wan93b] proposed a generalization of Wu's decompositions for affine varieties. This approach allows the resolution of quasi-algebraic systems. In that case $\mathbf{V}(F)$ is given as a (finite) union of regular zero sets of triangular systems. This method involves Wu's triangular sets but its process is different from Wu's one and seems to be more efficient.

Let us give an example to illustrate the difference between Wu, Lazard and Wang's way of solving, and Kalkbrener's one. We consider the system given by the following polynomials where the ordered variables are $c_2 > s_2 > c_1 > s_1 > b > a$ and where the coefficients lie in the field of rational numbers:

$$\left\{c_1\ c_2 - s_1\ s_2 + c_1 - a,\ s_1\ c_2 + c_1\ s_2 + s_1 - b,\ c_1^2 + s_1^2 - 1,\ c_2^2 + s_2^2 - 1\right\}$$

Our implementation of Lazard's method produces the decomposition $\{T_1, T_2, T_3\}$ where:

$$\begin{array}{rcl} T_1 & = & \{(4\ b^2 + 4\ a^2)\ s_1^2 + (-4\ b^3 - 4\ a^2\ b)\ s_1 + b^4 + 2\ a^2\ b^2 + a^4 - 4\ a^2, \\ & & 2\ a\ c_1 + 2\ b\ s_1 - b^2 - a^2, \\ & & 2\ a\ s_2 + (2\ b^2 + 2\ a^2)\ s_1 - b^3 - a^2\ b, \\ & & 2\ c_2 - b^2 - a^2 + 2\} \\ T_2 & = & \{a,\ 2\ s_1 - b,\ 4\ c_1^2 + b^2 - 4,\ s_2 - b\ c_1,\ 2\ c_2 - b^2 + 2\} \\ T_3 & = & \{a,\ b,\ c_1^2 + s_1^2 - 1,\ s_2,\ c_2 + 1\} \end{array}$$

What does this solution mean? How this solution has to be understood? In T_1, one may arbitrarily choose a and b once $a(b^2 + a^2) \neq 0$, and obtain successively the values of the indeterminates s_1, c_1, s_2, c_2. The triangular sets T_2 and T_3 describe the case $a = 0$. Note that in T_2, one may choose an arbitrary b whereas it is zero in T_3. So, where is the case $b^2 + a^2 = 0$? It is described by T_3. In fact, if we add this equation to the input system the computed decomposition is only $\{T_3\}$. Now, our implementation of Kalkbrener's algorithm produces the decomposition $\{C\}$ where:

$$\begin{array}{rcl} C & = & \{(4\ b^2 + 4\ a^2)\ s_1^2 + (-4\ b^3 - 4\ a^2\ b)\ s_1 + b^4 + 2\ a^2\ b^2 + a^4 - 4\ a^2, \\ & & 2\ a\ c_1 + 2\ b\ s_1 - b^2 - a^2, \\ & & s_2 - b\ c_1 + a\ s_1, \\ & & s_1\ c_2 + b\ c_1^2 - a\ s_1\ c_1 + s_1 - b\} \end{array}$$

In that case a point is a solution of the input system if it lies in the closure of the set of the regular zeros of C. Although C and T_1 are different, they have the same regular zero sets and the closure of these sets contains the regular zeros of the previous T_2 and T_3. Thus Kalkbrener's output is simpler however further computations are needed to describe the zeros satisfying $a(b^2 + a^2) = 0$.

In the conclusion of [Kal93] the author writes: A comparison with the algorithms of Ritt, Wu and Lazard seems to be interesting. In [Wan93b] the author concludes: A systematic analysis and comparison among them (the elimination methods of Lazard and Kalkbrener) both theoretically and practically remain interesting for future work.

The aim of our work is to compare from a practical point of view the methods of [Wu87], [Laz91a], [Kal95] and [Wan93b]. We realized a unified implementation in the AXIOM computer algebra system [JS92, BDI+94] in order to compare these four methods. In Section 7.3, we discuss the matter of comparing the capabilities of different algorithms. Let us mention here that a crucial point is that their implementations need to share the same polynomial arithmetic and data-structures.

The complexity of these algorithms, based on pseudo-division, is not known and to determine it is still a challenging task. Anyway, theoretical complexity considerations are not sufficient for the development of Computer Algebra; it is crucial to evaluate the possible efficiency of the algorithms on an experimental level.

Few papers report on the implementation of some method for computing triangular decompositions of algebraic systems. Moreover, the examples which are presented in these papers differ from one to the other and the characteristics of the computer are generally not much detailed. Thus the capabilities of the different algorithms do not clearly appear. Besides, it is important to focus on the properties of the outputs (representation, size, legibility,

...) since a triangular decomposition of a given polynomial system is not uniquely defined and two distinct implementations of the same method may produce distinct outputs on the same example.

Let us recall that an experimental comparison between Wu's method and Wang's triangular series based method is reported in [Wan96]. It appears that Wang's method is more efficient than Wu's characteristic set method. This extensive comparison is performed with the three notions of reduction, proposed in [Wu87]. Another notion of reduction (in the sense of iterated initials, see Definition 2.1.8) is presented here. Our implementation of Wu's algorithm is realized with this new notion and confirm the experimental results of [Wan96].

Obviously, the methods considered in this experimental work can also be applied to a (lexicographical) Gröbner basis as input. It happens sometimes that this is the only way to get a result in a human time. However we restrict ourselves to methods which accept any set of equations as input and do not compute Gröbner bases explicitly. This choice was influenced by complexity reasons: Gröbner bases have double exponential behavior in worst cases – see [MM82] and [Huy86] – and direct triangular methods may simply have exponential complexity as indicated by [GM90]. This is a strong reason for solving polynomial systems by means of methods which do not rely on explicit Gröbner bases computations.

Thus our comparative implementation excludes methods like *Lextriangular* [Laz92] or the approach of M. Möller [Möl93], which is generalized in [Grä95].

We also specify that polynomial factorization (into irreducibles) is not a necessary tool in the four methods of our comparison. It is true that this technique is exploited in some implementations since it may discover some splits and thus make the decomposition easier to obtain. However it is not a general rule, and systematic factorizations may also be costly in difficult problems (and the AXIOM factorizer is not very efficient). After some preliminary tests it appeared that the use of factorization did not really modify the differences between the four methods of our comparison. Hence, we implemented the methods without using this technique.

7.2 Methods

This section summarizes the four methods. We recall the specifications of each method together with the properties of the decompositions that they compute. A detailled review of these methods could not take place here. The reader may refer to the original papers.

We present the first method proposed by D. Wang in [Wan93b]. In fact we suggest here a recursive presentation of this method. Note that the outputs of Wang's algorithm are different from the other ones in the sense that they are not triangular sets but *fine triangular quasi-algebraic systems* (Definition 7.2.3).

The basic ideas of Wu's method are given but for more details one can refer to [Wu87] or [Wan91].

We recall the main features of the methods of Lazard [Laz91a] and Kalkbrener [Kal91] which both involve gcd computations over towers of simple extensions.

Our implementation of Lazard's method is based on an algorithm for gcd computations of univariate polynomials with coefficients in a separable tower of simple extensions [Mor97].

The idea is a generalisation of the one of [MR95]. This algorithm is rather technical and could not be sketched here.

We use the AXIOM programming language for describing the algorithms presented in this section.

Notation 7.2.1 *Let $p \in \mathbf{P}_n$ be a polynomial and $T \subseteq \mathbf{P}_n$ be a triangular set. There exists a polynomial $r \in \mathbf{P}_n$, initially reduced w.r.t. T, and, a product of the initials of T, denoted by s, such that $sp - r \in \langle T \rangle_{\mathbf{P}_n}$. We define* $\mathsf{iRed}(p, T) = r$*. For algorithmical details about reduction of polynomials w.r.t. triangular sets see [Mor97]. Now, for $F \subseteq \mathbf{P}_n$ we set* $\mathsf{iRed}(F, T) = \{\mathsf{iRed}(p, T)\ ,\ p \in F\}$*. Finally, we define* $\mathsf{prem}(F, T) = \{\mathsf{prem}(p, T)\ ,\ p \in F\}$*.*

7.2.1 Wang's method

Wang's method computes a finite family $\{(T_1, Q_1), \ldots, (T_r, Q_r)\}$ of fine triangular q.a.s. (see Definition 7.2.3 below) such that

$$\mathbf{V}(F) \ = \ \bigcup_{i=1}^{r} \mathbf{Z}(T_i, Q_i)\ .$$

Such a decomposition is produced by the algorithm $\mathsf{triangulation}(F, \emptyset, \emptyset)$ presented below (Theorem 7.2.8). There is no reason for a fine triangular system produced by the method of Wang (called *elimination without projection* in [Wan93b]) to be necessarily consistent (definition 7.2.3). But, may be due to our optimizations, we never encountered an inconsistent fine triangular system during our experiences. Note that Wang also proposes a method called *elimination with projection* to produce necessarily consistent outputs.

Notation 7.2.2 *Let F be a subset of $\mathbf{P}_n$ such that $F \not\subseteq k$. We denote by* $\mathsf{mvar}(F)$ *the greatest variable which occurs in the polynomials of F.*

Definition 7.2.3 *Every couple $\mathfrak{S} = (P, Q)$, where P and Q are two finite subsets of $\mathbf{P}_n$, is called a* quasi-algebraic system *in $\mathbf{P}_n$* (q.a.s. *for short). Let $\mathfrak{S} = (P, Q)$ be a q.a.s. in $\mathbf{P}_n$. The q.a.s. $\mathfrak{S}$ is called* triangular *if P is a triangular set of $\mathbf{P}_n$. If $Q \neq \emptyset$ then we denote by $h(\mathfrak{S})$ the product of the elements of Q, otherwise we define $h(\mathfrak{S}) = 1$. We call a* zero *of $\mathfrak{S}$ every element of the subset of K^n denoted by $\mathbf{Z}(\mathfrak{S})$ and defined by:*

$$\mathbf{Z}(\mathfrak{S}) = \mathbf{V}(P) \setminus \mathbf{V}(h(\mathfrak{S}))$$

The q.a.s. $\mathfrak{S}$ is called inconsistent *if $\mathbf{Z}(\mathfrak{S}) = \emptyset$, otherwise it is called* consistent*. Finally, following [Wan93a] and [Wan93b], a triangular q.a.s. $\mathfrak{S} = (T, Q)$ is called* fine *if $\mathbf{V}(h(T)) \cap \mathbf{Z}(\mathfrak{S}) = \emptyset$ and $0 \notin \mathsf{prem}(Q, T)$ where $h(T)$ is the product of the initials of T.*

Let $\mathfrak{S} = (P, Q)$ be a q.a.s. in $\mathbf{P}_n$. From now on we assume that $P \not\subseteq k$. Let $\mathsf{mvar}(P) = x_i$. The algorithm $\mathsf{elimination}(x_i, P, Q)$ presented below (Proposition 7.2.7) splits the q.a.s. $\mathfrak{S}$ into several q.a.s. which contain at most one equation with x_i as main variable (see Definition 7.2.4). Its proof is based on the following Lemma 7.2.5 [Wan93a] and Lemma 7.2.6.

Definition 7.2.4 *Let $1 \leq i \leq n$ and $\mathfrak{S} = (P, Q)$ be a q.a.s. in $\mathbf{P}_n$ such that $P \subseteq \mathbf{P}_i$ and $Q \subseteq \mathbf{P}_n$. We call* elimination *of the variable x_i in $\mathfrak{S}$ a set Λ of triplets (P_k, Q_k, τ_k) such that P_k, Q_k and τ_k are finite subsets of $\mathbf{P}_n$ which satisfy the following conditions:*

(i) $P_k \neq \emptyset \Rightarrow \mathsf{mvar}(P_k) < x_i$

(ii) $\tau_k \neq \emptyset \ \Rightarrow \ (\exists t \in \mathbf{P}_i \setminus \mathbf{P}_{i-1}) \ \mid \ \tau_k = \{t\}$

(iii) $\mathbf{Z}(P, Q) = \bigcup_{(P_j, Q_j, \tau_j) \in \Lambda} \mathbf{Z}(P_j \cup \{\tau_j\}, Q_j)$.

Lemma 7.2.5 *Let f be a non constant polynomial in $\mathbf{P}_n$ and (P, Q) a q.a.s. in $\mathbf{P}_n$. Then*

$$\mathbf{Z}(P \cup \{f\}, Q) = \ \mathbf{Z}(\mathsf{prem}(P, f) \cup \{f\}, Q \cup \{\mathsf{init}(f)\}) \ \cup \ \mathbf{Z}(P \cup \{\mathsf{init}(f), \mathsf{tail}(f)\}, Q) \ .$$

Proof. Let $p \in P$ and $r = \mathsf{prem}(p, f)$. There exists $e \in \mathbb{N}$ et $q \in \mathbf{P}_n$ such that $h^e p = q f + r$. From this relation we deduce $\mathbf{Z}(P \cup \{f\}, \{h\}) = \mathbf{Z}(G \cup \{f\}, \{h\})$. Then the result is easily obtained by splitting the zeros of $P \cup \{f\}$ to $\mathbf{Z}(P \cup \{f\}, \{h\})$ and $\mathbf{Z}(P \cup \{f, h\})$. □

Lemma 7.2.6 *Let (P, Q) be a q.a.s. in $\mathbf{P}_n$ and $f \in \mathbf{P}_n \setminus k$. Then*

$$\mathsf{init}(f) \in Q \Rightarrow \mathbf{Z}(P \cup \{f\}, Q) = \mathbf{Z}(P \cup \{f\}, \mathsf{prem}(Q, f)) \ .$$

Proof. Let us denote $\mathsf{init}(f)$ by h and suppose that $h \in Q$. Since h is reduced w.r.t. f we also have $h \in R$. Let $q \in Q$ and $r = \mathsf{prem}(q, f)$. There exists a positive integer e and a polynomial q' such that

$$h^e \, q \ = \ f \, q' \ + r. \tag{7.1}$$

Let us considerer $x \in K^n$ such that $f(x) = 0$ and $h(x) \neq 0$. We deduce from the relation (7.1) that $q(x) \neq 0$ iff $r(x) \neq 0$. Then it follows that $x \in \mathbf{Z}(P \cup \{f\}, Q)$ iff $x \in \mathbf{Z}(P \cup \{f\}, R)$. □

Proposition 7.2.7 *Let v be a variable in $\{x_1, \ldots, x_n\}$ and (P, Q) a q.a.s. in $\mathbf{P}_n$ such that $\mathsf{mvar}(P) \leq v$. Then the algorithm $\mathsf{elimination}(v, P, Q)$ given below, computes an elimination of the variable v in the q.a.s. (P, Q). In particular, if the output of the algoritm is the empty set, then $\mathbf{Z}(P, Q) = \emptyset$.*

- $\mathsf{elimination}(v, P, Q) ==$
  - $P := P \setminus \{0\}$
  - $(0 \in Q)$ **or** $(P \cap k \ \neq \emptyset) \ => \ $ **return**$(\{\ \})$
  - $P_v^- := \{p \in P \mid \mathsf{mvar}(p) < v\}$
  - $P_v := P \setminus P_v^-$
  - $P_v = \emptyset \ => $ **return** $(\ \{(P, Q, \emptyset)\}\ )$
  - $f :=$ a polynomial in P_v with minimal degree in v
  - $P_1 := (P_v \setminus \{f\}) \ \cup \ \{\mathsf{init}(f), \mathsf{tail}(f)\} \ \cup \ P_v^-$
  - $Q_2 := Q \ \cup \{\mathsf{init}(f)\}$
  - **empty?** $(P_v \setminus \{f\}) =>$ **return** $(\ \{(P_v^-, \mathsf{prem}(Q_2, f), \{f\})\} \ \cup \ \mathsf{elimination}(v, P_1, Q)\ )$
  - $P_2 := \mathsf{prem}(P_v \setminus \{f\}, f) \ \cup \ \{f\} \ \cup \ P_v^-$
  - **return** $(\ \mathsf{elimination}(v, P_2, Q_2) \ \cup \ \mathsf{elimination}(v, P_1, Q)\ )$

Proof. Let us define $s(P) = \sum_{p \in P \setminus \{0\}} \mathsf{deg}(p, v)$. We will prove termination and correctness by induction on $s(P)$.

If a constant occurs in P or if $0 \in Q$, the result is obvious. Otherwise, if $s(P) = 0$, then $P_v = \emptyset$ and the algorithm terminates. The correctness is obvious. Now we assume that $s(P) > 0$, i.e. P_v is not empty. First we remark that $s(P_1) < s(P)$ since $\mathsf{deg}(\mathsf{init}(f), v) = 0$ and $\mathsf{deg}(\mathsf{tail}(f), v) < \mathsf{deg}(f, v)$. Two cases can be distinguished:

(i) $P_v = \{f\}$. By induction $\mathsf{elimination}(v, P_1, Q)$ terminates and is correct. Therefore the algorithm $\mathsf{elimination}(v, P, Q)$ terminates. The correction follows from Lemma 7.2.5 and Lemma 7.2.6.

(ii) $P_v \setminus \{f\} \neq \emptyset$. We put $P' = P_v \setminus \{f\}$. For any p in P' we have $\mathsf{deg}(\mathsf{prem}(p, f), v) < \mathsf{deg}(f, v) \leq \mathsf{deg}(p, v)$. Since P' is not empty, we obtain $s(\mathsf{prem}(P', f)) < s(P')$, and consequently $s(P_2) < s(P)$. Then termination and correctness follow by application of Lemma 7.2.5 and induction hypothesis.

□

By repetead use of the algorithm $\mathsf{elimination}$ with v decreasing, we easily obtain a triangulation of any q.a.s. with the algorithm $\mathsf{triangulation}$ presented below.

Theorem 7.2.8 *Let $1 \leq i \leq n$ and (P, Q) a q.a.s. in $\mathbf{P}_n$ such that $P \subseteq \mathbf{P}_i$. Let T a triangular set of $\mathbf{P}_n$ such that $T \cap \mathbf{P}_i = \emptyset$. Then the following algorithm* $\mathsf{triangulation}(P, Q, T)$ *computes a finite family $\{(T_1, Q_1), \ldots, (T_r, Q_r)\}$ of triangular q.a.s. such that*

$$\mathbf{Z}(P \cup T, Q) = \bigcup_{k=1}^{r} \mathbf{Z}(T_k, Q_k).$$

• $\mathsf{triangulation}(P, Q, T)$ ==
  $P := P \setminus \{0\}$
  $(0 \in Q)$ **or** $(P \cap k \neq \emptyset)$ => **return** ({ })
  empty? P => **return** ($\{(T, Q)\}$)
  $v := \mathsf{mvar}(P)$
  $\Lambda := \mathsf{elimination}(v, P, Q)$
  return ($\bigcup_{(P_j, Q_j, \tau_j) \in \Lambda}$ $\mathsf{triangulation}(P_j, Q_j, \tau_j \cup T)$)

Proof. The proof of the algorithm is obtained by induction on the smallest integer such that $P \subseteq \mathbf{P}_i$, which we will denote by $i(P)$. For $i(P) = 0$, i.e. $P \subseteq R$, the result is obvious. Now assume that $i(P) > 0$. We can eliminate the case $0 \in Q$, the case $P \cap k \neq \emptyset$, and the case $\Lambda = \emptyset$, which terminate immediately and are clearly correct. Then by specifications of the algorithm $\mathsf{elimination}$, we obtain

$$\mathbf{Z}(P \cup T, Q) = \mathbf{Z}(P, Q) \cap \mathbf{V}_K(T) = \bigcup_{(P_j, Q_j, \tau_j) \in \Lambda} \mathbf{Z}(P_j \cup (\{\tau_j\} \cup T), Q_j).$$

Let us denote $T_j = \{\tau_j\} \cup T$. The triplets (P_j, Q_j, T_j) satisfy the input conditions of $\mathsf{triangulation}$. And since $i(P_j) < i(P)$, the result follows from the induction hypothesis. □

Remark 7.2.9 It is easy to check that the quasi-algebraic systems produced by the algorithm $\mathsf{triangulation}(F, \emptyset, \emptyset)$ are fines.

7.2.2 Wu's method

Wu used Ritt's work to provide an algorithm for solving systems of algebraic equations by means of triangular sets which only requires pseudo-remainder computations (i.e. no factorizations are needed). Wu's process is based on a procedure called CHRST-REM, see p. 3 in [Wu87]. Given a finite subset F of $\mathbf{P}_n$, this procedure computes a Wu characteristic set T of a finite subset G of $\mathbf{P}_n$ such that $\langle F\rangle = \langle G\rangle$. It involves Ritt ordering for (initially) reduced triangular sets of $\mathbf{P}_n$.

Definition 7.2.10 *Let F be a non-empty finite subset of non constant polynomials in $\mathbf{P}_n$. We call* basic set *of F a subset B of F such that B is a minimal element for Ritt ordering among the family of initially reduced triangular sets contained in F.*

It is easy to compute a basic set of F. Let us denote by $\mathsf{basicSet}(F)$ the result of an algorithm which computes a basic set of F. Now the following algorithm $\mathsf{charSet}$ either returns the set $C = \{1\}$ or computes an initially reduced triangular set C. In both cases C is a Wu characteristic set of F (see Definition 4.2.2) and satisfies the relations of Proposition 4.2.3.

```
charSet(F) ==
    R := F \ {0}
    Q := ∅
    C := ∅
    while (R ≠ ∅) and (R ∩ k = ∅) repeat
        Q := Q ∪ R ∪ C
        C := basicSet(Q)
        Q := Q \ C
        R := iRed(Q, C) \ {0}
    R ∩ k ≠ ∅ => return({1})
    return C
```

Remark 7.2.11 The set C obtained by the above algorithm may be a fine triangular set (i.e. none of its initials reduces to 0 w.r.t. C) of F even if F generates the unit ideal of $\mathbf{P}_n$. For instance, choose $F = \{x_1^2 - x_1, x_1x_2 - 1, (x_1 - 1)x_3 + x_2\}$. In this case the algorithm $\mathsf{charSet}(F)$ returns F itself, but we have $\langle F\rangle = \langle 1\rangle$.

Let $p \in C$. We remark that $\mathbf{V}(F \cup \{\mathsf{init}(p)\}) = \mathbf{V}(F \cup C \cup \{\mathsf{init}(p)\})$. Moreover, the set $C \cup \{\mathsf{init}(p)\}$ has obviously a basic set which is smaller than C w.r.t. Ritt ordering. Therefore, by computing $\mathsf{charSet}(F \cup C \cup \{\mathsf{init}(p)\})$, we obtain a smaller characteristic set than C w.r.t. Ritt ordering. Now one can easily check that every strictly decreasing chain of triangular sets for Ritt ordering is finite. Thus, by virtue of the above formula (ii), repeated calls to the algorithm $\mathsf{charSet}$, allow the computation of a finite family $\{T_1, \ldots, T_r\}$ of initially reduced triangular sets such that

$$\mathbf{V}(F) = \bigcup_{i=1}^{r} \mathbf{W}(T_i)\ .$$

Remark 7.2.12 Note that not only some components $\mathbf{W}(T_i)$ of Wu's decomposition may be empty (as shown in Remark 7.2.11), but also the algorithm may produce superfluous components in the following sense: for some $i \in \{1, \ldots, r\}$ such that $\mathbf{W}(T_i) \neq \emptyset$ there exists $j \in \{1, \ldots, r\}$ with $i \neq j$ such that $\mathbf{W}(T_i)$ is contained in $\mathbf{W}(T_j)$.

7.2.3 Lazard's method

Let T be a triangular set of $\mathbf{P}_n$ and $i \in \{0, \ldots, n\}$. We use below the notations introduced in Section 4.5. Recall that $\mathbf{A}_i = \mathrm{fr}(\mathbf{P}_i/\mathsf{sat}_i(T \cap \mathbf{P}_i))$ and F_i is the canonical algebra homormophism from $\mathbf{P}_{i+1}$ to $\mathbf{A}_i[x_{i+1}]$. The concept of normalization recalled in 2.2.5 is introduced in [Laz91a] which defines the following strong notion of triangular sets.

Definition 7.2.13 *Let T be a triangular set in $\mathbf{P}_n$. For each variable x_i in $\mathsf{algVar}(T)$ we put $t_i = T_{x_i}$ and denote by t_i' the derivative of t_i w.r.t. x_i. We say that T is a* Lazard set *if T is normalized, and if for each variable $x_i \in \mathsf{algVar}(T)$ we have*

(i) [square-free] *$F_{i-1}(t_i)$ and $F_{i-1}(t_i')$ generate the unit ideal in $\mathbf{A}_{i-1}[x_i]$,*

(ii) [primitive] *for each j in the range $1, \ldots, i-1$, the coefficients of t_i, interpreted as a multivariate polynomial in $(\mathbf{A}_{j-1}[x_j])[x_{j+1}, \ldots, x_i]$ generate the unit ideal of $\mathbf{A}_{j-1}[x_j]$.*

It follows from Proposition 4.3.14 that a Lazard set is a regular triangular set. From the requirement (i) we then obtain by induction that the ideal $\langle F_{i-1}(t_i), F_{i-1}(t_i')\rangle$ is radical (see Proposition 3.3.9) and the ring A_i is a finite product of fields. These results may also be found in [Mor97].

Remark 7.2.14 Let $\mathbf{A}_i = \mathbf{K}_{i,1} \times \ldots \times \mathbf{K}_{i,r_i}$. Condition (i) means that for $\ell = 1, \ldots, r_{i-1}$ the image of t_i modulo $\mathbf{K}_{i-1,\ell}$ is square-free. Condition (ii) can be viewed as follows: for each j in $\{1, \ldots, i-1\}$, and for $\ell = 1, \ldots, r_{j-1}$, the image of t_i in $(\mathbf{K}_{j-1,\ell}[x_j])[x_{j+1}, \ldots, x_i]$ is a primitive multivariate polynomial.

Example 7.2.15 Let $T = \{x_1x_2^2 - 3, x_3^2 - 2x_1x_2x_3 + 3x_1\}$. Here $t_3 = x_3^2 - 2x_1x_2x_3 + 3x_1$ and $t_3' = 2x_3 - 2x_1x_2$. We have $\mathbf{A}_2 = k(x_1)[x_2]/\langle x_1x_2^2 - 3\rangle$. It is easy to check that $t_3 \equiv 4{t_3'}^2$ modulo the ideal $\langle x_1x_2^2 - 3\rangle$. Thus, in $\mathbf{A}_2[x_3]$ the polynomial $F_2(t_3)$ lies in the ideal generated by $F_2(t_3')$. Therefore T is not a Lazard set. In fact the polynomial t_3' is the square-free form of t_3 if they are both interpreted in $\mathbf{A}_2[x_3]$ and $\{x_1x_2^2 - 3, t_3'\}$ is a Lazard set.

Let i be in the range $0 \ldots n-1$. Let $T \subseteq \mathbf{P}_i \setminus \mathbf{P}_{i-1}$ be a Lazard set. We put $\mathbf{A}_i = \mathbf{k}_1 \times \cdots \times \mathbf{k}_m$. The main tool for Lazard's method is the computation of gcd in $\mathbf{A}_i[x_{i+1}]$ by a dynamic process of splitting such as the one described in Section 3.3. Computations may be split when a zero-divisor is discovered. Full details of this gcd algorithm and the implementation of Lazard's method appear in [Mor97].

The main procedure of Lazard's method is called $\mathsf{intersect}$. Given $T \subseteq \mathbf{P}_n$ and $p \in \mathbf{P}_n$ the operation $\mathsf{intersect}(p, T)$ returns a finite family of Lazard sets $\{S_1, \ldots, S_l\}$ such that

$$\mathbf{V}(p) \cap \mathbf{W}(T) \subseteq \cup_1^l \mathbf{W}(S_i) \subseteq \overline{\mathbf{V}(p) \cap \mathbf{W}(T)}$$

Given $\{T_1, \ldots, T_s\}$, a finite family of Lazard sets, we define $\mathsf{intersect}(p, \{T_1, \ldots, T_s\})$ as the union of the $\mathsf{intersect}(p, T_i)$. Then, given a finite subset $F = \{f_1, \ldots, f_m\}$ of $\mathbf{P}_n$ we define $\mathsf{intersect}(F, T) = \mathsf{intersect}(f_1, \mathsf{intersect}(\ldots, \mathsf{intersect}(f_m, T)))$. Thus $\mathsf{intersect}(F, \emptyset)$ produces a finite family of Lazard sets $\{S_1, \ldots, S_l\}$ such that

$$\mathbf{V}(F) = \bigcup_{i=1}^{r} \mathbf{W}(S_i) \ .$$

Lazard's decompositions are *irredundant* in the following sense:

$$\bigcup_{j \neq i} \mathbf{W}(T_j) \neq \bigcup_{j} \mathbf{W}(T_j) \ .$$

We will not describe here how to produce irredundant decompositions but give the main steps of the operation $\mathsf{intersect}(p, T)$ proceeds in the following way. Let us mention that an operation is available in our implementation to compute $F_n(p)$.

(l_1) If p is normalized w.r.t. T then go to step (l_2) with $r = p$ else go to next step.

($l_1{}'$) If p is not normalized w.r.t. T, compute two polynomials $q, r \in \mathbf{P}_n$ such that r is normalized w.r.t. T and $F_n(pq - r) = 0$ and ($F_n(p) = 0 \iff F_n(r) = 0$). Polynomials q and r are computed by means of an extended (i.e. with Bezout coefficients) version of the gcd algorithm sketched above. Here the computations may be split if $F_n(p)$ is a zero-divisor. The polynomial r is also denoted by $\mathsf{normalize}(p, T)$. Now, go to next step.

(l_2) If $r = 0$ then return $\{T\}$. Else, if $r \in k$ then returns $\{\,\}$. Else go to next step.

(l_3) Return $\mathsf{intersect}(\mathsf{tail}(r), \mathsf{intersect}(\mathsf{init}(r), T))$ and go to next step.

(l_4) Remove the content of r viewed as univariate in $\mathsf{mvar}(r)$ and go to next step.

(l_5) If $T^-_{\mathsf{mvar}(r)} \cup \{r\}$ is a square-free triangular set (that is, which satisfy squarefree condition of Definition 7.2.13) then go to step (l_7).

(l_6) Let $v = \mathsf{mvar}(r)$. Compute a (normalized w.r.t. T_v^-) gcd of r and its derivative w.r.t. v while interpreting their coefficients in the tower associated to T_v^- (here computations may be split). Let g be this gcd. Replace r by $\mathsf{pquo}(r, g)$. Thus $T_v^- \cup \{r\}$ is now a square-free regular set. Go to step (l_3).

(l_7) Let $v = \mathsf{mvar}(r)$. Define $T_v^+ = \{t_k, \ldots, t_l\}$ with $\mathsf{mvar}(t_k) < \cdots < \mathsf{mvar}(t_l)$. Compute $\mathcal{D} = \mathsf{intersect}(t_l, \mathsf{intersect}(\ldots, \mathsf{intersect}(t_k, T_v^- \cup \{r\})))$. Then remove from $\mathcal{D}$ any triangular set U such that $\mathsf{normalize}(\mathsf{init}(t_i), U^-_{\mathsf{mvar}(t_i)}) = 0$ for some $i \in \{k, \ldots, l\}$. Now, go to next and last step.

(l_8) return $\mathsf{intersect}(p, \mathcal{D})$ where p is the input polynomial.

7.3 Implementation

7.3.1 General requirements

In the introduction we specified why comparing methods for computing triangular decompositions is not an easy task. Recall that each of the algorithms studied in this paper has its own specifications and that a triangular decomposition of a polynomial system by a given method is not uniquely defined.

In order to realize a reasonable comparison we think that the following requirements should meet.

(1) The algorithms must be implemented and run with the same human, material and software conditions (using the same data structures and sub-routines).

(2) A process to check the correctness of the computed decompositions must be implemented.

(3) The experiments must not only focus on timings but also on the legibility of the outputs and their suitability for further computations.

The goal of the first requirement is to get as close as possible to the ideal situation where the differences between computations of triangular decompositions - for a given system - only depend on the corresponding algorithms. Thus our implementations of these methods need to use the same data structures and sub-routines. It is clear that even with the same hardware and software, experimental comparisons strongly depend on some implementation choices.

We thought that the AXIOM computer algebra system [JS92, BDI+94], with its strongly typed and object-oriented language, is convenient to satisfy our first requirement. We defined categories corresponding to the different properties of triangular sets, packages and domains for the common data structures and sub-routines. Furthermore, AXIOM (version 1.2) is connected with GB, the very powerful Gröbner engine developed by J.C. Faugère [Fau94]. This allowed us to run the non-trivial Gröbner basis computations that are required in order to satisfy our other two requirements .

We mentioned that two implementations of the same method for computing triangular decompositions may produce different outputs for a given polynomial system. Therefore it is difficult to be sure that a decomposition is correct. We concentrated on this problem rather than trying to produce very optimized implementations. We think that only checking *by hand* some computations (necessarily simple) produced by an implementation is not sufficient to make sure that this implementation is correct, especially for mixed-dimensional problems. For instance, we discovered a bug in the management of the elimination of redundant branches in our implementation of Wu's method by verifying the computed output on Liu's example. More generally our checking process (described below) is a convenient debugging tool for our implementations.

This checking process:

(i) has been intensively tested for more than a year, *(ii)* is based on simple and well known algorithms and

(iii) is implemented in a direct way in AXIOM as an top-level package of the GB software.

Thus it can be safely considered as reliable.

In our analysis of the computed solutions we also looked for other informations than timings and correctness. Given a solution, we wanted to know if some of the computed triangular sets are inconsistent or if some quasi-components $\mathbf{W}(T_i)$ are contained in another quasi-component $\mathbf{W}(T_j)$ (or in the closure of another quasi-component). An overview of these facilities is given in the subsequent paragraph.

7.3.2 Description of the implementation

Each implementation of the four methods uses the same AXIOM domain for polynomials (with a sparse and recursive representation). Let us recall that an AXIOM category specifies the mathematical properties of the domains which belong to this category. It may also give default definitions for exported operations (eventually redefined in the domains of this category). The main categories and domains of our implementation are described below and their hierarchy is illustrated in Figure 7.1.

First we defined a category *PolynomialSetCategory* for finite subsets of $\mathbf{P}_n$. This category exports and implements operations on sets, ideals and varieties like $(I, J) \longmapsto I \cap J$ and $(I, p) \longmapsto I : p^{\infty}$ where $I, J \subseteq \mathbf{P}_n$ denote ideals and $p \in \mathbf{P}_n$ is a polynomial. We implemented these operations by means of Gröbner bases techniques [CLO92] in an AXIOM package using the connection between AXIOM and the powerful Gröbner engine GB.

Then we wrote a category for triangular sets of $\mathbf{P}_n$ named *TriangularSetCategory*. This category exports and implements basic operations like $(T, v) \longmapsto T_v$ and $(p, T) \longmapsto \mathsf{prem}(p, T)$ and $(p, T) \longmapsto \mathsf{iRed}(p, T)$ (see Notation 7.2.1) where v is a variable and $T \subseteq \mathbf{P}_n$ is a triangular set. It also exports and implements more sophisticated operations like :

(i) $T \longmapsto \mathsf{sat}(T)$ which computes a Gröbner basis of the saturated ideal of T,

(ii) $(F \subseteq \mathbf{P}_n, \{T_1, \ldots, T_r \subseteq \mathbf{P}_n\}) \longmapsto \mathbf{V}(F) \stackrel{?}{=} \cup_i \overline{\mathbf{W}(T_i)}$ which tests if the variety $\mathbf{V}(F)$ is the union of the closures of the $\mathbf{W}(T_i)$.

We use the operations from the category *PolynomialSetCategory* that we mentioned above to perform these latter operations. That way we can check the consistency of a triangular set and the correctness of a triangular decomposition.

Moreover the category *TriangularSetCategory* exports (but does not implement) an operation $F \subseteq \mathbf{P}_n \longmapsto \mathsf{zeroSetSplit}(F)$ which represents any method for solving polynomial system by means of triangular systems.

From the category of general triangular sets we derived a category for *towers of simple extensions* (t.o.s.e.) which corresponds to the properties of regular chains. It exports the associated map of a t.o.s.e. implemented with the operation $(p, T) \longmapsto F_n(p)$ (see Section 4.5). It also exports operations like $(p, T) \longmapsto$ is-$F_n(p)$-a-unit?.

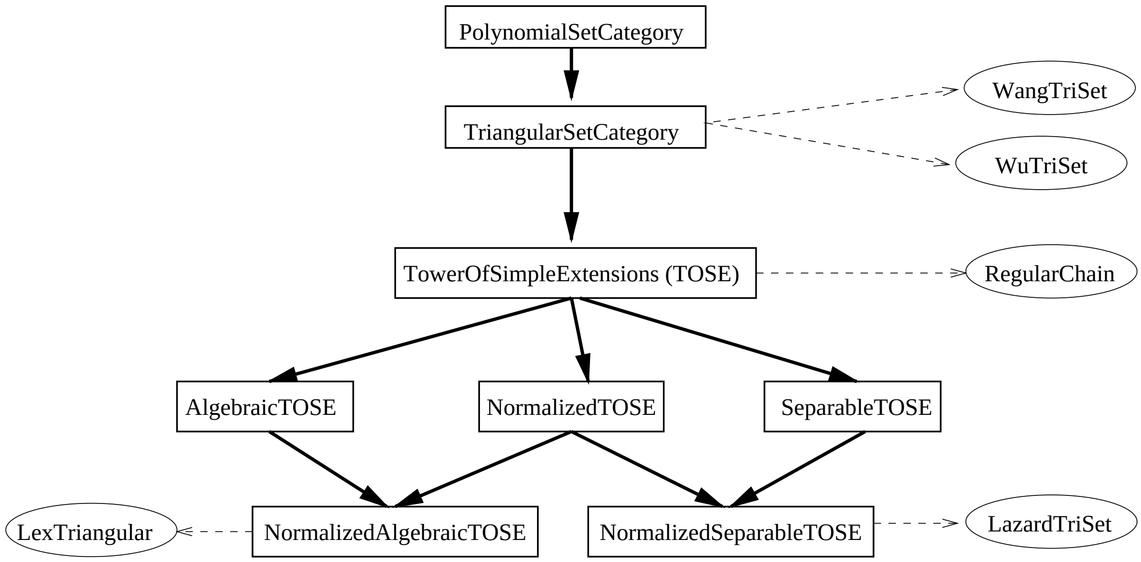

FIG. 7.1 –: *Categories and domains of the implementation*

Finally, from the category of t.o.s.e. we derived three categories corresponding to particular properties.

(1) A category for the towers $T \subseteq \mathbf{P}_n$ such that $\mathsf{algVar}(T) = \{x_1, x_2, \ldots, x_n\}$, called *algebraic t.o.s.e.*,

(2) A category for the normalized towers called *normalized t.o.s.e.*,

(3) A category for the separable towers called *separable t.o.s.e.*

Each method for computing triangular decompositions is an implementation of the operation $F \subseteq \mathbf{P}_n \longmapsto \mathsf{zeroSetSplit}(F)$ in an AXIOM domain of the suitable category. For instance, Kalkbrener's method is implemented in an domain which belongs to the category of t.o.s.e and which is called *RegularChain* (see Figure 7.1). Note that the lexTriangular method [Laz92] is implemented by using the techniques described in [MR95] in an AXIOM domain which belongs to both categories of normalized t.o.s.e. and algebraic t.o.s.e.

7.3.3 Some techniques used in the implementation

Before studying the implementation of each method, let us give some common techniques and optimizations.

We mentioned in the introduction that we do not use polynomial factorization into irreducibles. However square-free factorization of multivariate polynomials has a lower cost. We use it at certain steps of each method, in particular in order to clean up the triangular sets in the outputs: this increases their legibility and helps to discover inconsistent components in Wu's method.

Another common technique is the use of what we call *pre-processing*: the idea is to perform some *inter-reductions* in a polynomial set Q before calling a procedure with Q as a parameter. For instance, this is the case in Wu's method before calling charSet(Q). More precisely polynomials in Q with constant initials are used to reduce the other polynomials. This speeds up the computation of a characteristic set from Q. The same way, in Wang's method, before running elimination(v,P,Q) we reduce the polynomials with main variable v by the polynomials in P_v^- with a constant initial. It appears that this also speeds up our implementation. For the methods of Kalkbrener and Lazard, a *pre-processing* is only performed with the input system F. In this case for each v which is the main variable of some polynomial in F we chose f_v a minimal polynomial in F_v w.r.t. Ritt and Wu ordering. Then we use these polynomials f_v to reduce the other polynomials in F in the sense of Gröbner bases (i.e. we use the division algorithm in $\mathbf{P}_n$ as in [CLO92] p. 59). In many examples (*Arnborg-Lazard, Gonnet, Hairer-2, Butcher*), this speeds up the computation of a triangular decomposition. The factor may go up to 4 in the previous examples for Kalkbrener's method. This may also slow down sometimes the computations (*Gerdt, Liu-Li*). However, this *pre-processing* is used for both methods with all examples.

Concerning the case of Wu's method, most of the optimizations that we use appear in [Wu87] and [Wan92b]. Note that the removal of the redundant branches for this method is not easy since empty components may be produced. Thus, many heuristics are needed.

Several techniques are given in [Wan93b] to improve the practical efficiency of the method. In particular, the author points out the removal of the redundant factors. By means of gcd computations and exact divisions, our implementation actually removes the redundant factors which appear among the set of inequations, or between equations and inequations. Another technique to increase the legibility of an output triangular set T is to reduce the polynomials in T by those with a constant initial.

We remarked in Section 7.2 that some superfluous components may occur in Kalkbrener's decompositions. There may exist indices i_1 and i_2 such that $\overline{\mathbf{W}(T_{i_1})} \subseteq \overline{\mathbf{W}(T_{i_2})}$. As suggested by Kalkbrener, one way to avoid some of these redundant computations is to use Krull's *Primeidealkettensatz* (see p.240 in [SZ67]): since the height of the saturated ideal of a regular chain T equals the number of its elements, we can delete from the output any regular chain which contains more elements than the input system. However, it is not sufficient to remove all superfluous components and we also use the following trick. If the initials of the polynomials in T_{i_1} are all in k then we have $\overline{\mathbf{W}(T_{i_1})} = \mathbf{V}(T_{i_1})$. In this case we may easily check the inclusion by using the algorithm split presented in [Kal98], and remove eventually T_{i_2} from the output.This process is implemented in the domain *RegularChain* by an operation called removeSomeSuperfluousComponents. It is automatically performed in the final step of the triangular decomposition function used for our tables of results.

With this last strategy we can remove 8 components on the *Gonnet* example and 4 on *Butcher*. It happens that this technique slows down the computation as in the example systemL3 where the triangular decomposition contains 13 components. None of them is superfluous but the decomposition is performed 1.5 smaller than when we do not try to detect superfluous components with the operation removeSomeSuperfluousComponents. However we use it with every example.

Most of the computing time in the methods of Kalkbrener and Lazard is dedicated to gcd computations modulo regular chains. Moreover some of these gcd computations may be repeated. So we keep the results of these computations in hash-tables.

A last optimization of our implementation of Kalkbrener's method is the use of subresultant techniques for computing gcd modulo regular chains. This limits the growth of the coefficients.

The normalization and the computation of the square-free part of a polynomial w.r.t. a Lazard set are expensive operations. Thus an improvement of Lazard's method is to avoid these operations as much as possible. A typical situation where normalization can be avoided is the following. Assume that $T \subseteq \mathbf{P}_i$ is a Lazard set with i polynomials (thus the saturated ideal of T is zero-dimensional) and let p be a polynomial in $\mathbf{P}_i$. Recall that $\mathsf{normalize}(p, T)$ returns a list of couples (n_i, T_i) such that n_i is a normalized polynomial w.r.t. the Lazard set T_i and such that n_i and p are associated w.r.t. the t.o.s.e. associated with T_i. It follows from our assumptions that each n_i is a constant. Thus, either p is invertible w.r.t. T_i and we can set n_i to 1 or p and n_i are null. Hence, it is sufficient to check whether p is invertible w.r.t. T by a simple gcd computation without Bezout coefficients.

Another improvement of Lazard's method is to relax the square-freeness condition for Lazard sets in the intermediate computations. In fact it is sufficient to guarantee that this property holds for the normalized sets of the final decomposition. The algorithm sketched in the previous section remains correct with with this relaxation technique. However the procedure for deciding whether a $\mathbf{W}(T_{i_1})$ is contained in a $\mathbf{W}(T_{i_2})$ becomes a partial operation: in some cases the inclusion cannot be checked. Thus, some redundant computations may only be removed at the end of the computations, when square-freeness is required. Note also that the normalization procedure needs some adaptation. This relaxation technique leads to a great speed up (except for the L_3 example). This is due to the fact that in practice very few normalized sets are not square-free.

Many other tricks can be used for improving Lazard's method, especially in dimension zero. For instance, it is possible to delay the normalization condition for zero-dimensional Lazard sets until the final decomposition. This implies some adaptation of the algorithm sketched in the previous section but speeds up the computations. In positive dimension, the normalization condition cannot be delayed. This explains why Lazard's method (using these relaxation techniques) is more satisfactory in dimension zero, as we will see in the next section.

As suggested in [Laz91a], a last idea to speed up the computations of decompositions into regular chains is to generate these chains by decreasing dimension. If this is done, the superfluous sets may be removed before any computation is performed with them. Since the practical complexity of gcd computations (and thus normalizations) w.r.t. a tower of simple extensions increases with the height of this tower, some unnecessary and expensive computations can be avoided by using this dimension argument.

7.4 Results

We now present four tables of results from our experiments and study the outputs for some examples. The sources of our examples are specified in Tables 7.1 and 7.4. For every example F (which is given by a list of polynomials in $\mathbf{P}_n$) and every method which decomposes $\mathbf{V}(F)$ into triangular systems $\sigma_1, \ldots, \sigma_r$ we give two informations. The first one is the computing time (evaluation and garbage collector). It can be found in Table 7.2 for zero dimensional examples and in Table 7.5 for examples of positive dimension. If $\mathbf{V}(F)$ has dimension zero the second information is given in Table 7.3. It is a sequence $n(\sigma_1), \ldots, n(\sigma_r)$ where $n(\sigma_i)$ denotes the number of solutions of σ_i (counted with their multiplicities). For examples of positive dimension, the second information consists of a sequence $d(\sigma_1), \ldots, d(\sigma_r)$ where $d(\sigma_i)$ denotes the dimension of $\mathsf{sat}_n(\sigma_i)$. It is given in Table 7.6.

In order to make these sequences of numbers easier to read, we use some notations. Let us take the example **Z8** with Wang's method in Table 7.3. The sequence $2^2, 4, 16^2$ means that the decomposition contains two triangular sets with 16 solutions, one triangular set with 4 solutions and two triangular sets with 2 solutions. The same kind of notation applies for sequences of dimensions.

During our checking process, the empty components produced by Wu's method are automatically removed. So their number is not reported in our tables. In a similar way, the degrees given for Wu's method are obtained after removing the empty components. Note that the number of empty components depends on the heuristics and optimizations used in implementing Wu's method. So counting them does not make sense. Without using this *cleaning process* the decompositions of Wu's method are not easy to read, even for small examples. See for instance the output of the *Singular Points* example (**Z13**). Another example is the *Romin* system (**P17**): our implementation of Wu's method produces 31 components, 17 being empty and 4 being non-empty but redundant. Our implementation of Wang's method may also produce empty components. However, it happens much less frequently than with that of Wu.

We also give the timings for computing the lexicographical Gröbner bases with AXIOM and GB. To compute these bases with AXIOM we use the `groebner` operation. With GB we use the *FGLM* algorithm [FGLM93] for zero-dimensional systems and we use the *Sugar* [GMN+91] and the *Trace* [Fau94] algorithms for all the systems. We also use with GB the following strategy for computing the lexicographical Gröbner basis of some system F:

- computing a Gröbner basis for the total degree ordering
- homogenizing the obtained system
- computing the lexicographical Gröbner basis from this system
- dishomogenizing the result and reduce it since this is a Gröbner basis of F which is not generally minimal
- verifying the result with the Hilbert function (see [Tra96]).

In our tables, the column GB-DIRECT gives the best timing between the *Sugar* and the *Trace* algorithms. the colum GB gives the timing obtained with the above strategy.

The AXIOM timings for the `groebner` operation are interesting to give an idea on the efficiency of both classes of methods, based on different tools (triangular systems and Gröbner bases), but implemented within similar conditions (using the same AXIOM polynomial domain). Nevertheless remember that solving algebraic systems does not have the same meaning for those different classes of methods. One cannot extract the same information from a Gröbner basis as from a triangular decomposition.

Unfortunately, our AXIOM programs for computing triangular decompositions are probably far to be as optimized as some Gröbner bases implementations are. Thus, the ratio between AXIOM and GB timings (for computing lexicographical Gröbner bases) may inform of the eventual increase of performances that we could obtain with optimized methods and implementations. These GB timings should only be understood for this purpose. They should not be considered as references. Indeed, several efficient algorithms and tools have been developed recently in the field of Gröbner bases such as the choice of good strategies [GMN+91], new data representations or algorithms for changing monomial ordering [Fau94], [Tra96], [CKM97]. These methods generally provide a good way to compute a lexicographical Gröbner basis for our examples when a direct computation is not efficient. Some of them are used by default in some softwares for computing lexicographical Gröbner bases (MAGMA for instance).

With the method described above for computing lexicographical Gröbner bases (GB timings), we remark all the bases of our tables can be computed with GB. Note that for the examples **Z5** (*Rose*) and **P12** (*Hairer-2*) our implementations of Wang's method and Kalkbrener's method give better timings than GB. Moreover, on several relevant examples (**Z6**, **Z7**, **Z12**, **P15**, **P18**) the ratio between both is satisfactory for Kalkbrener's method. Indeed, it is well known that polynomial arithmetic can be implemented much more efficiently in C/C++ than in AXIOM.

The degree of the ideal generated by the input system F may be obtained from a Gröbner basis. We mention it in Table 7.3 (column *Gröbner basis*) for the zero-dimensional examples. The existence of multiplicities thus appears by comparing this degree with the sum of the degrees given in the column *Lazard* since the square-free triangular sets produced by Lazard's method generate radical ideals. By comparing the decompositions produced by our implementations of the methods of Lazard and Kalkbrener, we observed that the saturated ideals of the regular chains of the latter method are generally radical. Let us specify finally that the dimension of an ideal $\langle F \rangle$ is equal to the maximal dimension occuring in any of its decompositions reported in Table 7.6.

All our benchmarks have been made three times. First on a SPARC 10 station then on Pentium II PC and finally on an DEC Alpha station. The timings reported here are these obtained with this last machine (which has a EV5.6 (21164A) processor operating at 531 MHz and 512 Meg of RAM memory).

The timings are given in seconds. In the tables < 1 means that the computation finished within less than a second whereas > 1000 means that the computation was not finished after 1000 seconds. This last notation does not mean that the computation never finished. For instance our implementation of Kalkbrener's method produced an output with the **Z16** example within 1672 seconds and our implementation of Lazard's method produced an output with the **P14** example within 5160 seconds.

TAB. 7.1 –: *Zero dimensional examples*

Ex.	Source or description
Z1	Trinks 1 [BGK86] with $B < S < T < Z < P < W$.
Z2	Trinks 2 [BGK86] with $B < S < T < Z < P < W$.
Z3	Katsura 3 [BGK86] with $U3 < U2 < U1 < U0$.
Z4	Katsura4 [BGK86] with $U0 < U1 < U2 < U3 < U4$.
Z5	Rose [BGK86] with $A46 < U4 < U3$.
Z6	4 bodies problem [Kot98] $\mathcal{S}_4$ with $\phi < s < p$.
Z7	5 bodies problem [Kot98] $\mathcal{S}_5$ with $\phi < s < p$.
Z8	Caprasse [Com92] with $t < z < y < x$.
Z9	Caprasse with order $x < y < z < t$ given in [Li95].
Z10	Arnborg-Lazard [GMN+91] with $x < y < z$.
Z11	Cyclic 5 [Laz92] with $e < d < c < b < a$.
Z12	Problem 5(a) in [CG86] with $d < p < c < q$ (example 16 in [Wan93b]).
Z13	Singular Points: $F = \{f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\}$ where $f = (y-x)(y^2+x^2-1)(y^2-x)$ and $x < y$.
Z14	System $R_5 = \{x_1(x_1+1), (x_2^2+x_2+1)x_1+x_2, p_3, p_4, p_5\}$ where $p_i = x_i x_{i-1}^{i-1} + (x_i^i+1)x_{i-1} + x_i$ and $x_5 < \cdots < x_1$.
Z15	System $R_6 = \{x_1(x_1+1), (x_2^2+x_2+1)x_1+x_2, p_3, p_4, p_5, p_6\}$ with $x_6 < \cdots < x_1$.
Z16	System $R_7 = \{x_1(x_1+1), (x_2^2+x_2+1)x_1+x_2, p_3, p_4, p_5, p_6, p_7\}$ with $x_7 < \cdots < x_1$.
Z17	System $L_2 = \{x_1^2+x_2+x_3-1, x_1+x_2^2+x_3-1,\ x_1+x_2+x_3^2-1\}$ with $x_1 < x_2 < x_3$.
Z18	System $L_3 = \{x_1^3+x_2+x_3+x_4-1, x_1+x_2^3+x_3+x_4-1, x_1+x_2+x_3^3+x_4-1,$ $x_1+x_2+x_3+x_4^3-1\}$ with $x_1 < \cdots < x_4$.

TAB. 7.2 –: *Timings for zero dimensional examples*

	Wang	Wu	Kalkb.	Lazard	AXIOM	GB-DIRECT	FGLM	GB
Z1	< 1	2	< 1	1	< 1	< 1	< 1	< 1
Z2	< 1	< 1	< 1	< 1	< 1	< 1	< 1	< 1
Z3	< 1	< 1	< 1	1	< 1	< 1	< 1	< 1
Z4	3	> 1000	5	7	2	< 1	< 1	< 1
Z5	2	> 1000	3	22	> 1000	> 1000	> 1000	5
Z6	69	> 1000	51	66	> 1000	> 1000	24	3
Z7	74	> 1000	200	495	> 1000	> 1000	92	11
Z8	7	> 1000	2	2	4	< 1	< 1	< 1
Z9	4	> 1000	2	2	> 1000	< 1	< 1	< 1
Z10	5	72	3	6	300	2	< 1	< 1
Z11	> 1000	> 1000	6	6	6	< 1	< 1	< 1
Z12	> 1000	> 1000	83	197	> 1000	> 1000	17	3
Z13	< 1	1	< 1	< 1	< 1	< 1	< 1	< 1
Z14	< 1	> 1000	< 1	< 1	< 1	< 1	< 1	< 1
Z15	< 1	> 1000	5	< 1	< 1	< 1	< 1	< 1
Z16	< 1	> 1000	> 1000	< 1	2	< 1	< 1	< 1
Z17	< 1	< 1	< 1	< 1	< 1	< 1	< 1	< 1
Z18	5	> 1000	6	16	6	< 1	< 1	< 1

TAB. 7.3 –: *Degrees of outputs (zero-dimensional examples)*

	Wang	Wu	Kalkb.	Lazard	Gröbner basis
Z1	10	10	10	10	10
Z2	2	2	2	2	2
Z3	8	10	1,7	1,7	8
Z4	4,12	?	4,12	$2^2, 12$	16
Z5	132	?	4,128	4,128	136
Z6	$2^2, 39$	?	$2^2, 39$	$2^2, 39$	99
Z7	$2^2, 45$	?	$2^2, 45$	$2^2, 45$	99
Z8	$2^2, 4, 16^2$	?	$2, 6, 8, 16$	$4^2, 8, 16$	56
Z9	$2, 6, 8, 12^2$	?	$4^2, 8, 16$	$4^2, 8, 16$	56
Z10	$2, 18$	$2, 18$	$2, 18$	$2, 18$	20
Z11	?	?	$10^3, 20^2$	$10^5, 20$	70
Z12	?	?	24	24	24
Z13	4^2	$1, 3, 4$	$1, 3, 4$	$1^2, 2, 4$	8
Z14	$1, 120$	?	$1, 120$	$1, 120$	121
Z15	1,720	?	1,720	1,720	721
Z16	1,5040	?	1,5040	1,5040	5041
Z17	$2, 3$	$2, 4$	$1^3, 2$	$1^3, 2$	8
Z18	$1, 2, 6, 8, 18, 32^2$	?	$1^5, 2^4, 8, 12, 16, 32$	$1^5, 2^4, 8, 12, 16, 32$	81

Now, we focus on some of our examples. Each example is denoted by a letter and a number. The letter is **Z** or **P** and indicates if the system is zero-dimensional (**Z**) or has positive dimension (**P**). The zero-dimensional examples are can be found in table 7.1 and the corresponding results of our tests in tables 7.2 and 7.3. For the positive dimension, the examples are given in 7.4 and the results of the tests in tables 7.5 and 7.6.

Example 7.4.1 (Z8) Unfortunately our implementation of Wu's method does not succeed on this example. The methods based on gcd computations provide the best outputs and the best timings. Moreover, this example shows that these methods may provide a better way to get a triangular decomposition than a Gröbner basis computation followed by a call to the lexTriangular algorithm. Furthermore, the computation of the Gröbner basis becomes hard with the variable ordering used in example (see **Z9**).

– Wang's method :

$$
\begin{array}{rcl}
(T_1 & = & \{t^4 - 10\ t^2 + 1,\ z,\ (t^3 - 5\ t)\ y - 5\ t^2 + 1,\ x\}, \\
Q_1 & = & \emptyset), \\
(T_2 & = & \{3\ t^4 + 10\ t^2 + 3\ , \\
 & & (44289\ t^2 + 14769)\ z^4 + (-354288\ t^2 - 118080)\ z^2 + \\
 & & +708592\ t^2 + 236208, \\
 & & ((354276\ t^3 + 118044\ t)\ z^2 + 708600\ t^3 + 236232\ t)\ y + \\
 & & (-44289\ t^2 - 14769)\ z^4 + (-708588\ t^2 - 236196)\ z^2 + \\
 & & -2834360\ t^2 - 944808, \\
 & & (t^2 - 1)\ x + 2\ t\ z\ y - 2\ z\}\ , \\
Q_2 & = & [(29523\ t^2 + 9837)\ z^2 + 59050\ t^2 + 19686])\ , \\
(T_3 & = & \{t^2 + 1,\ z,\ t\ y - 1,\ x\}, \\
Q_3 & = & \emptyset)\ , \\
(T_4 & = & \{t^2 - 1,\ z^8 - 16\ z^6 + 256\ z^2 - 256,\ t\ y - 1, \\
 & & (z^3 - 8\ z)x + (-4\ t\ z^2 + 8\ t)y - 4\ z^2 + 8\}, \\
Q_4 & = & \emptyset)\ , \\
(T_5 & = & \{t^2 - 1,\ z,\ t\ y + 1,\ x\}, \\
Q_5 & = & \emptyset)\ .
\end{array}
$$

– Kalkbrener's method:

$$
\begin{array}{rcl}
C_1 & = & \{t^2 - 1,\ z^8 - 16\ z^6 + 256\ z^2 - 256,\ t\ y - 1, \\
 & & (z^3 - 8\ z)\ x + (4\ t\ z^2 + 8\ t)\ y - 12\ z^2 + 8\}\ , \\
C_2 & = & \{3\ t^4 + 10\ t^2 + 3,\ 3\ t^2\ z^2 - 14\ t^2 - 6, \\
 & & (z^2 + 5\ t^2 - 1)\ y - t\ z^2 + t^3 - 5\ t, \\
 & & (t^2 - 1)\ x + 2\ t\ z\ y - 2\ z\}\ , \\
C_3 & = & \{t^2 - 1,\ z,\ t\ y + 1,\ x\}\ , \\
C_4 & = & \{t^6 - 9\ t^4 - 9\ t^2 + 1,\ z,\ (t^3 - 5\ t)\ y - 5\ t^2 + 1,\ x\}\ .
\end{array}
$$

– Lazard's method:

$$\begin{array}{rcl} L_1 & = & \{t^2-1,\ z^8-16\ z^6+256\ z^2-256,\ y-t, \\ & & 96\ x-z^7+14\ z^5+16\ z^3-128\ z\}, \\ L_2 & = & \{3\ t^2+1,\ 3\ z^2+4,\ y+t,\ x+z\}, \\ L_3 & = & \{t^2+3,\ z^2-4,\ y+t,\ x-z\}, \\ L_4 & = & \{t^8-10\ t^6+10\ t^2-1,\ z, 24\ y-5\ t^7+49\ t^5+5\ t^3-25\ t,\ x\}. \end{array}$$

Example 7.4.2 (Z11) This classical example (cyclic 5) is not considered as a difficult one for Gröbner bases techniques. The results show the interest of methods based on gcd computations modulo towers of extension since they are the only ones which compute a triangular decomposition. Their computations are so easy as the computation of the lexicographical Gröbner basis with AXIOM, and they detect more splits than lexTriangular. Some coefficients in the output obtained with Kalkbrener's method are bigger than the coefficients in the output of Lazard's method and lexTriangular. This difference is due to the fact the latter methods produce normalized triangular sets whereas Kalkbrener's method does not. For $n > 5$ it is much more difficult to obtain a direct triangular decomposition for the cyclic-n system than computing a lexicographical Gröbner basis.

Example 7.4.3 (Z13) Here the methods give different results and we can note that Lazard's decomposition is more legible than the others. One can check that $\mathbf{W}(W_2) = \mathbf{W}(C_3)$ and $\mathbf{W}(W_3) = \mathbf{W}(C_1)$.

– Wang's method:

$$\begin{array}{rcl} (T_1 & = & \{x^2+x-1,\ x\ y^2+x-1\}, \\ Q_1 & = & \emptyset), \\ (T_2 & = & \{2\ x^4-2\ x^3-x^2+x, \\ & & (46\ x^5+48\ x^4-64\ x^3-24\ x^2+18\ x+2)\ y+ \\ & & -48\ x^5-51\ x^4+70\ x^3+28\ x^2-25\ x\}, \\ Q_2 & = & \emptyset), \end{array}$$

– Wu's method:

$$\begin{array}{rcl} W_1 & = & \{x^2+x-1,\ (86\ x-53)\ y^2+139\ x-86\}, \\ W_2 & = & \{2\ x^4+x^3-3\ x^2+x, \\ & & (208\ x^3+104\ x^2-312\ x+104)\ y+ \\ & & 11960\ x^9-5660\ x^8-20990\ x^7+26143\ x^6+ \\ & & -9968\ x^5-990\ x^4+1601\ x^3-218\ x^2-36\ x\}, \\ W_3 & = & \{4\ x^7-2\ x^6-10\ x^5+9\ x^4+2\ x^3-4\ x^2+x, \\ & & (66\ x^6+29\ x^5-131\ x^4+24\ x^3+43\ x^2-15\ x)\ y+ \\ & & -64\ x^{10}-76\ x^9+142\ x^8+96\ x^7+ \\ & & -124\ x^6-21\ x^5+32\ x^4+2\ x^3-3\ x^2\}. \end{array}$$

TAB. 7.4 –: *Positive dimensional examples*

Ex.	Source or description
P1	Donati-Traverso [DT89].
P2	Alonso [Com92]: $\{(u-r-2)\,x-u-2\,t^4+1,\ r\,y-t^2\,u-1,\ t\,u\,z-1,\ v-t\,r\}$ with $t<r<u<v<z<y<x$.
P3	Alonso with order $v<z<y<x<t<u<r$ given in [Li95].
P4	Wang's example in [Wan92a].
P5	Wu's example in [Wan92a].
P6	ex. 4 in [Wu86] and ex. 2 in [Wan93b], with $x10<\ldots<x13<x21<x22<x23<x30<x101<\ldots<x105$.
P7	[Bro86] p.248 (right-middle) with $a<b<y<x$ and example 12 in [Wan93b].
P8	Gerdt [BGK86] with $L1<L2<\ldots<L7$.
P9	Gonnet [BGK86] with $A0<A2\ldots<A5<B0\ldots<B5<C0\ldots<C5$.
P10	Butcher [BGK86] with $B<C2<C3<A<B3<B2<A32<B1$.
P11	Hairer1 [BGK86]
P12	Hairer2 [BGK86] with $A43>A42>A41>A32>A31>A21>B1>B2>B3>B4>C4>C3>C2$.
P13	Vermeer (example 2 p.110 in [Wan93b]).
P14	Neural Network [Kal91].
P15	Liu [Liu89] with order $a<t<z<y<x$.
P16	Liu with $a<x<y<z<t$ as in [Li95].
P17	Robot Romin [GR91] $\{-d\,s_1-a, d\,c_1-b, l_2\,c_2+l_3\,c_3-d, 2\,s_2+l_3\,s_3-c, s_1^2+c_1^2-1, s_2^2+c_2^2-1, s_3^2+c_3^2-1\}$ with $d<c<b<a<l_3<l_2<c_3<s_3<c_2<s_2<c_1<s_1$.
P18	f633 [FdSMR96] $\{2u_6+2u_5+2u_4+2u_3+2u_2+1, 2U_6+2U_5+2U_4+2U_3+2U_2+1,$ $(8u_6+8u_5)\,U_5+(8u_6+8u_5+8u_4)\,U_4+(8u_6+8u_5+8u_4+8u_3)\,U_3+$ $(8u_6+8u_5+8u_4+8u_3+8u_2)\,U_2-13,$ $(8u_5+8u_4+8u_3+8u_2)\,U_6+(8u_5+8u_4+8u_3+8u_2)\,U_5+$ $(8u_4+8u_3+8u_2)\,U_4+(8u_3+8u_2)\,U_3+8u_2U_2-13,$ $u_2U_2-1, u_3U_3-1, u_4U_4-1, u_5U_5-1, u_6U_6-1\}$ with $u_2<u_3<u_4<u_5<u_6<U_2<U_3<U_4<U_5<U_6$.
P19	The $(8,3)$ configuration as in [Li95].

TAB. 7.5 –: *Timings for positive dimensional examples*

	Wang	Wu	Kalkb.	Lazard	AXIOM	GB-DIRECT	GB
P1	< 1	1	1	< 1	3	< 1	< 1
P2	< 1	< 1	< 1	< 1	< 1	< 1	< 1
P3	9	> 1000	6	> 1000	1	< 1	< 1
P4	1	4	2	4	1	< 1	< 1
P5	< 1	< 1	< 1	1	< 1	< 1	< 1
P6	4	53	51	177	9	< 1	< 1
P7	3	10	< 1	2	< 1	< 1	< 1
P8	2	16	5	3	3	< 1	< 1
P9	1	3	< 1	1	< 1	< 1	< 1
P10	4	4	2	2	85	9	< 1
P11	< 1	< 1	< 1	< 1	< 1	< 1	< 1
P12	4	> 1000	7	74	> 1000	136	39
P13	> 1000	> 1000	8	> 1000	> 1000	> 1000	< 1
P14	> 1000	> 1000	8	> 1000	8	< 1	< 1
P15	48	> 1000	61	> 1000	> 1000	> 1000	3
P16	49	> 1000	119	> 1000	> 1000	> 1000	1
P17	2	8	9	8	2	< 1	< 1
P18	3	32	2	50	12	< 1	2
P19	122	> 1000	702	> 1000	> 1000	> 1000	112

TAB. 7.6 –: *Dimensions for positive dimensional examples*

	Wang	Wu	Kalkbrener	Lazard
P1	$0^2, 1$	$0^2, 1$	1	$0^2, 1$
P2	$2^2, 3$	$2^2, 3$	3	$2^2, 3$
P3	$1^7, 2^3, 3$	?	3	?
P4	1^3	1^4	1^3	1^4
P5	01	$0^5 1$	1	$0^5, 1$
P6	$1^4, 2$	$1^5, 2$	$1^8, 2$	$1^4, 2$
P7	$1^9, 2^2$	$1^5, 2^2$	$1, 2^2$	$1, 2^2$
P8	$1^2, 2^3, 3$	$1^7 2^5, 3$	$1^3, 2^3, 3$	$1^2, 2^3, 3$
P9	3^3	3^3	3^3	3^3
P10	$0, 2^2, 3^4$	$0, 2^5, 3^3$	$0, 2^2, 3^3$	$0, 2^2, 3^3$
P11	$1^2, 2^3$	$1^4, 2^3$	2^3	$1^2, 2^3$
P12	$1^3, 2$	?	2	$1^3, 2$
P13	?	?	$1, 1$	?
P14	?	?	1^2	$1^2, 0^{16}$
P15	$0^9, 1$	?	1	?
P16	$0^6, 1$	?	1	?
P17	$3^5, 4^5, 5$	$3^6, 4^5, 5$	5	$3^4, 4^5, 5$
P18	$1^3, 2$	$0^3, 1^{10}, 2$	2	$0, 1^4, 2$
P19	# 331	?	$7, 5^{16}$	?

– Kalkbrener's method:

$$
\begin{aligned}
C_1 &= \{x^2 + x - 1,\ (86\ x - 53)\ y^2 + 139\ x - 86\}\,, \\
C_2 &= \{2\ x^3 - 2\ x^2 - x + 1,\ (102\ x^2 - 39\ x - 23)\ y - 63\ x^2 - 28\ x + 51\}\,, \\
C_3 &= \{x,\ y\}\,.
\end{aligned}
$$

– Lazard's method:

$$
\begin{aligned}
L_1 &= \{2\ x^2 - 1,\ y - x\}\,, \\
L_2 &= \{x^2 + x - 1,\ y^2 - x\}\,, \\
L_3 &= \{x,\ y\}\,, \\
L_4 &= \{x - 1,\ y - 1\}\,.
\end{aligned}
$$

Example 7.4.4 (Z14,Z15,Z16) All methods produce the same output (which can be computed by hand from the input system) but our implementation of Kalkbrener's method is inefficient in this particular example. This follows from the sense of reduction that we use for our regular chains. A polynomial in a regular chain T is reduced only w.r.t. the other polynomials in T whose initials are in the base field k. In many cases the outputs are more legible with this choice and the timings are not significally different. But for this particular systems the full reduction (as it is used in Lazard's method and lexTriangular) simplifies a lot the intermediate triangular sets and thus speeds up the gcd computations. If we choose a full reduction in our implementation of Kalkbrener's method then the example **Z16** is performed within less than a second.

Example 7.4.5 (P1) This classical example of Donati and Traverso shows that the computation of a lexicographical Gröbner basis is not always very interesting. The timing with AXIOM is bigger than those obtained by our triangular decompositions. With GB the result is not obtained with the *Trace* algorithm. Finally the Gröbner basis is much bigger than the outputs of the triangular decompositions.

Example 7.4.6 (P2) Alonso's example corresponds to a prime ideal of dimension 3. Kalkbrener method describes it with only one regular chain C_1. The other algorithms extract points which are in the closure of the regular zeros of C and provide similar results.

– Wu's method:

$$
\begin{aligned}
W_1 &= \{r,\ t^2\ u + 1,\ v - t\ r,\ t\ z + t^2,\ (2\ t^2 + 1)\ x + t^2\ u + 2\ t^6 - t^2\}\,, \\
W_2 &= \{r + 2\ t^4 + 1,\ u - r - 2,\ v - t\ r, \\
&\qquad (2\ t^5 - t)\ z + 1,\ (2\ t^4 + 1)\ y + t^2\ u + 1\}\,, \\
W_3 &= \{v - t\ r,\ t\ u\ z - 1,\ r\ y - t^2\ u - 1(u - r - 2)\ x - u - 2\ t^4 + 1\}\,.
\end{aligned}
$$

– Wang's method:

$$
\begin{aligned}
(T_1 &= \{v - t\ r,\ t\ u\ z - 1,\ r\ y - t^2\ u - 1,\ (u - r - 2)\ x - u - 2\ t^4 + 1\}\,, \\
Q_1 &= [u,\ r,\ t,\ u - r - 2])\,, \\
(T_2 &= \{r,\ t^2\ u + 1,\ v,\ z + t,\ (2\ t^2 + 1)\ x + t^2\ u + 2\ t^6 - t^2\}\,, \\
Q_2 &= [2\ t^2 + 1,\ t])\,, \\
(T_3 &= \{r + 2\ t^4 + 1,\ u + 2\ t^4 - 1,\ v + 2\ t^5 + t,\ (2\ t^5 - t)\ z + 1 \\
&\qquad (2\ t^4 + 1)\ y - 2\ t^6 + t^2 + 1\}\,, \\
Q_3 &= [2\ t^4 + 1,\ 2\ t^4 - 1,\ t])\,.
\end{aligned}
$$

– Kalkbrener's method:

$$C_1 = \{v - t\ r,\ t\ u\ z - 1,\ r\ y - t^2\ u - 1,\ (u - r - 2)\ x - u - 2\ t^4 + 1\}.$$

– Lazard's method:

$$\begin{aligned} L_1 &= \{v - t\ r,\ t\ u\ z - 1,\ r\ y - t^2\ u - 1,\ (u - r - 2)\ x - u - 2\ t^4 + 1\}, \\ L_2 &= \{r + 2\ t^4 + 1,\ u + 2\ t^4 - 1,\ v + 2\ t^5 + t,\ (2\ t^5 - t)\ z + 1, \\ &\quad (2\ t^4 + 1)\ y - 2\ t^6 + t^2 + 1\}, \\ L_3 &= \{r,\ t^2\ u + 1,\ v,\ z + t,\ (2\ t^2 + 1)\ x + 2\ t^6 - t^2 - 1\}. \end{aligned}$$

Example 7.4.7 (P3) This is the same polynomial system as in **P2**. A comparison with the results of **P2** shows how the order of variables may dramatically augment the computing time of triangular decompositions. While it is easy to obtain a decomposition with the order of **P2** for all the methods (see above), only Wang's and Kalkbrener's methods can provide a solution for **P3**. It seems with the outputs of Wang's method that the methods which decompose into regular zeros have more cases to examine than in **P2**. On the contrary, Kalkbrener's method still gives a unique output. This is surely due to the criterion on the height of the saturated ideals of a regular chain that we implemented in this method (see Section 7.3).

Example 7.4.8 (P14) Only the methods based on gcd computations over towers of simple extensions succeed with this example. The decomposition computed by our implementations of Kalkbrener's method is much more compact than the lexicographical Gröbner basis and it is obtained within the same time. It produces two regular chains corresponding to saturated ideals of dimension one which are given below. The decomposition computed by our implementations of Lazard's method produce 18 regular chains, two of them corresponding to components of dimension one and the others to zero-dimensional components. The use of normalization and full reduction in this method dramatically breaks down the intermediate computations with this example.

– $\{4az^7 - 4z^6 - 4a^2z^5 + (a^3 - 4)z^3 + a^2z^2 - az - 1,$
$(6az^7 - 6z^6 - 7a^2z^5 + 2az^4 + (2a^3 + 1)z^3 + a^2z^2 - 2az - 1)y + 4az^5 - 4z^4 - 3a^2z^3$
$+2az^2 + z,$
$(y^2 + z^2 - a)x + 1\}$

– $\{2z^7 - 5az^5 - z^4 + 4a^2z^3 + 2az^2 + (-a^3 - 1)z - a^2,$
$(8az^6 + (-2a^3 - 20)z^5 - 18a^2z^4 + (4a^4 + 28a)z^3 + (12a^3 - 4)z^2 + (-2a^5 - 6a^2)z - 2a^4)$
$y^2 + (-8z^6 + 4a^2z^5 + 20az^4 + (-8a^3 - 16)z^3 - 16a^2z^2 + (4a^4 + 4a)z + 4a^3)y - 6a^2z^6$
$+(a^4 + 2a)z^5 + (13a^3 - 14)z^4 + (-2a^5 - 2a^2)z^3 + (-8a^4 + 28a)z^2 + (a^6 - a^3 - 10)z$
$+a^5 - 10a^2,$
$(y^2 + z^2 - a)x + 1\}$

Example 7.4.9 (P19) This example illustrates that solving in the sense of the regular zeros (as in the methods of Wu, Wang and Lazard) is sometimes much harder than solving in the sense of the Zariski closure (as in Kalkbrener's method). Our implementation of Wang's method succeeds with this example but produces 331 triangular systems whereas our decomposition into regular chains is much more compact and legible.

7.5 Some other implementations

The main purpose of our work is a comparison within a same implementation of four methods of triangulation based on pseudo division. We explained this point in Section 7.3. However the problem of solving systems of polynomials has been already studied by different approaches. The implementations may involve techniques like factorization and Gröbner basis computations that we do not use, or different data structures. In this section, we take into account some experimental results already published and try to compare them with our work.

lexTriangular: In [MR95], the authors report an efficient implementation in AXIOM of the algorithm *Lextriangular* presented in [Laz92]. The main tool of this algorithm is a theorem by [Gia87] and [Kal87] which exploits the properties of Gröbner bases in the zero-dimensional case. *Lextriangular* computes decompositions into Lazard sets (see Definition 7.2.13), but it works only under the restriction that the input is a lexicographical Gröbner basis of a zero-dimensional ideal.

The four methods of our implementation work with any input. Therefore they do not exploit the properties of a particular case to avoid some branches of computations. Thus, when the input is a zero-dimensional Gröbner basis, it is clear that they cannot be as efficient as *Lextriangular* to compute a triangular decomposition. But remark that in some case, a triangular decomposition may be computed faster by running some of the four methods than computing directly the lexicographical Gröbner basis and apply *Lextriangular*.

Möller, Gräbe: In [Möl93] is presented another algorithm which decomposes zero dimensional varieties from Gröbner bases. It involves lexicographical Gröbner bases computations of quotients which are generally costly. This approach has been improved and extended to positive dimension in [Grä95], which reports an implementation in REDUCE.

The algorithms presented in [Grä95] involve factorized Gröbner bases and reduction to dimension zero. Several zero dimensional examples are given. The variant ZS2 for decomposing zero dimensional varieties seems the most interesting. It uses as much as possible the degrevlex order for computing Gröbner bases. This allows to decompose the example *katsura5* which is not computed by our implementations. The other timings for this variant have the same order as our implementation of Kalkbrener's method running on a SPARC 10 station (it is difficult to be more acute since the material conditions are different). But it would have been interesting to see more various examples (three of the five examples are *katsura* which split only on the univariate polynomial of the Gröbner base).

Some positive dimensional examples in [Grä95] appear in our tables (**P1**, **P9**, **P11**). It seems that they are decomposed slower with the different variants in [Grä95] than with our implementations of the methods of Kalkbrener, Lazard and Wang on a SPARC 10 station.

Dynamic evaluation: This method involves particular data-structures like the dynamic sets and dynamic polynomials [Gom92]. Therefore it could not enter within our comparative implementation. However we tested our examples with the implementation available in AXIOM. This was performed under the same material conditions as our experiments with the methods of Wu, Wang, Kalkbrener and Lazard. Our results show that dynamic evaluation cannot actually compare with our implementations to compute triangular decompositions of systems. The computations performed with dynamic evaluation are generally one or two order slower when they terminate. But note that dynamic evaluation is designed to deal with more general subjects than polynomial system solving.

D. Wang : [Wan96] reports experiments with the methods of Wu and Wang. It concludes that the different variants of Wu method which are studied are less efficient than the method developped by Wang. These implementations do not use the notion of reduction (w.r.t. the iterated initials) that we employ in our implementation. Our results hence complete the comparison of [Wan96] and confirm that the decomposition into fine triangular systems proposed by Wang is more efficient than the characteristic set method of Wu.

On the contrary of our implementation Wang uses factorization. Many of our examples are in the tables given by [Wan96]. But the experimental conditions are different and it seems difficult to compare the efficiency of our implementation with the results of [Wan96].

Ziming Li : In [Li95] is reported an efficient implementation of the characteristic set method of Wu, based on SACLIB 1.2, which involves factorization, subresultant techniques and modular algorithms. Li remarked that it is a difficult task to verify the correctness of the triangular decompositions. We think that the tools that we have implemented for this purpose are useful.

We don't find any information about the outputs of the examples given in [Li95] but we can take into account the timings since the computations are done with the same first machine as our examples (SPARC 10 station). Li computes the example **P1** slower than our implementations. Example **Z11** is decomposed slower than by our implementations of the methods of Kalkbrener or Lazard. Example **P16** is not computed while our implementations of the methods of Wang or Kalkbrener are able to compute a triangulation. But Li decomposes efficiently the examples **P3** and **P13**. He also succeed in computing a decomposition of cyclic6 that we do not compute.

7.6 Conclusions

Our conclusions are highly influenced by the way that we have implemented these four methods, even if we have tried to limit the differences which are due only to the implementation.

For easy examples, we remark that all methods generally have good computing times and that the legibility of the outputs that they produce is satisfactory. Nevertheless Wu's method fails in some rather easy zero-dimensional examples (**Z8**, **Z14**) and for both cases of dimension zero and positive dimension, this method clearly solves less problems than the other methods. Moreover, for the most difficult examples that Wu's method can solve, the outputs are hard to read (see **P17**). In our opinion, the reason is the following. Wu's method cannot split the computations (in order to obtain several triangular sets) before computing a characteristic set of F (which is sometimes hard to compute, especially for zero-dimensional problems) whereas the other methods may split their computations earlier. More generally, it seems that methods based on gcd computations over tower of simple extensions, namely those of Lazard and Kalkbrener, may discover factorizations that other methods cannot find (**Z11**).

Let us now concentrate on Wang's method. This method may be very efficient for difficult examples. Indeed, it has the best timings for the examples **Z7**, **P15**, **P16** and**P19**. However the decompositions that it produces are generally less legible than the ones of Kalkbrener and Lazard. Furthermore, as Wu's method, the method of Wang is disappointing in some easy examples, namely **Z11** and **P14**.

Kalkbrener's method is the only method which solves every example and often produces the most concise outputs (except for **Z11**). Moreover, some examples (**P13**, **P14**) can only be processed by this method. But one has to keep in mind that this method solves polynomial systems in a *more lazy way* than the other three. Our strategy for this method is also inefficient for some zero-dimensional examples (**Z16**) whereas Lazard and Wang's method succeeds with these examples. In some cases the gcd computations of this method may be simplified a lot when a strong reduction is used. We think that the use of normalized triangular sets in Lazard's method is generally a good way to solve zero-dimensional problems. This may replace big algebraic expressions by a single integer in zero-dimensional examples.

However, normalization and square-free factorization over tower of separable extensions may be time consuming in Lazard's method (**P14**). For describing affine varieties by means of regular zeros of triangular sets, this method gives the best output. Moreover, this is the only method which produces decompositions without redundant components.

We think that the methods based on gcd computations over towers of extensions are promising. The experiments show that they must be investigated further for more efficiency. For problems of positive dimension, it appears that solving in the sense of the Zariski closure as Kalkbrener's method may be a good way to obtain a decomposition for the most difficult ones. Such a decomposition may be sufficient for further uses. Decomposing in the sense of the regular zeros as Lazard's method needs more work in positive dimension and the gcd computations which sometimes may be prohibitive. We finally remark that for solving in the sense of the regular zeros, Wang's method is a powerful tool in some hard examples.

Chapitre 8

Quelques applications

Résumé

Nous présentons quelques applications de nos implantations. Nous montrons d'abord que les outils que nous avons développés s'appliquent efficacement en théorie de Galois pour calculer les ensembles triangulaires normalisés séparables qui engendrent des idéaux de Galois (voir le chapitre 6), en particulier l'idéal des relations entre les racines d'un polynôme donné. Nous donnons des exemples de calcul pour des polynômes de degrés 7 et 8. Pour calculer ces bases de Gröbner triangulaires, nous obtenons en général des performances au moins comparables à celles de logiciels réputés pour le calcul de bases de Gröbner tels que MAGMA et GB. Ces calculs n'étaient pas réalisables avec la méthode originale de Kalkbrener qui utilise des chaînes régulières générales. Il faut absolument travailler dans ce domaine avec des ensembles triangulaires normalisés pour obtenir un résultat, ce qui montre l'intérêt de la notion de normalisation de [Laz91a] et de notre algorithme de la section 5.3. De plus, nous avons construit pour les idéaux de Galois un domaine AXIOM d'ensembles triangulaires qui tient compte des spécificités de ces idéaux et entraîne une meilleure efficacité.

D'autre part, avec des optimisations récentes, nous parvenons à une meilleure efficacité. C'est ainsi que les temps de calcul de certains exemples donnés dans le chapitre 7 sont améliorés. La décomposition d'une variété en clôtures de zéros réguliers d'ensembles triangulaires réguliers peut ainsi être utilisée pour s'attaquer à des problèmes *intéressants*. Nous présentons par exemple un problème réel traitant de la compression d'images par une méthode exposée dans [FdSMR96]. On peut calculer directement une décomposition triangulaire du système de départ dans certains cas, même s'il est encore nécessaire de le résoudre en partant d'une base de Gröbner pour des systèmes plus gros. Nous avons aussi utilisé nos méthodes avec succès pour la résolution de problèmes en mécanique céleste étudiés par I. Kotsireas ([Kot98]. On obtient une solution complète pour des systèmes de dimension zéro qui permet immédiatement une exploitation numérique en un temps proche de celui du calcul d'une base de Gröbner avec le logiciel GB.

8.1 Corps de décomposition d'un polynôme

Nous avons constaté expérimentalement que nos algorithmes de décomposition triangulaire sont un moyen efficace pour résoudre des systèmes en théorie de Galois algébrique. Nous nous intéressons dans cette section au problème bien connu de la détermination de l'idéal des relations entre les racines d'un polynôme séparable f de $k[X]$, ou plus généralement d'un idéal de Galois de f (voir les définitions 6.2.1 et 6.2.2).

Rappelons notre résultat de structure du théorème 6.5.4 : un idéal de Galois I d'un polynôme $f \in k[X]$ de degré n est engendré par un ensemble triangulaire normalisé séparable de $\mathbf{P}_n$. Rappelons aussi qu'un tel ensemble est une base de Gröbner lexicographique de I (voir la proposition 4 p. 103 de [CLO92]). On sait ainsi qu'une base de Gröbner de I pourra être facilement construite à partir d'une décomposition triangulaire de I par restes chinois. Dans le cas où I est un idéal de relations, alors I est maximal. Puisque sa variété associée est irréductible, toute méthode qui décompose un système quelconque de générateurs de I en ensembles triangulaires normalisés fournit donc la base de Gröbner lexicographique minimale de I (à un coefficient du corps de base près).

Lorsque nous parlerons de décomposition triangulaire dans cette section, ce sera une décomposition en ensembles triangulaires normalisés et séparables. Rappelons que les idéaux sont tous de dimension zéro pour ces problèmes.

A partir de nos algorithmes permettant de décomposer le radical d'un idéal en ensembles triangulaires normalisés séparables, nous avons construit un nouveau domaine AXIOM d'ensemble triangulaires appelé GaloisIdeal qui prend en compte les spécificités des idéaux de Galois pour plus d'efficacité. Jusqu'à maintenant nous n'avons pu tester ce domaine qu'à partir de quelques exemples de calcul d'idéaux de Galois que nous a fournis L. Ducos (Université de Poitiers). Nous n'avons pas eu le temps d'en construire d'autres nous-même. Il s'agissait d'en calculer la base de Gröbner lexicographique (triangulaire) à partir des modules de Cauchy d'un polynôme donné et de plusieurs évaluations de facteurs de résolvantes. Le groupe de Galois est dans ce type de problème connu d'avance. L'objectif est généralement d'aboutir à calculer le corps de décomposition du polynôme pour envisager le calcul sur ce corps. Remarquons à ce sujet que les algorithmes que nous avons présentés permettent justement de calculer sur un tel corps de décomposition. C'est même un cas bien particulier puisqu'on sait qu'aucun scindage n'est possible. À partir de notre domaine GaloisIdeal on obtient donc immédiatement en spécialisant notre algorithme split, un domaine dont les éléments sont des ensembles triangulaires réguliers qui engendrent un idéal maximal de dimension zéro.

Les bases de Gröbner lexicographiques des exemples traités ne se calculent pas facilement. Leur structure triangulaire pourrait laisser penser qu'il vaut mieux les calculer directement pour l'ordre lexicographique. En fait, on n'arrive à aucun résultat ainsi avec des logiciels performants tels que GB et MAGMA. Il vaut mieux laisser MAGMA faire appel à sa stratégie implantée par défaut, où interviennent homogénéisation, calcul d'une base pour l'ordre du degré et changement d'ordre (algorithme du Gröbner Walk [CKM97]). De manière similaire, les résultats les plus probants ont été obtenus sur GB avec la stratégie décrite dans la section 7.4 page 118. Les temps de calcul présentés dans cette partie ont été obtenus sur la machine anne de l'UMS MEDICIS (Dec Alpha EV56, 400 Mhz).

Considérons l'exemple le plus facile à résoudre pour notre implantation. Le but est de calculer l'idéal I des relations entre les racines du polynôme

$$f_1 = X^7 - 7X + 1 .$$

Les degrés des polynômes de la base de Gröbner triangulaire T de l'idéal I peuvent être connus à l'avance (voir le théorème 6.5.4). Pour cet exemple, ils sont donnés par la liste $[7, 6, 1, 4, 1, 1, 1]$, en suivant l'ordre croissant des polynômes de T.

Puisque l'idéal cherché est un idéal maximal, il est clair qu'une décomposition triangulaire du système de départ ne fournira qu'un seul ensemble triangulaire en sortie. Puisque notre implantation calcule des ensembles triangulaires normalisés séparables nous obtenons une base de Gröbner de l'idéal I. Les résultats sont ainsi immédiatement vérifiables.

Notre implantation réalise le calcul de la base de Gröbner de I en 270 secondes alors qu'il faut 430 secondes au logiciel MAGMA. Le choix d'une Dec Alpha pour réaliser nos tests nous permet de disposer de résultats significatifs pour notre comparaison d'efficacité avec MAGMA puisque son implantation est mieux optimisée pour ce type de machine que pour les PC. Le calcul avec GB prend 1480 secondes avec la stratégie de la section 7.4. Nous avions essayé auparavant de calculer les bases directement pour les ordres lexicographiques et du degré sans y arriver en un temps raisonnable.

La série d'exemples suivants concerne le calcul d'idéaux de Galois associés au polynôme f_2 de degré 7 suivant :

$$f_2 = X^7 + X^6 - 12X^5 - 7X^4 + 28X^3 + 14X^2 - 9X + 1 .$$

Nous donnons les temps de calcul en secondes dans le tableau ci-dessous. Deux des idéaux à déterminer ne sont pas maximaux; dans ces deux cas le système ne se décompose pourtant pas en plusieurs ensembles triangulaires avec notre implantation, et nous obtenons là encore la base de Gröbner lexicographique G comme unique sortie. On remarquera que le système qui n'admet aucun zéro est pourtant le plus long à calculer.

degrés des polynômes de G	Dec. Triangulaire	MAGMA
$[7, 6, 1, 4, 1, 1, 1]$	2630	2450
$[7, 2, 1, 1, 1, 1, 1]$	3490	4190
$I = \mathbf{P}_7$	3620	4730
$[7, 1, 1, 1, 1, 1, 1]$ (idéal des relations)	2340	1040

Le dernier exemple est de degré 8. Il s'agit de calculer l'idéal des relations du polynôme

$$f_3 = X^8 - 8X^7 + 28X^6 - 54X^5 + 71X^4 - 58X^3 + 30X^2 - 10X + 3 .$$

Les degrés des polynômes de la base de Gröbner triangulaire sont donnés par la liste $[8, 1, 6, 4, 1, 2, 1]$. Alors que le calcul de la base de Gröbner nécessite 74400 secondes sur MAGMA et que nous n'avons pas obtenu de réponse après plus de 2 jours de calcul sur GB, notre implantation détermine cette base en 220 secondes seulement.

8.2 Compression d'images

Dans [FdSMR96] est présentée une méthode de compression d'images par bancs de filtres à l'aide de méthodes symboliques. Après tout un travail de mise en équations du problème, on aboutit à un système polynomial qu'il s'agit de résoudre. Pour finir, il faut déterminer la dimension du système et l'existence de racines réelles.

Ce problème a généré plusieurs systèmes de dimension positive. Les bases de Gröbner correspondantes ont été calculées avec GB. L'utilisation de méthodes de décomposition triangulaire sur la base de Gröbner permet de passer à l'exploitation numérique des résultats. Notons qu'il est possible pour les cas les plus accessibles de calculer directement (sans passer par le calcul de base de Gröbner) une décomposition triangulaire en saturés à l'aide de nos implantations. C'est ainsi que nous obtenons pour le premier système, nommé *f633*, un résultat en 2 secondes sur un Alpha 550 Mhz (exemple **P13** du chapitre 7). Les zéros du système peuvent être représentés par l'unique ensemble triangulaire régulier séparable T ci-dessous dont le saturé est un idéal premier de dimension 2 sur le corps des complexes.

$$
\begin{aligned}
T \;=\; & \{((20\,u_2{}^2+56\,u_2+32)\,u_3{}^2+(32\,u_2{}^3+120\,u_2{}^2+64\,u_2)\,u_3+64\,u_2{}^3+32\,u_2{}^2)\,u_4{}^2\\
& +((52\,u_2{}^2+120\,u_2+32)\,u_3{}^3+(84\,u_2{}^3+201\,u_2{}^2+84\,u_2)\,u_3{}^2\\
& +(32\,u_2{}^4+120\,u_2{}^3+52\,u_2{}^2)\,u_3)u_4+(32\,u2^2+64\,u_2)\,u_3{}^4\\
& +(64\,u_2{}^3+120\,u_2{}^2+32\,u_2)\,u_3{}^3+(32\,u_2{}^4+56\,u_2{}^3+20\,u_2{}^2)\,u_3{}^2,\\
& (((4\,u_2+8)\,u_3+8\,u_2)\,u_4+8\,u_2\,u_3)\,u_5+((4\,u_2+8)\,u_3+8\,u_2)\,u_4{}^2\\
& +((4\,u_2+8)\,u_3{}^2+(4\,u_2{}^2+13\,u_2)\,u_3)\,u_4,\ 2\,u_6+2\,u_5+2\,u_4+2\,u_3+2\,u_2+1,\\
& u_2\,U_2-1,\ u_3\,U_3-1,\ u_4\,U_4-1,\\
& (8\,u_4+8\,u_3+8\,u_2+4)\,U_5+(8\,u_3+8\,u_2+4)\,U_4+(8\,u_2+4)\,U_3+4\,U_2+13,\\
& 2\,U_6+2\,U_5+2\,U_4+2\,U_3+2\,U_2+1\}
\end{aligned}
$$

A partir du second système (*f744*) ci-dessous

$$
\left\{
\begin{array}{l}
2\,u_7+2\,u_6+2\,u_5+2\,u_4+2\,u_3+2\,u_2+1,\\
2\,U_7+2\,U_6+2\,U_5+2\,U_4+2\,U_3+2\,U_2+1,\\
(8\,u_7+8\,u_6)\,U_6+(8\,u_7+8\,u_6+8\,u_5)\,U_5+(8\,u_7+8\,u_6+8\,u_5+8\,u_4)\,U_4+\\
(8\,u_7+8\,u_6+8\,u_5+8\,u_4+8\,u_3)\,U_3+(8\,u_7+8\,u_6+8\,u_5+8\,u_4+8\,u_3+8\,u_2)\,U_2-17,\\
(8\,u_6+8\,u_5+8\,u_4+8\,u_3+8\,u_2)\,U_7+(8\,u_6+8\,u_5+8\,u_4+8\,u_3+8\,u_2)\,U_6+\\
(8\,u_5+8\,u_4+8\,u_3+8\,u_2)\,U_5+(8\,u_4+8\,u_3+8\,u_2)\,U_4+(8\,u_3+8\,u_2)\,U_3+8\,u_2\,U_2-17,\\
(16\,u_4\,U_3+(16\,u_4+16\,u_3)\,U_2+8\,u_4+8\,u_3+8\,u_2+18)\,U_5\\
+(16\,u_3\,U_2+8\,u_3+8\,u_2+18)\,U_4+(8\,u_2+18)\,U_3+18\,U_2+11,\\
(16\,u_3+16\,u_2+8)\,u_5\,U_4+((16\,u_2+8)\,u_5+(16\,u_2+8)\,u_4)\,U_3+(8\,u_5+8\,u_4+8\,u_3)\,U_2+\\
18\,u_5+18\,u_4+18\,u_3+18\,u_2+11,\\
u_2\,U_2-1, u_3\,U_3-1, u_4\,U_4-1, u_5\,U_5-1, u_6\,U_6-1, u_7\,U_7-1
\end{array}
\right.
$$

notre implantation calcule directement un unique ensemble triangulaire dont le saturé est de dimension 1, mais le temps de calcul monte à 500 secondes environ.

8.3 Problème des n-corps

On considère n particules de masses égales dans un espace euclidien de dimension $n-2$ soumis à un champ de potentiel newtonien (correspondant aux lois de gravitation). Lorsque les n corps forment une *configuration centrale*, c'est-à-dire quand la configuration des n-corps reste constante au cours du temps, on cherche à déterminer les distances mutuelles entre les particules.

L'étude du cas des configurations centrales est important car exploitable pour l'analyse de configurations de corps célestes ou des orbites de collision des systèmes gravitationnels en expansion. De nombreux auteurs se sont donc intéressés à ce problème. Les travaux de O. Dziobeck, A. Albouy et A. Chenciner se basent sur l'utilisation des distances mutuelles des corps. Dans cette optique, I. Kotsireas a récemment étudié le problème à l'aide de diverses méthodes symboliques. Nos implantations permettent de résoudre certains problèmes qu'il a traité et que nous résumons ci-dessous. Pour une vision complète de ces problèmes, nous invitons le lecteur à se référer à [Kot98].

Pour $n=4$, A. Albouy a montré que toute configuration centrale pour des masses égales admet au moins une symétrie (voir [Alb96]). Avec cette hypothèse, le travail d'I. Kotsireas permet de reformuler le système de polynômes de 6 équations à 6 inconnues qui modélise le problème. Il obtient alors le système $\mathcal{S}_4$ ci-dessous à 3 inconnues :

$$\mathcal{S}_4 \left\{ \begin{array}{l} -2\,p^3 + 2\,p^3\phi^3 - 4\,\phi^3 s p^2 + 5\,\phi^3 s^3 p - \phi^3 s^5 \\ -2\,s\,p^3 - 2\,\phi^3 s^2 + \phi^3 s^4 - 3\,\phi^3 s^2 p + 2\,\phi^3 p \\ -2\,s^2 + s^4 - 4\,s^2 p + \phi^2 + 1 + 4\,p \end{array} \right.$$

Nous avons donc calculé une décomposition triangulaire de ce système en prenant l'ordre $\phi < s < p$. La seule contrainte était de prendre ϕ comme plus petite variable en vue de la recherche des solutions réelles effectives du problème. En effet, cette variable représente une distance du problème alors que s et p représentent respectivement une somme et un produit qui fourniront ensuite les autres distances mutuelles cherchées. L'implantation que nous avons utilisée pour traiter les systèmes proposés par I. Kotsireas produit des ensembles triangulaires où le polynôme de variable principale ϕ est irréductible. La décomposition obtenue est composée de 4 ensembles triangulaires $T_1, \ldots, T_4$ de hauteur maximale, autrement dit la variété est de dimension zéro. Les sorties vérifient donc en fait la relation

$$\mathbf{V}(\mathcal{S}_4) = \cup_{j=1}^{4} \mathbf{V}(T_j)$$

(voir la proposition 4.3.8) et l'idéal engendré par chaque T_i est radical. On peut alors chercher immédiatement les solutions réelles du système à partir des T_j. Les degrés des polynômes de variable principale ϕ sont respectivement $2, 2, 2, 37$. Mis à part l'ensemble triangulaire $\{\phi, s^2 - 1, p\}$, les autres n'ont que des degrés principaux égaux à 1 pour les polynômes de variable principale autre que ϕ.

Sur un Pentium Pro 200 Mhz de l'UMS Medicis, le calcul est effectué en moins d'une minute, ce qui correspond au temps de calcul de la base de Gröbner lexicographique par GB. Précisons que la base de Gröbner a été obtenue par un calcul de la base pour l'ordre du degré suivi du changement d'ordre avec l'algorithme FGLM [FGLM93], le calcul direct étant trop coûteux.

Notons que les améliorations apportées à nos implantations depuis le travail de comparaison expérimentale du chapitre 7 permettent d'obtenir une décomposition en un temps à peine supérieur alors que la machine est bien moins performante (voir l'exemple **Z6** dans la section 7.4).

Passons maintenant au problème de 5 corps dans l'espace. On ne dispose plus de théorème de symétrie comme dans le cas de 4 corps. Le problème ne sera ici étudié que pour des configurations centrales avec deux plans de symétrie. Le système $\mathcal{S}_5$ correspondant (exemple **Z7** de la section 7.4) obtenu par I. Kotsireas est le suivant :

$$\mathcal{S}_5 \left\{ \begin{array}{l} -4\,p^3\phi^3 + 6\,p^3 + 12\,p^2 s\phi^3 - 15\,ps^3\phi^3 + 3\,ps\phi^3 - s^3\phi^3 + 3\,s^5\phi^3 \\ -5\,p\phi^3 + 6\,p^3 s + 9\,ps^2\phi^3 + 5\,s^2\phi^3 - 3\,s^4\phi^3 \\ 3 + 4\,\phi^2 + 12\,p - 12\,ps^2 - 6\,s^2 + 3\,s^4 \end{array} \right.$$

L'implantation utilisée pour le système $\mathcal{S}_4$ calcule en 280 secondes sur le même Pentium Pro 200 Mhz de l'UMS Medicis (amélioration ici encore par rapport aux résultats de la section 7.4), la décomposition triangulaire suivante du système $\mathcal{S}_5$:

$$\begin{array}{rcl} T_1 & = & \{\phi,\, s^2 - 1,\, p\} \\ T_2 & = & \{4\,\phi^2 + 3,\, s,\, p\} \\ T_3 & = & \{3\,\phi^2 - 8, (46242673847977111759080\,2463\,\phi - 7551397017917798068124497 72)\,s \\ & & + 2927129633120086892216473 09\,\phi - 4779982674876098400963567 96, \\ & & (2237611289865630815961714421600169131027450266059707601763 3 \\ & & 304449515199836068648003119585161125233574194459\phi - 36540039 \\ & & 352411329310393638875538387743197496596952746125313720320 43 \\ & & 8142628641756413422882225836033664576396)p + 365400393524113 \\ & & 2931039363887553838774319749659695274612531372032043814262 8 \\ & & 6417564134228822258360336645763 96\phi - 5966963439641682175897 9 \\ & & 05124267117682739867376159220271368881186537386622951639467 \\ & & 49855604296672895311852 24\} \\ T_4 & = & \{31104\,\phi^{43} - 2238678\,\phi^{41} - 3172608\,\phi^{40} + 4299696\,\phi^{39} + 82401057\,\phi^{38} + 147278268\,\phi^{37} \\ & & - 309919608\,\phi^{36} - 865276476\,\phi^{35} - 3800850210\,\phi^{34} + 7126315778\,\phi^{33} \\ & & + 733665114\,\phi^{32} + 50333677740\,\phi^{31} - 84536396175\,\phi^{30} + 54761689638\,\phi^{29} \\ & & - 407185692120\,\phi^{28} + 632999590560\,\phi^{27} - 588645975519\,\phi^{26} \\ & & + 2353657296636\,\phi^{25} - 3242763707526\,\phi^{24} + 3529599532956\,\phi^{23} \\ & & - 9834864198930\,\phi^{22} + 10874183827806\,\phi^{21} - 12929906294532\,\phi^{20} \\ & & + 25468176715884\,\phi^{19} - 20799000437175\,\phi^{18} + 26462275638408\,\phi^{17} \\ & & - 32404595385312\,\phi^{16} + 17924890161384\,\phi^{15} - 24267247513272\,\phi^{14} \\ & & + 11128176042048\,\phi^{13} - 2859261720048\,\phi^{12} + 1566352284768\,\phi^{11} \\ & & + 8812742163408\,\phi^{10} - 8998593854976\,\phi^{9} + 9865121279616\,\phi^{8} \\ & & - 9903015936000\,\phi^{7} + 8795401003008\,\phi^{6} - 4873412542464\,\phi^{5} \end{array}$$

$$+\,6091765678080\,\phi^4 - 949399584768\,\phi^3 + 2724364025856\,\phi^2 + 495338913792,$$
$$f_2(\phi, s), f_3(\phi, s, p)\}$$

où $\mathsf{mdeg}(f_2) = \mathsf{mdeg}(f_3) = 1$. Le degré de la variété est donc 51.

Pour comparaison, le calcul de la base de Gröbner lexicographique est réalisé sur GB en 260 secondes, en utilisant un changement d'ordre comme pour le système $\mathcal{S}_4$. On obtient ainsi sur un problème *réel* une efficacité comparable au calcul d'une base de Gröbner avec des logiciels spécialisés. Il semble raisonnable de prétendre que nos méthodes peuvent être concurrentielles dans un certain nombre de cas, surtout si l'on tient compte du fait que les performances devraient être nettement améliorées par un passage de nos implantations dans un langage plus efficace que AXIOM.

Notons pour finir que l'ordre des variables joue un rôle important pour l'efficacité de nos méthodes. À cet effet, nous avons implanté un package de choix heuristique de l'ordre dont le principe est proposé par D. Wang dans [Wan92a]. Pour les deux problèmes ci-dessus, si on choisit l'ordre $s < \phi < p$ indiqué par notre package, on obtient alors une décomposition plus rapidement qu'une base de Gröbner avec GB. Le temps de calcul est approximativement identique pour l'obtention de la base de Gröbner alors que la décomposition triangulaire de $\mathcal{S}_4$ est calculée en 20 sec. environ (3 fois plus vite que ci-dessus) et celle de $\mathcal{S}_5$ prend 45 sec (6 fois plus vite que ci-dessus).

Annexe A

Notions mathématiques

Ce chapitre présente les notions mathématiques que nous utilisons dans l'ouvrage et rappelle certains résultats d'algèbre commutative sur lesquels nous nous appuyons.

La première section est consacrée aux généralités sur les idéaux. La section 2 traite des anneaux de fractions. Les algorithmes qui sont présentés dans le chapitre 5 travaillent en fait implicitement dans un anneau total de fractions associé à un ensemble triangulaire de polynômes. Le lecteur dispose dans cette section assez détaillée de tous les éléments nécessaires à la compréhension des résultats du chapitre 4 qui utilisent le passage dans un anneau de fractions. La section 3 rappelle la notion de hauteur pour les idéaux, et la section 4 celle de suite régulière dans un anneau. Les suites régulières sont un moyen d'étudier la hauteur des idéaux premiers associés à un idéal lorsqu'on est dans un anneau de Macaulay. Nous nous en servons pour montrer le résultat d'équidimensionnalité du théorème 4.1.4.

A.1 Idéaux

Soit I un idéal de A. Pour tout élément a de A, on désigne par $\overline{a}^I$ l'image par l'homomorphisme surjectif canonique de A dans l'anneau quotient A/I. L'ensemble des idéaux premiers de A, appelé *spectre* de A, est noté $\mathrm{spec}(A)$.

Rappelons que les idéaux premiers présentent la propriété bien connue ci-dessous qui est souvent employée en algèbre commutative (voir par exemple [AM69] prop. 1.11 p.8).

Proposition A.1.1 *Soit A un anneau et I un idéal de A contenu dans une union finie d'idéaux premiers $\cup_i \mathcal{P}_i$. Alors I est inclus dans l'un des $\mathcal{P}_i$. D'autre part, si un idéal premier $\mathcal{P}$ contient une intersection finie $\cap_i I_i$ d'idéaux de A alors $\mathcal{P}$ contient l'un des I_i. Et cette inclusion est une égalité lorsque $\mathcal{P} = \cap_i I_i$.*

Lorsque deux idéaux I et J de A vérifient $I + J = A$, on dit qu'ils sont *comaximaux*. Il est clair que deux idéaux maximaux distincts sont comaximaux. On dispose alors du théorème des restes chinois ci-dessous.

Proposition A.1.2 (restes chinois) *Soit A un anneau et $I_1, \ldots, I_m$ des idéaux de A deux à deux comaximaux. Alors $\cap_{j=1}^{s} I_j = I_1 I_2 \ldots I_m$ et $A/I \simeq A/I_1 \times \ldots \times A/I_m$.*

Preuve. voir [Zip93] p. 227. □

Soit A et B deux anneaux et φ un homomorphisme d'anneaux unitaires de A dans B. On s'intéressera plus loin au cas où B est un anneau de fractions de A et à celui où B est l'anneau polynomial $A[X]$. Dans la situation ci-dessus, si I est un idéal de A alors l'idéal $I^e = \langle\varphi(I)\rangle_B$ est appelé *extension* de I. Si I' est un idéal de B, l'idéal $I'^c = \varphi^{-1}(I')$ est appelé *contraction* de I'.

Remarque A.1.3 Lorsque A est un sous-anneau de B on prend naturellement pour φ l'application identité de A dans B. On a ainsi $I'^c = I' \cap A$. Nous rencontrerons cette situation avec les anneaux de polynômes $A[X]$.

Les propriétés générales ci-dessous se vérifient alors facilement.

Proposition A.1.4 *Soit A et B deux anneaux. Avec les notations d'extension et de contraction définies ci-dessus, on a :*

(i) $I \subseteq I^{ec}$; $I'^{ce} \subseteq I'$

(ii) $(I_1 + I_2)^e = I_1^e + I_2^e$

(iii) $(I_1 I_2)^e = I_1^e I_2^e$

(iv) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$

(v) $(\sqrt{I})^e \subseteq \sqrt{I^e}$

(vi) $(I' \cap J')^c = (I'^c \cap J'^c)$

(vii) $(\sqrt{I'})^c = \sqrt{I'^c}$.

A.1.1 Idéal quotient et idéal saturé

Notation A.1.5 *Soit F un sous-ensemble de l'anneau A et I un idéal de A. On note $I : F$ l'ensemble $I : F = \{a \in A \mid (\forall f \in F)\ fa \in I\}$. Si $F = \{f\}$ alors on écrit simplement $I : f$.*

En notant Fa l'ensemble des produits de a par un élément de F, on peut aussi écrire que $I : F = \{a \in A \mid\ Fa \subseteq I\}$. On vérifie alors aisément que $I : F$ est un idéal de A tel que :

– si $F \subseteq I$ alors $I : F = A$,

– si $F \not\subseteq I$ alors $I : F$ est un idéal propre de A qui contient l'idéal I.

De plus, il est clair que si $I_1 \subseteq I_2$ alors $(I_1 : F) \subseteq (I_2 : F)$.

Définition A.1.6 *Si I et J sont des idéaux de A on dit que l'idéal $I : J$ est l'*idéal quotient *de I par J.*

Rappelons les relations classiques :

$$
\begin{aligned}
(\bigcap_{i=1}^{r} I_i) : F &= \bigcap_{i=1}^{r}(I_i : F) , &\text{(A.1)}\\
I : \sum_{i=1}^{r} F_i &= \bigcup_{i=1}^{r}(I : F_i) , &\text{(A.2)}\\
(I : F_1) : F_2 &= I : (F_1F_2) . &\text{(A.3)}
\end{aligned}
$$

Lemme A.1.7 *Soit I un idéal de A et F une partie de A. Alors $\sqrt{I : F} \subseteq \sqrt{I} : F$.*

Preuve. Soit $a \in \sqrt{I : F}$. Il existe $m \in \mathbb{N}$ tel que $a^m \in I : F$. Pour tout $f \in F$ on a $fa^m \in I$ donc $(fa)^m \in I$, autrement dit $fa \in \sqrt{I}$. On a ainsi $a \in \sqrt{I} : F$. □

Remarque A.1.8 L'inclusion du lemme A.1.7 n'est pas en général une égalité. Il suffit de prendre par exemple $I = \langle x_1^2 x_2^2 \rangle$ et $F = \{x_1\}$ dans $\mathbf{P}_2$. On a ainsi $I : F = \langle x_1 x_2^2 \rangle$ d'où $\sqrt{I : F} = \langle x_1 x_2 \rangle$ alors que $\sqrt{I} : F = \langle x_2 \rangle$

Proposition A.1.9 *Soit I un idéal de A et F une partie de A. Si I est radical alors l'idéal $I : F$ est radical.*

Preuve. Il suffit de montrer que $\sqrt{I : F} \subseteq I : F$. Puisque $\sqrt{I} = I$, le résultat est une conséquence directe du lemme A.1.7. □

La notion d'idéal quotient est utile pour étudier la différence ensembliste de deux k-variétés. Généralement une différence de deux variétés n'est pas une variété. Considérons par exemple dans K^2 les variétés $V_1 = \mathbf{V}(x_1x_2)$ et $V_2 = \mathbf{V}(x_1)$. L'ensemble $W = V_1 \setminus V_2$ correspond à l'axe Ox_2 privé de l'origine. On peut vérifier que W n'est pas une variété, mais on constate qu'il manque peu de chose pour en faire une variété, à savoir l'ensemble des zéros de x_2. Lorsque le corps K est algébriquement clos ce phénomène s'explique avec la notion de clôture de Zariski (définition 1.1.6) comme le précise le théorème suivant.

Théorème A.1.10 *Soit I un idéal de $\mathbf{P}_n$ et F une partie de $\mathbf{P}_n$. On a*

$$\overline{\mathbf{V}_K(I) \setminus \mathbf{V}_K(F)} \subseteq \mathbf{V}_K(I : F) .$$

De plus, si K est algébriquement clos et I est un idéal radical, alors

$$\overline{\mathbf{V}_K(I) \setminus \mathbf{V}_K(F)} = \mathbf{V}_K(I : F) .$$

Preuve. Pour le premier résultat, il suffit de prouver que $\mathbf{V}_K(I) \setminus \mathbf{V}_K(F) \subseteq \mathbf{V}_K(I : F)$. Soit $\zeta \in \mathbf{V}_K(I) \setminus \mathbf{V}_K(F)$ et $p \in I : F$. Puisque ζ n'appartient pas à $\mathbf{V}_K(F)$, il existe un polynôme q de F tel que $q(\zeta) \neq 0$. D'autre part, on a $qp \in I$ donc $q(\zeta)p(\zeta) = 0$. On en conclut que ζ est un zéro de p dans K.

Supposons maintenant que K soit algébriquement clos et que I soit radical. Il ne reste à prouver que l'inclusion réciproque. Soit p un élément de $\mathbf{Id}_k(\mathbf{V}_K(I) \setminus \mathbf{V}_K(F))$ et $q \in F$. Pour $\zeta \in \mathbf{V}_K(I)$, si on a $q(\zeta) \neq 0$ alors $\zeta \in \mathbf{V}_K(I) \setminus \mathbf{V}_K(F)$ donc $p(\zeta) = 0$. On en déduit $qp \in \mathbf{Id}_k(\mathbf{V}_K(I))$ puis $qp \in \sqrt{I}$ selon le Nullstellensatz (théorème 1.2.1) . On a par hypothèse $I = \sqrt{I}$ donc $p \in I : F$. Par conséquent $\mathbf{Id}_k(\mathbf{V}_K(I) \setminus \mathbf{V}_K(F)) \subseteq I : F$ d'où $\mathbf{V}_K(I : F) \subseteq \mathbf{V}_K(\mathbf{Id}_k(\mathbf{V}_K(I) \setminus \mathbf{V}_K(F)))$. □

Proposition A.1.11 *Soit Q un idéal $\mathcal{P}$-primaire de A et $a \in A$. On a :*

- *si $a \in Q$ alors $Q : a = A$,*
- *si $a \notin Q$ alors $Q : a$ est $\mathcal{P}$-primaire,*
- *si $a \notin \mathcal{P}$ alors $Q : a = Q$.*

Preuve. La première affirmation est claire. Le troisième point découle immédiatement de la définition d'un idéal primaire. Pour prouver la deuxième affirmation on considère $xy \in Q : a$. Supposons que $y \notin \mathcal{P}$. Comme $(ax)y \in Q$ et Q primaire, on obtient $ax \in Q$, c'est-à-dire $x \in Q : a$. Par conséquent $Q : a$ est primaire. De plus, pour $x \in Q : a$ l'hypothèse $a \notin Q$ entraîne que $x \in \mathcal{P}$. On a ainsi $Q \subseteq Q : a \subseteq \mathcal{P}$. Par passage au radical on trouve $\sqrt{Q : a} = \mathcal{P}$. □

La notion de saturé d'un idéal rappelée ci-dessous présente des similarités avec celle d'idéal quotient. Elle intervient dans tout ce qui touche aux ensembles triangulaires de polynômes que nous manipulons dans les algorithmes de résolution de systèmes algébriques.

Définition A.1.12 *Soit $f \in A$. On appelle* saturé *de I par f la partie de A notée $I : f^\infty$ définie par*

$$I : f^\infty = \{a \in A \mid (\exists\, m \in \mathbb{N})\ f^m a \in I\}\ .$$

On constate aisément que le saturé de I par f est un idéal de A contenant I et qui vérifie les propriétés suivantes :

- Si $I \subseteq J$ alors $(I : f^\infty) \subseteq (J : f^\infty)$,
- $(I : f_1^\infty) : f_2^\infty = I : (f_1 f_2)^\infty$.

Proposition A.1.13 *Pour des idéaux I et J de A et un élément f de A, les relations suivantes sont vérifiées :*

(i) $(I \cap J) : f^\infty = (I : f^\infty) \cap (J : f^\infty)$,

(ii) $(I : f^\infty) + (J : f^\infty) \subseteq (I + J) : f^\infty$

Preuve. Montrons l'égalité (i). L'inclusion $(I \cap J) \subseteq I$ donne immédiatement $(I \cap J) : f^\infty \subseteq I : f^\infty$. On obtient de même $(I \cap J) : f^\infty \subseteq J : f^\infty$, ce qui prouve l'inclusion directe. Réciproquement, si $a \in (I : f^\infty) \cap (J : f^\infty)$ alors il existe deux entiers m et n tels que $f^m a \in I$ et $f^n a \in J$. On a donc $f^{m+n} a \in (I \cap J)$, c'est-à-dire $a \in (I \cap J) : f^\infty$.

L'inclusion (ii) est évidente en se servant du fait que l'inclusion est conservée par passage aux saturés. □

Soit I un idéal de A et $f \in A$. En utilisant les propriétés ci-dessus, on peut construire la suite croissante d'idéaux suivante :

$$I \subseteq I : f \subseteq I : f^2 \ldots \subseteq I : f^j \subseteq \ldots \subseteq I : f^\infty \ . \tag{A.4}$$

On en déduit le résultat bien connu que si A est un anneau noethérien alors il existe un entier m_0 tel que $I : f^\infty = I : f^{m_0}$.

Dans le cas particulier où I est radical, la proposition A.1.14 suivante précise que les inclusions de la chaîne croissante d'idéaux (A.4) sont quasiment toutes des égalités. Une comparaison avec le lemme A.1.7 permet de constater que le passage au radical s'effectue de façon plus satisfaisante pour les saturés que pour les idéaux quotients.

Proposition A.1.14 *Soit I un idéal de A et $f \in A$. Pour tout entier strictement positif m on a*

(*i*) $\sqrt{I} : f^\infty = \sqrt{I} : f^m = \sqrt{I} : f$,

(*ii*) $\sqrt{I : f^\infty} = \sqrt{I} : f^\infty = \sqrt{I} : f$.

Preuve. Soit m un entier strictement positif. L'inclusion $\sqrt{I} : f \subseteq \sqrt{I} : f^m$ est triviale. Réciproquement, si $a \in \sqrt{I} : f^m$ alors $f^m a \in \sqrt{I}$. On a donc $(fa)^m \in \sqrt{I}$, d'où $fa \in \sqrt{I}$, et par conséquent $a \in \sqrt{I} : f$. On a ainsi montré $\sqrt{I} : f^m = \sqrt{I} : f$. Mais le fait que m soit fixé n'a pas été utilisé; de la même manière on obtient donc $\sqrt{I} : f^\infty = \sqrt{I} : f$.

Pour la partie (*ii*) nous n'avons plus à montrer que la première égalité. L'inclusion directe s'obtient facilement de la même manière que dans le lemme A.1.7 en remplaçant F par f^∞. Réciproquement, si $a \in \sqrt{I} : f$ alors $fa \in \sqrt{I}$. Il existe ainsi un entier m tel que $(fa)^m \in I$. Par conséquent $a^m \in I : f^\infty$ d'où $a \in \sqrt{I : f^\infty}$. □

Le cas des idéaux primaires étudié dans la proposition ci-dessous sera exploité dans les anneaux noethériens.

Proposition A.1.15 *Soit Q un idéal primaire de A et $\mathcal{P} = \sqrt{Q}$. Soit h un élément de A. Alors*

(*i*) $h \in \mathcal{P} \Rightarrow Q : h^\infty = A$

(*ii*) $h \notin \mathcal{P} \Rightarrow Q : h^\infty = Q$

Preuve. Supposons que $h \in \mathcal{P}$. Il existe $m \in \mathbb{N}$ tel que $h^m \in Q$. Par conséquent pour tout $a \in A$, on a $h^m a \in Q$, donc $a \in Q : h^\infty$, ce qui montre (*i*).

Considérons maintenant un élément h de A tel que $h \notin \mathcal{P}$. On a trivialement $Q \subseteq Q : h^\infty$. Réciproquement, si $a \in Q : h^\infty$ alors il existe $m \in \mathbb{N}$ tel que $h^m a \in Q$. L'idéal Q étant primaire et $h^m \notin \mathcal{P}$, on obtient $a \in Q$. Par conséquent $Q : h^\infty = Q$. □

Finalement, pour un idéal I et un polynôme f donnés dans $\mathbf{P}_n$, le passage au saturé permet d'étudier les zéros de I qui ne sont pas zéros de f en s'affranchissant de l'hypothèse de radicalité du théorème A.1.10.

Proposition A.1.16 *Soit I un idéal de $\mathbf{P}_n$ et $f \in \mathbf{P}_n$. Si K est algébriquement clos alors*

$$\mathbf{V}_K(I : f^\infty) = \overline{\mathbf{V}_K(I) \setminus \mathbf{V}_K(f)} \ .$$

Preuve. Puisque K est algébriquement clos on a $\mathbf{V}_K(I : f^\infty) = \mathbf{V}_K(\sqrt{I : f^\infty})$. Il résulte de la proposition A.1.14 que $\mathbf{V}_K(I : f^\infty) = \mathbf{V}_K(\sqrt{I} : f)$. En appliquant le théorème A.1.10 on obtient alors l'égalité voulue. □

A.1.2 Décomposition primaire

Dans cette partie, l'anneau A est supposé noethérien.

Définition A.1.17 *Si $Q_1, \ldots, Q_s$ sont des idéaux primaires d'un anneau noethérien A on dit que $I = \cap_{i=1}^s Q_i$ est une* décomposition primaire *de l'idéal I. Si, de plus, les $\sqrt{Q_i}$ sont tous distincts et $Q_i \not\supseteq \cap_{j\neq i} Q_j$ $(1 \leq i \leq s)$, alors la décomposition primaire est dite* minimale *(ou* réduite*).*

Rappelons que dans un anneau noethérien tout idéal propre admet une décomposition primaire minimale. De plus, le premier théorème d'unicité affirme que pour une décomposition primaire minimale $I = \cap_{i=1}^s Q_i$, le nombre de composantes et l'ensemble des idéaux premiers $\{\sqrt{Q_1}, \ldots, \sqrt{Q_s}\}$ ne dépendent pas de la décomposition choisie (voir [AM69] p. 52), ce qui justifie la définition ci-dessous.

Définition A.1.18 *Si $I = \cap_{i=1}^s Q_i$ est une décomposition primaire minimale de I alors les idéaux premiers $\mathcal{P}_i = \sqrt{Q_i}$ sont appelés* idéaux premiers associés *à I. L'ensemble des idéaux premiers associés à I est noté* $\mathsf{ass}(I)$*. Les éléments minimaux de* $\mathsf{ass}(I)$ *pour l'inclusion sont dits* idéaux premiers isolés *de I et les autres sont dits* immergés*. Une composante primaire Q_i de I est dite isolée (resp. immergée) si son radical est un idéal premier isolé (resp. immergé) de I.*

Remarque A.1.19 Reprenons les notations de la définition A.1.18. Étant donné que lorsqu'un idéal premier $\mathcal{P}$ contient l'idéal I alors il contient l'un des $\mathcal{P}_i$ (proposition A.1.1), les idéaux premiers isolés d'un idéal I sont les éléments minimaux de la famille des idéaux premiers de A qui contiennent I. D'autre part, un idéal I est radical si et seulement si tous les idéaux primaires $Q_1, \ldots, Q_s$ sont premiers. Dans ce cas, il est clair que les idéaux premiers associés à I sont tous isolés.

Par passage au radical, une décomposition primaire minimale de I donne une décomposition primaire de $\sqrt{I}$, dont les composantes sont les idéaux premiers associés à I. Mais la décomposition de $\sqrt{I}$ ainsi obtenue n'est pas forcément minimale. Il faut donc prendre garde à ne pas confondre $\mathsf{ass}(I)$ et $\mathsf{ass}(\sqrt{I})$. L'exemple élémentaire suivant illustre cette remarque :

Considérons les idéaux $Q_1 = \langle x_1 \rangle$ et $Q_2 = \langle x_1, x_2 \rangle^2$ dans $\mathbf{P}_2$. On vérifie sans peine que ces idéaux sont primaires. Soit $I = Q_1 \cap Q_2$. Cette décomposition primaire de I est minimale et $\mathsf{ass}(I) = \{\langle x_1 \rangle, \langle x_1, x_2 \rangle\}$. Mais par passage au radical, on a $\sqrt{I} = \langle x_1 \rangle \cap \langle x_1, x_2 \rangle = \langle x_1 \rangle$ puisque $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle$. On trouve alors $\mathsf{ass}(\sqrt{I}) = \{\langle x_1 \rangle\}$.

Nous montrons dans le chapitre 4 que l'idéal que nous associons à un ensemble triangulaire de polynômes de $\mathbf{P}_n$ n'a que des composantes primaires isolées. Par conséquent, son ensemble des idéaux premiers associés n'est pas modifié par passage au radical.

La proposition ci-dessous décrit la décomposition primaire du saturé d'un idéal par un élément de A. Nous l'utiliserons couramment par la suite.

Proposition A.1.20 *Soit I un idéal d'un anneau noethérien A et h un élément de A. Soit $I = Q_1 \cap Q_2 \cap \ldots \cap Q_r \ldots \cap Q_s$ une décomposition primaire de I, ordonnée de sorte que pour $j \in [1, r]$ on a $h \notin \sqrt{Q_j}$, et pour $j \in [r+1, s]$ on a $h \in \sqrt{Q_j}$. Alors*

$$I : h^\infty = \bigcap_{j=1}^{r} Q_j.$$

De plus, si la décomposition primaire de I est minimale alors la décomposition de $I : h^\infty$ ainsi obtenue est minimale.

Preuve. Avec la proposition A.1.13 on obtient $I : h^\infty = (\cap_{j=1}^s Q_j) : h^\infty = \cap_{j=1}^s (Q_j : h^\infty)$. La proposition A.1.15 entraîne alors immédiatement la décomposition voulue. De plus, si la décomposition primaire de I est minimale, alors les $\sqrt{Q_j}$ sont tous distincts et pour tout j on a $(\cap_{j \neq j} Q_j) \not\subseteq Q_j$. Ces deux propriétés sont évidemment conservées dans la décomposition primaire de $I : h^\infty$ obtenue. Celle-ci est donc minimale. □

Le corollaire suivant est une conséquence directe de la proposition A.1.20.

Corollaire A.1.21 *Soit h un élément de A. Alors $I : h^\infty = I$ si et seulement si h n'appartient à aucun idéal premier associé à I.*

La proposition A.1.22 ci-dessous caractérise les idéaux premiers associés. Elle est fondamentale et induit le résultat classique de la proposition A.1.23 dont il est fait régulièrement usage dans tout le document.

Proposition A.1.22 *Soit I un idéal propre dans un anneau noethérien A. Si $\mathcal{P}$ est un idéal premier de A alors $\mathcal{P} \in \mathsf{ass}(I)$ si et seulement si il existe $a \in A$ tel que $\mathcal{P} = I : a$.*

Preuve. Soit $I = \cap_{j=1}^m Q_j$ une décomposition primaire minimale de I. Prenons $\mathcal{P} = \sqrt{Q_1}$ sans perte de généralité. Rappelons qu'il existe l tel que $\mathcal{P}^l \subseteq Q_1$ puisque A est noethérien ([vdW91] théorème 5 p. 125). La décomposition primaire de I étant minimale, il existe $b \in \cap_{j>1} Q_j$ tel que $b \notin Q_1$. On a ainsi $Q_1 b \subseteq I$ donc $\mathcal{P}^l b \subseteq I$. Notons ℓ le plus petit des entiers l tels que $\mathcal{P}^l b \subseteq I$. On prend alors $a \in \mathcal{P}^{\ell-1} b$ tel que $a \notin I$. Il est facile de voir que $a \notin Q_1$. Pour $x \in I : a$, la relation $ax \in I \subseteq Q_1$ entraîne donc $x \in \mathcal{P}$, ce qui prouve $I : a \subseteq \mathcal{P}$. D'autre part on a $\mathcal{P} a \subseteq \mathcal{P}^\ell b \subseteq I$ donc $\mathcal{P} \subseteq I : a$ et $\mathcal{P} = I : a$.

Supposons maintenant que $\mathcal{P} = I : a$. Il résulte alors de la proposition A.1.20 que $\mathcal{P} = \cap_{j=1}^m Q_j : a$. Il existe donc j tel que $\mathcal{P} = Q_j : a$ (proposition A.1.1), ce qui entraîne $\sqrt{Q_j} \subseteq \mathcal{P}$. D'autre part, si $b \in \mathcal{P}$ alors $ab \in Q_j$. On a forcément $a \notin Q_j$ sinon on aurait $\mathcal{P} = A$. On en déduit que $b \in \sqrt{Q_j}$, d'où $\mathcal{P} \subseteq \sqrt{Q_j}$ pour finir. □

Proposition A.1.23 *Soit I un idéal propre d'un anneau noethérien A. L'ensemble des diviseurs de zéro modulo I correspond à la réunion des idéaux premiers associés à I.*

Preuve. On note $I = \cap_{i=1}^s Q_i$ une décomposition primaire réduite de I. Soit $a \in \mathbf{Div}(A/I)$. Il existe $b \notin I$ tel que $ab \in I$. Il existe donc un indice i tel que $b \notin Q_i$ et $ab \in Q_i$. On en déduit $a \in \sqrt{Q_i}$. La réciproque se déduit directement de la proposition A.1.22. □

A.2 Anneaux de fractions

Nous utiliserons dans le chapitre 4 le passage dans un anneau de fractions pour prouver un résultat d'équidimensionnalité. La notion d'anneau de fractions généralise celle bien connue de corps des fractions d'un anneau intègre. Soit A un anneau commutatif et S une *partie multiplicativement close* de A, c'est-à-dire que $1 \in S$ et que le produit de deux éléments de S appartient à S. La relation $\sim$ sur $A \times S$ définie par $(a_1, s_1) \sim (a_2, s_2)$ si il existe $u \in S$ tel que $u(s_2 a_1 - s_1 a_2) = 0$ est une relation d'équivalence. On note la classe d'équivalence de $(a, s) \in A \times S$ par a/s. Un élément de a de A peut être identifié à $a/1$. L'ensemble des classes d'équivalence est noté $S^{-1}A$. L'ensemble de ces fractions à numérateur dans A et à dénominateur dans S, peut être muni d'une structure d'anneau avec l'addition et la mutiplication usuelle sur les fractions.

Définition A.2.1 *L'anneau $S^{-1}A$ ci-dessus est appelé* anneau des fractions *de A relativement à S. Lorsque S est le complémentaire dans A d'un idéal premier $\mathcal{P}$, l'anneau $S^{-1}A$ est noté $A_{\mathcal{P}}$ et aussi appelé* anneau local *de $\mathcal{P}$.*

Remarque A.2.2 On dispose d'un homomorphisme d'anneaux naturel $\lambda_S : a \to a/1$ de A dans $S^{-1}A$ tel que l'image de tout élément de S est inversible dans $S^{-1}A$. Le noyau de λ_S est l'ensemble des éléments $a \in A$ pour lesquels il existe $u \in S$ tel que $ua = 0$. Ainsi λ_S est injectif si et seulement si $S \cap \mathbf{Div}(A) = \emptyset$. De plus, tout élément a/s de $S^{-1}A$ peut s'écrire $\lambda_S(a)\lambda_S(s)^{-1}$.

Définition A.2.3 *L'ensemble des éléments réguliers de A (c'est-à-dire les éléments de A qui ne sont pas diviseurs de zéro), qu'on note $\mathbf{reg}(A)$, est une partie multiplicativement close de A. L'anneau des fractions de A relativement à $\mathbf{reg}(A)$ est appelé* anneau total des fractions *de A. On le désigne par $\mathrm{fr}(A)$. Cet anneau a la propriété que tout élément régulier de $\mathrm{fr}(A)$ admet un inverse dans $\mathrm{fr}(A)$.*

Dans la suite nous dirons simplement *partie multiplicative* de A au lieu de partie multiplicativement close. Les parties multiplicatives que nous emploierons dans le chapitre consacré aux ensembles triangulaires seront en général *saturées*.

Définition A.2.4 *Une partie multiplicative S de A est dite* saturée *si pour tout couple (a_1, a_2) d'éléments de A on a : $a_1 a_2 \in S \Rightarrow a_1 \in S$ et $\mathrm{a}_2 \in \mathrm{S}$.*

Les parties multiplicatives saturées sont caractérisées comme suit (voir théorème 2 p.2 dans [Kap74]).

Proposition A.2.5 *Une partie multiplicative S de A est saturée si et seulement si $A \setminus S$ est une réunion (éventuellement vide) d'idéaux premiers de A.*

Rappelons la "propriété universelle" pour les anneaux de fractions.

Théorème A.2.6 *Soit S une partie multiplicative de l'anneau A et $\lambda_S : A \to S^{-1}A$ l'homomorphisme canonique. Si $f : A \to B$ est un homomorphisme d'anneaux tel que $f(s)$ est inversible pour tout $s \in S$, alors il existe un unique homomorphisme d'anneaux $\bar{f} : S^{-1}A \to B$ tel que $f = \bar{f} \circ \lambda_S$. En fait, $\bar{f}$ est défini par $\bar{f}(a/s) = f(a)f(s)^{-1}$ pour tout $a \in A$ et tout $s \in S$.*

Preuve. Montrons d'abord que $\bar{f}$ ci-dessus est bien défini. On considère $a/s = b/t$ dans $S^{-1}A$. Il existe donc $u \in S$ tel que $u(at-bs) = 0$. On a ainsi $f(u)(f(a)f(t)-f(b)f(s)) = 0$. Les images $f(s)$, $f(t)$ et $f(u)$ étant inversibles par hypothèse, on multiplie l'égalité précédente par l'inverse de leur produit pour en déduire $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. On vérifie sans peine que $\bar{f}$ est bien un homomorphisme d'anneaux. Supposons maintenant que $g : S^{-1}A \to B$ soit un morphisme tel que $f = g \circ \lambda_S$. Pour $s \in S$ on a alors $1_B = g(1) = g(s/1)g(1/s) = f(s)g(1/s)$. Par conséquent $g(1/s) = f(s)^{-1}$. Il en découle pour $a/s \in S^{-1}A$ que $g(a/s) = g(a/1)g(1/s) = f(a)f(s)^{-1}$, donc $g = \bar{f}$. □

Remarque A.2.7 Avec les notations du théorème A.2.6, la définition de $\bar{f}$ entraîne immédiatement que si f est injectif (resp. surjectif) alors $\bar{f}$ est injectif (resp. surjectif).

Avec le théorème A.2.6, on montre facilement que les propriétés de l'homomorphisme canonique λ_S données dans la remarque A.2.2 permettent de déterminer $S^{-1}A$ à isomorphisme près, comme il est précisé ci-dessous.

Proposition A.2.8 *Soit S une partie multiplicative de A et λ_S l'homomorphisme canonique de A dans $S^{-1}A$. Soit $f : A \to B$ un homomorphisme d'anneaux tel que :*

(i) les éléments de $f(S)$ sont inversibles dans B,

(ii) si $a \in \mathrm{Ker}(f)$ alors il existe $s \in S$ tel que $sa = 0$,

(iii) tout élément de B peut s'écrire $f(a)f(s)^{-1}$ avec $a \in A$ et $s \in S$.

Alors il existe un unique isomorphisme $\bar{f}$ de $S^{-1}A$ dans B tel que $f = \bar{f} \circ \lambda_S$.

Preuve. D'après le théorème A.2.6 on dispose d'un unique homomorphisme $\bar{f} : S^{-1}A \to B$ tel que $\bar{f}(a/s) = f(a)f(s)^{-1}$. Si $a/s \in S^{-1}A$ vérifie $\bar{f}(a/s) = 0$, on a donc $f(a) = 0$. Il résulte alors de l'hypothèse (ii) que $a/s = 0$, ce qui prouve l'injectivité de $\bar{f}$. L'hypothèse (iii) entraîne ensuite clairement la surjectivité de $\bar{f}$. □

Proposition A.2.9 *Soit S et T deux parties multiplicatives d'un anneau A telles que $S \subseteq T$. On note T' l'image de T dans $S^{-1}A$ par λ_S. Alors*

$$T^{-1}A \simeq T'^{-1}S^{-1}A .$$

Preuve. On considère le morphisme naturel $\lambda_{T'} : S^{-1}A \to T^{-1}A$ qui, à $a/s \in S^{-1}A$ associe a/s dans $T^{-1}A$. Il suffit de vérifier que $\lambda_{T'}$ vérifie les conditions de la proposition A.2.8 pour la partie multiplicative T'. Tout élément de T' s'écrit $t/1$ et son image par $\lambda_{T'}$ est donc inversible, ce qui prouve (i). Montrons (ii). Si $\lambda_{T'}(a/s) = 0$ alors il existe $t \in T$ tel que $ta = 0$. L'élément $t/1$ dans $S^{-1}A$ appartient à T' et vérifie $(t/1)(a/s) = 0$. L'assertion (iii) est claire puisque tout élément de $T^{-1}A$ peut s'écrire $a/t = (a/1)(t/1)^{-1}$. □

Nous rappelons dans ce qui suit les propriétés des idéaux dans les anneaux de fractions. Les notations d'extension et de contraction introduites au début de la section A.1 sont ici relatives à l'homomorphisme canonique $\lambda_S : a \to a/1$ décrit plus haut. Ainsi, pour tout idéal

I de A on désigne par I^e l'idéal engendré dans $S^{-1}A$ par $\lambda_S(I)$, et pour tout idéal I' de $S^{-1}A$ on désigne par I'^c l'idéal $\lambda_S^{-1}(I')$.

Proposition A.2.10 *Soit S une partie multiplicative d'un anneau A. Soit I un idéal de A. Alors l'idéal I^e de $S^{-1}A$ vérifie*

$$I^e \;=\; \{\, a/s \;,\; a \in I \text{ et } s \in S \,\} \;.$$

Preuve. Soit α un élément de I^e. Alors il existe $a_1, \ldots, a_m \in I$ et $b_1/s_1, \ldots, b_m/s_m \in S^{-1}A$ tels que $\alpha = \sum_{j=1}^m (b_j/s_j)(a_j/1) = \sum_{j=1}^m (b_j a_j/s_j)$. On met le membre droit de l'égalité sur un même dénominateur $s \in S$ (puisque S est une partie multiplicative), et on en déduit l'inclusion directe. Quant à l'inclusion inverse, elle est claire. □

Chaque classe de I^e peut s'écrire comme quotient d'un élément de I par un élément de S, mais cela ne signifie pas pas pour autant que toute représentation a/s d'un élément de I^e est telle que a appartient à I. Nous verrons plus bas qu'un tel résultat sera vérifié dans le cas où I est primaire, mais ce n'est pas le cas en général.

Proposition A.2.11 *Soit S une partie multiplicative d'un anneau A et I un idéal de A. Alors*

$$I^{ec} \;=\; \{\, a \in A \;\mid (\exists s \in S)\;\; sa \in I \,\} \;.$$

Preuve. Soit $a \in A$. Il résulte de la proposition A.2.10 que $a \in I^{ec}$ si et seulement si il existe $b \in I$ et $t \in S$ tels que $a/1 = b/t$. Par définition de la relation d'équivalence $\sim$ il existe alors $u \in S$ tel que $u(at - b) = 0$. En posant $s = ut$ on en déduit que $sa \in I$. Comme $s \in S$ puisque S est une partie multiplicative, on a prouvé l'inclusion directe dans le corollaire. Réciproquement, si $sa \in I$ pour un élément s de S, alors $a/1 = (sa)/s$ appartient à I^e. □

Corollaire A.2.12 *Soit I un idéal de l'anneau A et S une partie multiplicative de A. Alors on a $I^e = S^{-1}A$ si et seulement si $I \cap S \neq \emptyset$.*

Preuve. Dire que $I^e = S^{-1}A$ revient à dire que $1 \in I^{ec}$. On vérifie immédiatement avec l'expression de la proposition A.2.11 que cela équivaut à une intersection non vide de $I \cap S$. □

Proposition A.2.13 *Soit I un idéal d'un anneau A et S une partie multiplicative de A. On note $\overline{S}$ l'image de S dans l'anneau quotient A/I. Alors $\overline{S}$ est une partie multiplicative de A/I et*

$$\overline{S}^{-1}(A/I) \;=\; (S^{-1}A)/I^e \;.$$

Preuve. Le fait que $\overline{S}$ soit une partie multiplicative de A/I est trivial. On considère l'homomorphisme $g : A \to S^{-1}A/I^e$ obtenu par composition du morphisme canonique de A dans $S^{-1}A$ et de la surjection canonique de $S^{-1}A$ dans $S^{-1}A/I^e$. On a $\mathrm{Ker}(g) = I^{ec} = \{\, a \in A \mid (\exists s \in S)\; sa \in I \,\}$. On en déduit un morphisme $f : A/I \to S^{-1}A/I^e$ tel que $\mathrm{Ker}(f) = \{\, \overline{a} \in A/I \mid (\exists \overline{s} \in \overline{S})\; \overline{s}\,\overline{a} = 0 \,\}$. La condition (ii) de la proposition A.2.8 est donc satisfaite pour f. Les deux autres conditions de cette proposition se vérifient sans difficulté en utilisant la relation $f(\overline{a}) = g(a)$. □

Dans les anneaux de fractions, les extensions d'idéaux ont des propriétés plus fortes que dans le cas général décrit dans la proposition A.1.4. On a ainsi :

Proposition A.2.14 *Soit S une partie multiplicative d'un anneau A. Soit I et J deux idéaux de A. Alors on a*

(*i*) $(I \cap J)^e = I^e \cap J^e$,

(*ii*) $(\sqrt{I})^e = \sqrt{I^e}$.

Preuve. Notons que les inclusions directes sont données dans les deux cas par la proposition A.1.4. Il ne reste plus qu'à prouver les inclusions réciproques. Commençons naturellement par (i). Soit $\alpha \in I^e \cap J^e$. On a donc $\alpha = a/s = b/t$ où $a \in I$ et $b \in J$, tandis que s et t sont des éléments de S. Il existe donc $u \in S$ tel que $u(at - bs) = 0$. Etant donné que $uta = -usb$, il en résulte que $uta \in J$. On a ainsi $uta \in I \cap J$. On peut alors écrire $\alpha = (uta)/(uts)$, ce qui prouve que $\alpha \in (I \cap J)^e$.

Passons à (ii) et considérons $\alpha \in \sqrt{I^e}$ avec $\alpha = a/s$ où $a \in I$ et $s \in S$. Il existe un entier m tel que $\alpha^m \in I^e$. On peut alors écrire $\alpha^m = b/t$ avec $b \in I$ et $t \in S$. On en déduit alors qu'il existe $u \in S$ tel que $u(a^m t - bs^m) = 0$. On obtient facilement $uta^m \in I$, d'où $(uta)^m \in I$ c'est-à-dire $uta \in \sqrt{I}$. Comme α s'écrit $(uta)/(uts)$, on a $\alpha \in (\sqrt{I})^e$. □

Lorsque A est un anneau noethérien, on montre facilement que tout anneau de fractions $S^{-1}A$ est noethérien. Pour un idéal I de A on peut alors exprimer les décompositions primaires minimales de I^e et de I^{ec} en fonction d'une décomposition primaire minimale de I. Ce lien est rappelé dans la proposition A.2.22.

Lemme A.2.15 *Soit Q un idéal primaire de A et $\mathcal{P}$ son radical. Alors $Q \cap S = \emptyset$ si et seulement si $\mathcal{P} \cap S = \emptyset$.*

Preuve. On montre que $\mathcal{P} \cap S$ est non vide si et seulement si $Q \cap S$ est non vide. Supposons $\mathcal{P} \cap S \neq \emptyset$ et considérons un élément a de $\mathcal{P} \cap S$. Il existe un entier m tel que $a^m \in Q$. Puisque S est une partie multiplicative on a donc $a^m \in Q \cap S$ et $Q \cap S$ non vide. La réciproque est évidente. □

Proposition A.2.16 *Soit Q un idéal primaire de A tel que $Q \cap S = \emptyset$. Alors toute représentation a/s d'un élément de Q^e est telle que $a \in Q$.*

Preuve. Soit a/s une représentation de $\alpha \in Q^e$. Il existe $b \in Q$ et $t \in S$ tels que $\alpha = b/t$. Par conséquent il existe $u \in S$ tel que $u(at - bs) = 0$, et donc $aut \in Q$. Comme $ut \in S$, l'hypothèse et le lemme A.2.15 assurent que $ut \notin \sqrt{Q}$. L'idéal Q étant primaire, on en déduit $a \in Q$. □

Proposition A.2.17 *Soit Q un idéal primaire de A. Si $Q \cap S = \emptyset$ alors $Q^{ec} = Q$.*

Preuve. Seule l'inclusion directe est à montrer. Supposons que $a \in Q^{ec}$. Puisque $Q^{ece} = Q$ on a $a/1 \in Q^e$. Par conséquent $a \in Q$ d'après la proposition A.2.16. □

Proposition A.2.18 *Soit $\mathcal{P}$ un idéal premier de A tel que $\mathcal{P} \cap S = \emptyset$. Alors $\mathcal{P}^e$ est un idéal premier de $S^{-1}A$.*

Preuve. D'abord l'idéal $\mathcal{P}^e$ est un idéal propre d'après le corollaire A.2.12. Considérons alors α et β dans $S^{-1}A$ tels que $\alpha\beta \in \mathcal{P}^e$. Soit (a/s) et (b/t) des représentations de α et β respectivement. On déduit de la proposition A.2.16 que $ab \in \mathcal{P}$. Puisque $\mathcal{P}$ est premier on obtient $a \in \mathcal{P}$ ou $b \in \mathcal{P}$. Par conséquent α ou β appartient à $\mathcal{P}$. □

Proposition A.2.19 *Soit Q un idéal $\mathcal{P}$-primaire de A tel que $Q \cap S = \emptyset$. Alors Q^e est un idéal $\mathcal{P}^e$-primaire de $S^{-1}A$.*

Preuve. On opère de la même façon que dans la proposition A.2.18 pour montrer que Q^e est primaire. Puis on utilise le point (ii) de la proposition A.2.14 pour obtenir le radical de Q^e. □

Proposition A.2.20 *Soit $\mathcal{P}'$ un idéal premier de $S^{-1}A$. Alors $\mathcal{P}'^c$ est un idéal premier de A tel que $S \cap \mathcal{P} = \emptyset$. De plus, on a $\mathcal{P}'^{ce} = \mathcal{P}'$.*

Preuve. C'est un fait bien connu que l'image réciproque d'un idéal premier par un homomorphisme est un idéal premier. Supposons que $S \cap \mathcal{P} \neq \emptyset$. Comme en toute généralité $\mathcal{P}'^{ce} \subset \mathcal{P}'$, alors $\mathcal{P}' = S^{-1}A$, en contradiction avec l'hypothèse. On en déduit que $S \cap \mathcal{P} = \emptyset$. Il ne reste plus en fait qu'à montrer $\mathcal{P}' \subset \mathcal{P}'^{ce}$. Soit $a/s \in \mathcal{P}'$ avec $s \in S$. Comme s est inversible dans $S^{-1}A$, on a $a/1 = (a/s)(s/1)$. Il en résulte $a \in \mathcal{P}'$ puis $a \in \mathcal{P}'^c$. Le résultat s'obtient alors immédiatement. □

Proposition A.2.21 *L'extension et la contraction définissent une bijection entre* $\operatorname{spec}(S^{-1}A)$ *et l'ensemble $\wp$ des idéaux premiers de A qui sont disjoints de S.*

Preuve. La proposition A.2.18 montre que l'extension est une application de $\wp$ vers le spectre de $S^{-1}A$. C'est une surjection d'après la proposition A.2.20. Pour vérifier l'injectivité, on considère $\mathcal{P}_1$ et $\mathcal{P}_2$ dans $\wp$ tels que $\mathcal{P}_1^e = \mathcal{P}_2^e$. La proposition A.2.17 entraîne alors $\mathcal{P}_1 = \mathcal{P}_2$. □

Proposition A.2.22 *Soit A un anneau noethérien. Soit $I = Q_1 \cap \ldots \cap Q_l \cap \ldots \cap Q_m$ une décomposition primaire d'un idéal I de A telle que $Q_i \cap S = \emptyset$ pour tout $i \in [1, l]$ et $Q_i \cap S \neq \emptyset$ pour tout $i \in [l+1, m]$. Si $l = 0$ alors $I^e = S^{-1}A$ et $I^{ec} = A$. Sinon, on a les décompositions primaires suivantes:*

$$\begin{aligned} I^e &= Q_1^e \cap \ldots \cap Q_l^e \ , \\ I^{ec} &= Q_1 \cap \ldots \cap Q_l \ . \end{aligned}$$

De plus, si la décomposition de I est minimale alors les deux autres le sont aussi.

Preuve. Le cas $l = 0$ étant clair, examinons la première égalité. Elle s'obtient à l'aide de la proposition A.2.14 et du corollaire A.2.12. La proposition A.2.19 assure que la décomposition est primaire. Supposons que la décomposition de I soit minimale. Les idéaux premiers $\sqrt{Q_i^e}$

sont alors tous distincts d'après la bijection établie dans la proposition A.2.21. De plus, si on avait $(\cap_{i=1,i\neq j}^{l} Q_i^e) \subset Q_j^e$ pour un entier j de $[1,l]$, la proposition A.2.17 impliquerait qu'on a la même relation sans extension. La décomposition de I^e est donc aussi minimale.

La deuxième égalité s'obtient à partir de la première en utilisant l'égalité (vi) de la proposition A.1.4 puis la proposition A.2.17. Le cas de minimalité est ici trivial. $\square$

Remarquons que dans la proposition A.2.22, on peut remplacer les hypothèses $Q_i \cap S = \emptyset$ par $\sqrt{Q_i} \cap S = \emptyset$ d'après le lemme A.2.15. On obtient ensuite directement les corollaires ci-dessous.

Corollaire A.2.23 *Soit A un anneau noethérien. Soit $Q_1 \cap \ldots \cap Q_l \cap \ldots \cap Q_m$ une décomposition primaire de l'idéal nul de A telle que $\sqrt{Q_i} \cap S = \emptyset$ pour tout $i \in [1,l]$ et $\sqrt{Q_i} \cap S \neq \emptyset$ pour tout $i \in [l+1,m]$. Alors le noyau de l'homomorphisme canonique λ_S est*

$$\mathrm{Ker}(\lambda_S) = \cap_{i=1}^{l} Q_i \ .$$

Corollaire A.2.24 *Si I est un idéal d'un anneau noethérien A tel que $I^e \neq S^{-1}A$. Alors*

$$\begin{aligned} \mathsf{ass}(I^e) &= \{\mathcal{P}^e \mid \mathcal{P} \in \mathsf{ass}(I) \text{ et } \mathcal{P} \cap \mathrm{S} = \emptyset\} \ , \\ \mathsf{ass}(I^{ec}) &= \{\mathcal{P} \mid \mathcal{P} \in \mathsf{ass}(I) \text{ et } \mathcal{P} \cap \mathrm{S} = \emptyset\} \ . \end{aligned}$$

Les algorithmes présentés dans le chapitre 5 manipulent des polynômes de $\mathbf{P}_n$ tout en les considérant comme des polynômes à une seule variable sur un anneau A défini par un ensemble triangulaire de polynômes. Le fonctionnement de ces algorithmes est en fait basé sur le fait que l'anneau A est un produit de corps. Pour établir cette structure dans le chapitre 4 nous faisons appel à certaines propriétés des *anneaux réduits* rappelées ci-dessous. Le lecteur pourra se référer à [Bou61a] et [Bou61b] pour une étude exhaustive de ces problèmes. Nous avons d'abord besoin de quelques éléments concernant la localisation par un idéal premier.

Définition A.2.25 *Un anneau A est dit* local *s'il admet un unique idéal maximal.*

Si $\mathcal{P}$ est un idéal premier de A alors l'anneau $A_{\mathcal{P}} = S^{-1}A$ est un anneau local. Son unique idéal maximal est l'extension de $\mathcal{P}$ dans $A_{\mathcal{P}}$ par le morphisme canonique λ_S. C'est un fait connu qui est une conséquence immédiate de la proposition A.2.21. Pour éviter des confusions nous éviterons d'utiliser la notation d'extension pour l'idéal maximal de $A_{\mathcal{P}}$ et nous le désignerons par $\mathcal{P}A_{\mathcal{P}}$.

Proposition A.2.26 *Soit A un anneau et S une partie multiplicative de A. Soit $\mathcal{P}'$ un idéal premier de $S^{-1}A$ et $\mathcal{P}$ son image réciproque par l'homomorphisme canonique λ_S de A dans $S^{-1}A$. Alors*

$$(S^{-1}A)_{\mathcal{P}'} \simeq A_{\mathcal{P}} \ .$$

Preuve. On pose $T = A \backslash \mathcal{P}$ et $T' = \lambda_S(T)$. D'après les hypothèses on a $S \subseteq T$ et $\mathcal{P}' = \mathcal{P}^e$.Il résulte clairement de la proposition A.2.16 que T' ne rencontre pas $\mathcal{P}'$. Supposons d'autre part qu'un élément a/s de $S^{-1}A$ n'appartienne pas à $\mathcal{P}'$. Etant donné que $a/1 = (a/s)(s/1)$ et que $s/1 \notin \mathcal{P}'$, on obtient $a/1 \notin \mathcal{P}'$ et par suite $a \notin \mathcal{P}$. On en conclut que $(S^{-1}A)\backslash\mathcal{P}' = S^{-1}T'$.

Il est facile de vérifier que l'anneau de fractions de $S^{-1}A$ relativement à $S^{-1}T'$ est le même que relativement à T', et par conséquent

$$(S^{-1}A)_{\mathcal{P}'} = T'^{-1}(S^{-1}A) \ .$$

Le résultat est alors une conséquence de la proposition A.2.9 qui assure l'isomorphisme

$$A_{\mathcal{P}} \simeq T'^{-1}(S^{-1}A) \ .$$

□

Lemme A.2.27 *Soit I un idéal d'un anneau A. Soit $\mathcal{P} \in \mathrm{spec}(A)$ tel que $I \subseteq \mathcal{P}$. On a alors $(A/I)_{\mathcal{P}/I} \simeq A_{\mathcal{P}}/IA_{\mathcal{P}}$ et $\mathrm{fr}(A/\mathcal{P}) \simeq A_{\mathcal{P}}/\mathcal{P}A_{\mathcal{P}}$.*

Preuve. Soit $S = A \backslash \mathcal{P}$ et $\overline{S}$ l'image de S dans l'anneau quotient A/I. On vérifie facilement que $\overline{S} = (A/I) \setminus (\mathcal{P}/I)$. On a alors par définition $(A/I)_{\mathcal{P}/I} = \overline{S}^{-1}(A/I)$ d'une part et $A_{\mathcal{P}}/IA_{\mathcal{P}} = S^{-1}A/IA_{\mathcal{P}}$ d'autre part. L'isomorphisme des deux structures est tout simplement assuré par la proposition A.2.13. La seconde partie du lemme s'obtient en prenant pour I l'idéal $\mathcal{P}$ lui-même. □

Proposition A.2.28 *Soient u et x deux éléments de A. Si u est une unité et si x est nilpotent, alors $u + x$ est une unité de A.*

Preuve. Soit $m \in \mathbb{N}$ tel que $x^m = 0$. On a alors :

$$(u+x)\left(\frac{1}{u} - \frac{x}{u^2} + \frac{x^2}{u^3} + \cdots + (-1)^{m-1}\frac{x^{m-1}}{u^m}\right) = 1$$

ce qui prouve que $u + x$ est une unité de A. □

Lemme A.2.29 *Soit A un anneau noethérien et $\mathcal{P}$ un idéal premier isolé de l'idéal nul. Si $\mathcal{P}$ est un idéal maximal alors le morphisme canonique de A dans $A_{\mathcal{P}}$ est surjectif.*

Preuve. Posons $S = A \setminus \mathcal{P}$. Il suffit de montrer que pour tout $s \in S$ il existe $b \in A$ tel que $1/s = b/1$ dans $A_{\mathcal{P}}$. Puisque $s \notin \mathcal{P}$, la maximalité de $\mathcal{P}$ entraîne que 1 appartient à l'idéal engendré par $\mathcal{P}$ et s. Il existe donc $c \in A$ et $p \in \mathcal{P}$ tels que $cs = 1 - p$. Notons Q la composante primaire de radical $\mathcal{P}$ dans une décomposition primaire réduite de l'idéal nul. Puisque p est nilpotent dans l'anneau quotient A/Q, la proposition A.2.28 entraîne que cs est inversible dans A/Q. Il existe donc $d \in A$ tel que $1 - cds \in Q$. Posons $b = cd$. L'idéal $\mathcal{P}$ étant isolé, c'est le seul idéal premier associé à $\langle 0 \rangle$ qui a une intersection vide avec S. Il résulte du corollaire A.2.23 que $Q = \mathrm{Ker}(\lambda_S)$ et par conséquent $1/s = b/1$. □

Définition A.2.30 *On dit qu'un anneau A est* réduit *si aucun élément non nul de A n'est nilpotent, autrement dit si* $\mathbf{Nil}(A)$ *est réduit à 0.*

Proposition A.2.31 *Soit A un anneau et S une partie multiplicative de A. Alors on a* $\mathbf{Nil}(S^{-1}A) = \mathbf{Nil}(A)^e$. *En particulier, si A est réduit alors $S^{-1}A$ est réduit.*

Preuve. Supposons que $(a/s)^m = a^m/s^m = 0$ où $a \in A$ et $s \in S$. Il existe donc $t \in S$ tel que $ta^m = 0$, d'où $(ta)^m = 0$ c'est-à-dire $ta \in \mathbf{Nil}(A)$. On a par conséquent $a/s = (ta)(ts)^{-1} \in \mathbf{Nil}(S^{-1}A)$. L'inclusion réciproque est immédiate. □

Dans la définition A.2.30 il revient au même de dire que l'idéal nul est radical. Dans un anneau réduit les idéaux premiers associés à l'idéal nul sont par conséquent tous isolés et ce sont les éléments minimaux de $\mathrm{spec}(A)$ (voir la remarque A.1.19). On obtient alors la propriété suivante lorsqu'on passe à l'anneau total des fractions de A.

Proposition A.2.32 *Soit A un anneau noethérien réduit. Alors le spectre de $\mathrm{fr}(A)$ est en bijection avec l'ensemble des idéaux premiers associés à l'idéal nul dans A par les opérations d'extension et de contraction entre A et $\mathrm{fr}(A)$. De plus, tout idéal $\mathcal{P} \in \mathrm{spec}(\mathrm{fr}(A))$ est à la fois un idéal premier minimal et maximal dans $\mathrm{spec}(\mathrm{fr}(A))$.*

Preuve. On pose $S = \mathbf{reg}(A)$. Considérons un idéal premier $\mathcal{P}'$ de $\mathrm{fr}(A) = S^{-1}A$. D'après la proposition A.2.21, c'est l'extension d'un idéal $\mathcal{P}$ de A tel que $S \cap \mathcal{P} = \emptyset$. Soit $\cap_{j=1}^{s}\mathcal{P}_j$ une décomposition primaire de l'idéal nul de A. On a donc $\mathcal{P} \subseteq \cup_{j=1}^{s}\mathcal{P}_j$. D'après la proposition A.1.1, l'idéal $\mathcal{P}$ est inclus dans l'un des $\mathcal{P}_j$, d'où $\mathcal{P} = \mathcal{P}_j$ puisque $\mathcal{P}_j$ est un élément minimal de $\mathrm{spec}(A)$. On a ainsi prouvé que $\mathrm{spec}(S^{-1}A) = \{\mathcal{P}_j^e, j \in [1,s]\}$. De plus, puisque les $\mathcal{P}_j$ sont en même temps minimaux et maximaux dans l'ensemble $\mathsf{ass}(0_A)$, on déduit la même chose pour les éléments de $\mathrm{spec}(S^{-1}A)$. □

Proposition A.2.33 *Soit A un anneau noethérien réduit et $\mathcal{P}$ un idéal premier associé à $\langle 0\rangle_A$. On note $\mathcal{P}^e$ l'extension de $\mathcal{P}$ dans $\mathrm{fr}(A)$. Alors*

$$\mathrm{fr}(A)/\mathcal{P}^e \;\simeq\; \mathrm{fr}(A/\mathcal{P})\ .$$

Preuve. On pose $S = \mathbf{reg}(A)$. Considérons l'homomorphisme canonique λ de $S^{-1}A$ dans $S^{-1}A_{\mathcal{P}^e}$. Il résulte de la proposition A.2.31 l'idéal $\mathcal{P}^e$ est une composante primaire de l'idéal nul de $S^{-1}A$; on vérifie alors aisément avec la proposition A.2.22 que $\mathrm{Ker}(\lambda) = \mathcal{P}^e$. De plus, l'idéal $\mathcal{P}^e$ est un idéal premier maximal selon la proposition A.2.32. Le lemme A.2.29 s'applique donc pour λ, d'où

$$(S^{-1}A)/\mathcal{P}^e \;\simeq\; (S^{-1}A)_{\mathcal{P}^e}\ .$$

Il résulte alors de l'isomorphisme de la proposition A.2.26 que

$$(S^{-1}A)/\mathcal{P}^e \;\simeq\; A_{\mathcal{P}}\ . \tag{A.5}$$

Remarquons que l'anneau $A_{\mathcal{P}}$ est un corps puisque $\mathcal{P}^e$ est un idéal maximal. L'idéal maximal $\mathcal{P}A_{\mathcal{P}}$ est un idéal propre de $A_{\mathcal{P}}$ donc forcément réduit à 0. On en déduit avec le lemme A.2.27 que

$$A_{\mathcal{P}} \;\simeq\; \mathrm{fr}(A/\mathcal{P})\ ,$$

ce qui établit avec (A.5) l'isomorphisme demandé. □

Proposition A.2.34 *Soit A un anneau noethérien réduit. Alors son anneau total des fractions* $\mathrm{fr}(A)$ *est un produit fini de corps. De plus, on a*

$$\mathrm{fr}(A) \simeq \mathrm{fr}(A/\mathcal{P}_1) \times \ldots \times \mathrm{fr}(A/\mathcal{P}_s)$$

où les $\mathcal{P}_i$ sont les idéaux premiers associés à l'idéal nul de A.

Preuve. En notant $S = \mathbf{reg}(A)$ et $\mathcal{P}_i^e$ l'extension de $\mathcal{P}_i$ dans $\mathrm{fr}(A)$, on a

$$\mathrm{fr}(A) = S^{-1}A = (S^{-1}A)/(\cap_{i=1}^s \mathcal{P}_i^e) .$$

Puisque selon la proposition A.2.32 les $\mathcal{P}_i$ sont maximaux, le théorème des restes chinois (proposition A.1.2) entraîne

$$\mathrm{fr}(A) = S^{-1}A/\mathcal{P}_1^e \times \ldots \times S^{-1}A/\mathcal{P}_s^e .$$

On a ainsi prouvé que $\mathrm{fr}(A)$ est un produit de corps. Quant à l'isomorphisme, c'est une conséquence de la proposition A.2.33. □

A.3 Notion de hauteur

Nous rappelons la notion de hauteur d'un idéal premier puis d'un idéal quelconque pour les anneaux noethériens. L'étude de ces concepts est à la base de la théorie de la dimension (chap. 3 de [Ser65]). Nous montrons dans le chapitre 4 que les ensembles triangulaires présentent des propriétés importantes liées à cette notion. En prenant en compte ces propriétés, il est en effet possible d'éliminer des branches de calculs inutiles dans les algorithmes que nous présentons dans le chapitre 5 et de permettre ainsi la décomposition de systèmes algébriques que nous n'avions pu effectuer avec nos premières implantations.

Définition A.3.1 *Soit A un anneau commutatif. On appelle* chaîne d'idéaux premiers *dans A toute suite finie d'idéaux premiers de A strictement croissante pour l'inclusion*

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_m .$$

L'entier m est appelé longueur *de la chaîne.*

La hauteur *d'un idéal premier $\mathcal{P}$ est la longueur maximale (éventuellement infinie) des chaînes d'idéaux premiers $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_m$ telles que $\mathcal{P}_m = \mathcal{P}$. On la note* $\mathsf{ht}(\mathcal{P})$.

La dimension *de l'anneau A est la borne supérieure des longueurs des chaînes d'idéaux premiers dans A. La dimension d'un idéal I correspond à la dimension de l'anneau quotient A/I.*

Remarque A.3.2 Il est clair que pour tous idéaux premiers $\mathcal{P}_1$ et $\mathcal{P}_2$ de A tels que $\mathcal{P}_1 \subset \mathcal{P}_2$, on a : $\mathsf{ht}(\mathcal{P}_1) \leq \mathsf{ht}(\mathcal{P}_2)$ et si les hauteurs sont égales alors $\mathcal{P}_1 = \mathcal{P}_2$.

Dans les anneaux noethériens, on a le théorème suivant très important qui permet de borner la hauteur des idéaux premiers associés à un idéal. Le lecteur pourra se référer à [SZ67] (p. 240) par exemple.

Théorème A.3.3 *Soit A un anneau noethérien et I un idéal propre de A. Si I admet une base composée de m éléments, alors pour tout idéal premier $\mathcal{P}$ isolé associé à I on a $\mathsf{ht}(\mathcal{P}) \leq m$.*

Il en résulte que tout idéal premier dans un anneau noethérien est de hauteur finie. On peut alors généraliser la notion de hauteur à des idéaux quelconques d'un anneau noethérien.

Définition A.3.4 *Soit I un idéal d'un anneau noethérien A. On définit la hauteur de I par*

$$\mathsf{ht}(I) = \min\{\,\mathsf{ht}(\mathcal{P}),\ \mathcal{P} \in \mathrm{spec}(A) \text{ et } \mathrm{I} \subset \mathcal{P}\,\}\ .$$

On vérifie aisément que $\mathsf{ht}(I) = \min\,\{\mathsf{ht}(\mathcal{P}),\ \mathcal{P} \in \mathsf{ass}(I)\}$, ce qui amène à la définition suivante.

Définition A.3.5 *Un idéal I d'un anneau noethérien A est dit* équidimensionnel *si tous les idéaux premiers isolés de I sont de même hauteur. L'idéal I est dit* purement équidimensionnel *si tous ses idéaux premiers associés sont de même hauteur.*

Un idéal I est donc purement équidimensionnel si et seulement si il est équidimensionnel et que toutes ses composantes primaires sont isolées. Dans l'anneau de polynômes $\mathbf{P}_n$, on définit une notion plus forte comme suit.

Définition A.3.6 *Soit I un idéal de $\mathbf{P}_n$. On dit que I est* fortement équidimensionnel *si pour tout $i \in [1, n]$ et pour tout $\mathcal{P}$ et tout $\mathcal{Q} \in \mathsf{ass}(I)$, on a $\mathsf{ht}(\mathcal{P} \cap \mathbf{P}_i) = \mathsf{ht}(\mathcal{Q} \cap \mathbf{P}_i)$*

La propriété importante suivante est une conséquence immédiate de la remarque A.3.2.

Proposition A.3.7 *Soit I un idéal d'un anneau noethérien A. Si I est purement équidimensionnel alors les composantes primaires de I sont toutes isolées.*

Pour toute partie multiplicative S d'un anneau noethérien A, la hauteur d'un idéal premier de $S^{-1}A$ est finie puisque $S^{-1}A$ est noethérien. Elle est même égale à celle de son contracté dans A ainsi qu'il est précisé ci-dessous.

Proposition A.3.8 *Soit A un anneau noethérien et S une partie multiplicative de A. Soit $\mathcal{P}$ un idéal premier de A tel que $\mathcal{P} \cap S = \emptyset$ et $\mathcal{P}^e$ son extension dans $S^{-1}A$. Alors on a $\mathsf{ht}(\mathcal{P}) = \mathsf{ht}(\mathcal{P}^e)$.*

Preuve. Soit $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_m$ une chaîne d'idéaux premiers de A telle que $\mathcal{P}_m = \mathcal{P}$. Pour tout $i \in [0, m]$ on a $\mathcal{P}_i \cap S = \emptyset$, donc

$$\mathcal{P}_0^e \subset \mathcal{P}_1^e \subset \ldots \subset \mathcal{P}_m^e$$

est une chaîne d'idéaux premiers de $S^{-1}A$ d'après la proposition A.2.21. On a par conséquent $\mathsf{ht}(\mathcal{P}^e) \geq \mathsf{ht}(\mathcal{P})$. De la même manière, à partir de toute chaîne d'idéaux premiers de $S^{-1}A$ d'extrémité $\mathcal{P}^e$, on obtient par contraction une chaîne d'idéaux premiers de A d'extrémité $\mathcal{P}^{ec}$. Puisque $\mathcal{P}^{ec} = \mathcal{P}$ par la proposition A.2.17, on en déduit alors $\mathsf{ht}(\mathcal{P}) \geq \mathsf{ht}(\mathcal{P}^e)$. □

A.4 Suites régulières

On rappelle la notion de suites régulières dans un anneau A et quelques-unes de leurs propriétés. On trouve aussi dans la littérature le terme de A-*suite* pour suite régulière ([Jeb93]). Pour plus de détails et sur la notion plus générale de suite régulière sur un A-module, on pourra consulter à [Kap74]. Dans les anneaux de Macaulay (voir définition A.4.10) cette notion permet de caractériser la hauteur d'un idéal premier. En utilisant le fait que $\mathbf{P}_n$ est un anneau de Macaulay, nous montrerons que les ensembles triangulaires de polynômes induisent des suites régulières dans un anneau de fractions; c'est ainsi que nous dégagerons le résultat d'équidimensionnalité du théorème 4.1.4.

Définition A.4.1 *Une suite $a_1, \ldots, a_s$ d'un anneau A est une* suite régulière *si :*

(i) $\langle a_1, \ldots, a_s \rangle \neq A$,

(ii) pour tout $i \in [1, s]$, $a_i \notin \mathbf{Div}(A/\langle a_1, \ldots, a_i \rangle)$.

Le nombre d'éléments s de la suite régulière est appelé longueur *de la suite.*

Exemple A.4.2 Si A est l'anneau de polynômes $k[x_1, \ldots, x_n]$ alors $x_1, \ldots, x_n$ est une suite régulière de A.

La proposition suivante se déduit facilement du second théorème d'isomorphisme.

Proposition A.4.3 *Soit $a_1, \ldots, a_s$ des éléments d'un anneau A. Les affirmations suivantes sont équivalentes :*

(i) $a_1, \ldots, a_s$ est une suite régulière de A,

(ii) $a_1, \ldots, a_r$ est une suite régulière de A et $a_{r+1}, \ldots, a_s$ est une suite régulière de l'anneau quotient $A/\langle a_1, \ldots, a_r \rangle$.

Proposition A.4.4 *Soit a_1, a_2 une suite régulière d'un anneau A. Alors* $a_1 \notin \mathbf{Div}(A/\langle a_2 \rangle)$.

Preuve. Supposons qu'il existe $u \in A$ tel que ua_1 soit nul dans $A/\langle a_2 \rangle$. Il existe $v \in A$ tel que $ua_1 = va_2$. Par hypothèse a_2 n'est pas diviseur de zéro dans $A/\langle a_1 \rangle$ donc $v \in \langle a_1 \rangle$. Par conséquent il existe $w \in A$ tel que $ua_1 = wa_1a_2$. Puisque $a_1 \notin \mathbf{Div}(A)$ on obtient $u = wa_2$ donc u est nul dans $A/\langle a_2 \rangle$, ce qui prouve l'assertion. □

Des propositions A.4.3 et A.4.4, on déduit facilement la proposition suivante.

Proposition A.4.5 *Soit $a_1, \ldots, a_s$ une suite régulière de A. Alors la suite $a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_s$ obtenue en permutant les termes de rang i et de rang $i+1$, est une suite régulière de A si et seulement si* $a_{i+1} \notin \mathbf{Div}(A/\langle a_1, \ldots, a_{i-1} \rangle)$.

Corollaire A.4.6 *Soit A un anneau et $a_1, \ldots, a_s$ une suite régulière de A. Soit b un élément de A tel que $a_1, \ldots, a_i, b, a_{i+1}, \ldots, a_s$ est une suite régulière de A. Alors $a_1, \ldots, a_s, b$ est une suite régulière de A.*

Preuve. Il suffit d'utiliser la proposition A.4.5 pour permuter b avec a_{i+1}, puis avec a_{i+2} et ainsi de suite jusqu'à a_s. □

En notant $I_j = \langle a_1, \ldots, a_i \rangle$, on vérifie facilement que $I_1, \ldots, I_s$ forme une suite strictement croissante d'idéaux de A. Dans un anneau noethérien les suites régulières sont par conséquent finies et on peut ainsi parler de suites régulières maximales. On suppose pour la fin de cette section que A est noethérien.

Lemme A.4.7 *Soit A un anneau noethérien et I un idéal de A. Une suite régulière $a_1, \ldots, a_s$ contenue dans I est maximale si et seulement si $I \subset \mathbf{Div}(A/\langle a_1, \ldots, a_s \rangle)$.*

Preuve. D'après le corollaire A.4.6, la suite $a_1, \ldots, a_s$ est maximale dans I si et seulement pour tout $b \in I$ la suite $a_1, \ldots, a_s, b$ n'est pas une suite régulière, ce qui revient à dire que b est diviseur de zéro dans $A/\langle a_1, \ldots, a_s \rangle$. □

Les suites régulières présentent la caractéristique majeure suivante :

Théorème A.4.8 *Soit I un idéal propre d'anneau noethérien A. Alors deux suites régulières maximales quelconques de A contenues dans I sont de même longueur.*

Preuve. Il revient au même de montrer que si $a_1, \ldots, a_s$ est une suite régulière maximale dans I et $b1, \ldots, b_s$ une suite régulière contenue dans I, alors $b_1, \ldots, b_s$ est maximale. Cela s'effectue par récurrence.

Soit $s = 1$. Puisque a_1 est maximale l'idéal I est inclus dans la réunion des idéaux premiers associés à $\langle a_1 \rangle$, donc dans l'un d'eux (proposition A.1.1) qu'on note $\mathcal{P}$. D'après la proposition A.1.22 il existe $u \in A$ tel que $\mathcal{P} = \langle a_1 \rangle : u$. On en déduit avec le lemme A.4.7que $Iu \subset \langle a_1 \rangle$. Il existe donc $v \in A$ tel que $a_2 u = a_1 v$. Plus généralement, pour $a \in I$ il existe $w \in A$ tel que $au = a_1 w$. Les deux dernières relations entraînent alors $aa_1 v = a_2 au = a_2 a_1 w$. Puisque par hypothèse a_1 est un élément régulier de A, on en déduit que $Iv \subset \langle a_2 \rangle$. On affirme de plus que $v \notin \langle a_2 \rangle$. En effet, dans le cas contraire on déduit facilement de la relation $a_2 u = a_1 v$ que u appartient à $\langle a_1 \rangle$, ce qui est impossible. On a ainsi montré que I est composé de diviseurs de zéro dans $A/\langle a_2 \rangle$. La suite a_2 est donc maximale dans I.

Pour $n > 1$, on pose $B_i = A/\langle a_1, \ldots, a_i \rangle$ et $C_i = A/\langle b_1, \ldots, b_i \rangle$ pour $i \in [1, n-1]$ et $B_0 = C_0 = A$. Il résulte du lemme A.4.7 que $I \not\subset \mathbf{Div}(B_i)$ et $I \not\subset \mathbf{Div}(C_i)$. Les ensembles $\mathbf{Div}(B_i)$ et $\mathbf{Div}(C_i)$ sont des réunions d'idéaux premiers. La proposition A.1.1 entraîne alors qu'il existe un élément c de I tel que c n'appartient à aucun des $\mathbf{Div}(B_i)$ et $\mathbf{Div}(C_i)$. Comme par hypothèse a_s est une suite régulière maximale de B_{s-1}, la suite c l'est aussi d'après le cas $s = 1$. En utilisant la proposition A.4.5, on peut permuter successivement c avec $a_{s-1}, \ldots, a_1$. On obtient ainsi une suite régulière $c, a_1, \ldots, a_{s-1}$ qui est clairement maximale dans I. De même $c, b_1, \ldots, b_{s-1}$ est une suite régulière de I. Sur l'anneau quotient $A/\langle c \rangle$ on dispose donc des suites régulières $a_1, \ldots, a_{n-1}$ et $b_1, \ldots, b_{s-1}$, la première étant maximale. L'hypothèse de récurrence implique que $b_1, \ldots, b_{s-1}$ est maximale sur $A/\langle c \rangle$. Il en découle que $c, b_1, \ldots, b_{s-1}$, puis $b_1, \ldots, b_{s-1}, c$ sont maximales sur A. En appliquant de nouveau le cas $s = 1$ sur l'anneau $A/\langle b_1, \ldots, b_{s-1} \rangle$, on conclut que $b_1, \ldots, b_s$ est maximale sur A. □

Lemme A.4.9 *Soit $a_1, \dots, a_s$ une suite régulière dans un anneau noethérien A et I l'idéal engendré par les éléments $a_1, \dots, a_s$. Pour tout idéal premier $\mathcal{P}$ associé à I la suite $a_1, \dots, a_s$ est une suite régulière maximale dans $\mathcal{P}$.*

Preuve. Soit b un élément de A tel que $a_1, \dots, a_i, b, a_{i+1}, \dots, a_s$ est une suite régulière de A. Alors $a_1, \dots, a_s, b$ est une suite régulière de A d'après le corollaire A.4.6. Par conséquent b n'est pas un diviseur de zéro dans A/I. On en conclut que $b \notin \mathcal{P}$, d'où le résultat. □

L'intérêt des suites régulières dans certains anneaux apparaît plus précisément ci-dessous.

Définition A.4.10 *On dit qu'un anneau noethérien A est un* anneau de Macaulay *(ou* anneau de Cohen-Macaulay *si pour tout idéal maximal $\mathcal{M}$ de A, la longueur commune des suites régulières maximales de $\mathcal{M}$ est égale à la hauteur de $\mathcal{M}$.*

On montre alors que dans un anneau de Macaulay, cette correspondance vaut pour tout idéal, autrement dit la longueur commune des suites régulières maximales contenues dans un idéal propre I est égale à $\mathsf{ht}(I)$ (voir le théorème 136 p. 97 de [Kap74]). D'autre part, le passage à un anneau de fractions conserve la propriété de Macaulay comme le rappelle la proposition suivante.

Proposition A.4.11 *Si A est un anneau de Macaulay et S une partie multiplicative de A, alors $S^{-1}A$ est un anneau de Macaulay.*

Preuve. voir [Kap74] page 100. □

Rappelons qu'un anneau de polynômes à plusieurs variables sur un corps est un anneau de Macaulay (voir [Kap74] p.110). Ce fait et la proposition A.4.11 permettent d'exploiter les propriétés ci-dessous dans le chapitre consacré aux ensembles triangulaires. Le théorème A.4.12 ci-dessous est une conséquence directe dans les anneaux de Macaulay du lemme A.4.9. Les corollaires A.4.13 et A.4.14 en résultent alors immédiatement (avec la remarque A.3.2).

Théorème A.4.12 *Soit A un anneau de Macaulay. Soit $a_1, \dots, a_s$ une suite régulière dans A et I l'idéal engendré par $a_1, \dots, a_s$. Alors pour tout idéal premier $\mathcal{P}$ associé à I on a* $\mathsf{ht}(\mathcal{P}) = s$.

Corollaire A.4.13 *Soit A un anneau de Macaulay et I un idéal de A engendré par une suite régulière. Alors les idéaux premiers associés à I sont tous isolés.*

Corollaire A.4.14 *Si I est un idéal engendré par une suite régulière dans un anneau de Macaulay alors I est purement équidimensionnel.*

Annexe B

Bases de Gröbner

Nous rappelons quelques éléments de la théorie des bases de Gröbner qui est omniprésente en calcul formel pour les problèmes traitant d'idéaux. Cette théorie a été développée principalement depuis les travaux de B. Buchberger qui a présenté dans [Buc65] un premier algorithme pour calculer des bases de Gröbner . Il fournit un ensemble canonique de générateurs d'un idéal relativement à un ordre donné, qui permet de tester l'appartenance d'un polynôme à l'idéal.

Cette théorie est basée sur une notion d'ordre sur les monômes unitaires de $\mathbf{P}_n$ grâce à laquelle on peut généraliser l'algorithme de la division eucidienne pour les polynômes à plusieurs variables. Rappelons que nous considérons nos variables ordonnées comme suit :

$$x_1 < x_2 < \ldots < x_n \; .$$

Définition B.0.15 *On note* $\mathbf{M_n}$ *l'ensemble* $\{x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{N}\}$ *des monômes (unitaires) de* $\mathbf{P}_n$ *Une relation d'ordre total "<" sur l'ensemble* $\mathbf{M_n}$ *est dite un* ordre admissible *si pour tous* $(\alpha_1, \ldots, \alpha_n)$ *et* $({}_beta_1, \ldots, \beta_n)$ *dans* $\mathbb{N}^n$ *les propriétés suivantes sont vérifiées :*

(i) $1 < x_1^{\alpha_1} \ldots x_n^{\alpha_n}$,

(ii) $x_1^{\alpha_1} \ldots x_n^{\alpha_n} < x_1^{\beta_1} \ldots x_n^{\beta_n} \Rightarrow \forall (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}^n \; x_1^{\alpha_1+\gamma_1} \ldots x_n^{\alpha_n+\gamma_n} < x_1^{\beta_1+\gamma_1} \ldots x_n^{\beta_n+\gamma_n}$.

Il existe divers ordres admissibles. Nous nous intéresserons plus particulièrement à l'ordre *lexicographique pur* qu'on peut rapprocher de la vision récursive des polynômes utilisée dans la théorie des ensembles triangulaires. Les bases de Gröbner lexicographiques bénéficient de propriétés fondamentales pour calculer un idéal d'élimination. Mentionnons que l'ordre du degré lexicographique inverse se révèle très efficace pour obtenir une base de Gröbner en pratique. Des ordres *par blocs* sont utilisés par exemple pour calculer des idéaux d'élimination plus facilement qu'avec l'ordre lexicographique.

Définition B.0.16 *L'ordre* lexicographique (pur)*, noté* $\prec_{lex}$*, est défini par :*

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec_{lex} x_1^{\beta_1} \ldots x_n^{\beta_n} \;\Leftrightarrow\; \exists \ell \in [1, n], \begin{cases} \alpha_j = \beta_j & \forall j \in [\ell+1, n] \\ \alpha_\ell < \beta_\ell \end{cases}$$

Nous supposons maintenant qu'un ordre admissible $<$ est fixé et omettons généralement la référence à cet ordre.

Définition B.0.17 *Soit p un polynôme de $\mathbf{P}_n$. L'élément maximal pour $<$ de l'ensemble des monômes de p est appelé monôme de tête de p et noté $\mathsf{lm}(p)$. Le coefficient de $\mathsf{lm}(p)$ dans p est appelé coefficient de tête de p. On le désigne par $\mathsf{lc}(p)$. Le terme de tête de p, noté $\mathsf{lt}(p)$ est défini par $\mathsf{lt}(p) = \mathsf{lc}(p)\,\mathsf{lm}(p)$. Pour un sous-ensemble G de $\mathbf{P}_n$ on note $\mathsf{lt}(G)$ l'idéal engendré par $\{\mathsf{lt}(g) \mid g \in G\}$.*

Définition B.0.18 *Un sous-ensemble fini $G = \{g_1, \ldots, g_r\}$ d'un idéal $I \subseteq \mathbf{P}_n$ est une* base de Gröbner *de I si*

$$\mathsf{lt}(G) = \mathsf{lt}(I) \ .$$

On dit qu'une base de Gröbner G est minimale *si les conditions suivantes sont vérifiées :*

(i) $\mathsf{lc}(g) = 1$ pour tout $g \in G$,

(ii) pour tout $g \in G$ on a $\mathsf{lt}(g) \notin \mathsf{lt}(G \setminus \{g\})$.

Théorème B.0.19 *Tout idéal de $\mathbf{P}_n$ admet une unique base de Gröbner minimale par rapport à l'ordre $<$.*

Preuve. Voir [BW93] p. 209. □

L'idéal $\mathsf{lt}(I)$ est un idéal *monomial*, c'est-à-dire engendré par des monômes. Il vérifie alors la propriété suivante, qui se déduit du lemme 2 p. 69 de [CLO92].

Proposition B.0.20 *Soit I un idéal de $\mathbf{P}_n$ engendré par une base de Gröbner G et $p \in \mathbf{P}_n$. Si p appartient à I alors il existe $g \in G$ tel que $\mathsf{lm}(g)$ divise $\mathsf{lm}(p)$.*

La proposition ci-dessous montre que les bases de Gröbner lexicographiques permettent de faire de l'élimination. Rappelons que si I est un idéal de $\mathbf{P}_n$, on dit qu'un idéal J de $\mathbf{P}_i$ est un *idéal d'élimination* de I si $J = I \cap \mathbf{P}_i$.

Proposition B.0.21 *Soit I un idéal de $\mathbf{P}_n$ et G une base de Gröbner de I pour l'ordre lexicographique. Pout tout $i \in [1, n]$ l'ensemble $G_i = G \cap \mathbf{P}_i$ est une base de Gröbner lexicographique de l'idéal d'élimination $I \cap \mathbf{P}_i$. On a en particulier*

$$I \cap \mathbf{P}_i = \langle G_i \rangle \ .$$

Index

Bibliographie

[Alb96] A. Albouy. The symmetric central configurations of four equal masses. *Contemporary Math.*, pages 131–135, 1996.

[ALM99] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 1999. À paraître.

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Addison Wesley, 1969.

[AM97] P. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems : a comparison of four methods. Rapport technique LIP6/009, Université Paris 6, 1997.

[AM99] P. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems : a comparative implementation of four methods. *Journal of Symbolic Computation*, 1999. À paraître.

[Arn76] J.M. Arnaudiès. Sur la résolution explicite des équations de degré 5, quand elles sont résolubles par radicaux. *Bull. Sc. Math.* 2^e *série*, 100:241–254, 1976.

[AV96] J.M. Arnaudiès and A. Valibouze. Lagrange resolvents. In A. Cohen and M.F. Roy, editors, *Special issue of MEGA'96*, pages 23–40. Journal of Pure and Applied Algebra, 1996.

[AV98] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. Presenté à MEGA'98 et soumis à Journal of Pure and Applied Algebra, 1998.

[BDI+94] P.A. Broadbery, S.S. Dooley, P. Iglio, S.C. Morisson, J.M. Steinbach, R.S. Sutor, and S. M. Watt. AXIOM *Library Compiler User Guide*. NAG, Oxford, United Kingdom, 1994.

[BGK86] W. Boege, R. Gebauer, and H. Kredel. Some examples for solving systems of algebraic equations by calculating Gröbner bases. *Journal of Symbolic Computation*, 2:83–98, 1986.

[Bjö85] G. Björk. Functions of modulus one on $\mathbf{Z}_p$ whose Fourier transforms have constant modulus. In *Proceedings of Alfred Haar Memorial Conference, Budapest, Colloquia Mathematica Societatis János Bolyai*, 49, pages 193–197, 1985.

[BLOP95] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In *Proc. ISSAC'95*, pages 158–166, Montréal, Canada, 1995.

[BLOP97] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. Rapport technique IT-306, Université de Lille I, 1997. soumis à Journal of Symbolic Computation.

[Bou61a] N. Bourbaki. *Algèbre commutative, chap. 2, Localisation*. Hermann, 1961.

[Bou61b] N. Bourbaki. *Algèbre commutative, chap. 4, Idéaux premiers associés et décomposition primaire*. Hermann, 1961.

[Bro86] M. Bronstein. Gsolve: a faster algorithm for solving systems of algebraic equations. In B.W. Char, editor, *Proc. SYMSAC'86*, pages 247–249, Waterloo, 1986. ACM Press.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Thèse de doctorat, Innsbruck, Autriche, 1965.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[CG86] S.R. Czapor and K.O. Geddes. On implementing Buchberger's algorithm for Gröbner bases. In *Proc. SYMSAC'86*, pages 425–440. Waterloo, B.W. Char, 1986.

[CG90] S.C. Chou and X.S. Gao. Ritt-Wu's decomposition algorithm and geometry theorem proving. In *Proc. CADE-10*, volume 449 of *Lecture Notes in Computer Science*, pages 207–220. Kaiserslautern, Germany, Springer Verlag, 1990.

[CG91] S.C. Chou and X.S. Gao. Computations with parametric equations. In *Proc. ISAAC'91*, pages 122–127, Bonn, Germany, 1991.

[CG92] S.C. Chou and X.S. Gao. Solving parametric algebraic systems. In *Proc. ISAAC'92*, pages 335–341, Berkeley, California, 1992. ACM Press.

[CG93] S.C. Chou and X.S. Gao. On the dimension of an arbitrary ascending chain. *Chinese Bull. of Sci.*, 38:799–804, 1993.

[Cho88] S.C. Chou. *Mechanical Geometry Theorem Proving*. Reidel, Dordrecht, 1988.

[CKM97] S. Collart, M. Kalkbrener, and D. Mall. Converting bases with the Gröbner walk. *Journal of Symbolic Computation*, 24(3,4):465–470, 1997.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Col95] A. Colin. Formal computation of Galois groups with relative resolvents. In G. Cohen, M. Giusti, and T. Mora, editors, *Proc. AAECC'11*, volume 948 of *Lecture Notes in Computer Science*, pages 169–182, Paris, France, 1995. Springer.

[Com92] European Commission. *PoSSo - Polynomial System Solving Research Project.* Esprit Scheme Project No. 6846, 1992.

[CP97] J.J. Cannon and C. Playoust. *An Introduction to Algebraic Programming with* MAGMA. University of Sydney, 1997.

[DD85] C. Discrescenzo and D. Duval. Algebraic computations on algebraic numbers. In *Computers and computing*, pages 54–61. Masson and Wiley, Paris, 1985.

[DDD85] J. Della Dora, C. Discrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *Proc. EUROCAL 85 Vol. 2*, volume 204 of *Lecture Notes in Computer Science*, pages 289–290. Springer-Verlag, 1985.

[DT89] L. Donati and C. Traverso. Experimenting the Gröbner basis algorithm with the alpi system. In *Proc. ISAAC'89*, pages 192–198. ACM Press, 1989.

[Duc96] L. Ducos. Algorithme de Bareiss, algorithme des sous-résultants. *Theoritical Informatics and Application*, 304:319–347, 1996.

[Duc97] L. Ducos. *Effectivité en théorie de Galois. Sous-résultants.* Thèse de doctorat, Université de Limoges, 1997.

[Duv87] D. Duval. *Questions Relatives au Calcul Formel avec des Nombres Algébriques.* Université de Grenoble, 1987. Thèse d'Etat.

[Eic96] Y. Eichenlaub. *Problèmes effectifs de théorie de Galois en degrés 8 à 11.* Thèse de doctorat, Université de Bordeaux 1, 1996.

[Fau94] J.C. Faugère. *Résolution des systèmes d'équations algébriques.* Thèse de doctorat, Université Paris 6, 1994.

[Fau97] J.C. Faugère. A new efficient algorithm for computing Gröbner basis (F4). Task 3.3.2.1 Frisco report, 1997.

[Fau99] J.C. Faugère. A new efficient algorithm for computing gröbner bases (F4). *Journal of Pure and Applied Algebra*, 2148, 1999.

[FdSMR96] J.C. Faugère, F. Moreau de Saint-Martin, and F. Rouiller. Design of nonseparable bidimensional wavelets and filter banks using Gröbner bases techniques. *IEEE SP Trans. Signal Processing*, 46, 1996. Special Issue on Theory and Applications of Filter Banks and Wawelets.

[FGLM93] 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.

[Gia87] P. Gianni. Properties of Gröbner bases under specializations. *Lecture Notes in Computer Science*, 378:293–297, 1987.

[Gir87] K. Girstmair. On invariant polynomials and their application in field theory. *Math. of Comp.*, 48(178):781–797, 1987.

[GM90] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proc. MEGA'90, Progress in Mathematics*, volume 94, pages 119–142, Livorno, Italy, 1990. Birkhäuser.

[GM91] G. Gallo and B. Mishra. Wu-Ritt characteristic sets and their complexity. In J.E. Goodman, R. Pollack and W. Steiger, editor, *Discrete and Computational Geometry: Papers from the DIMACS Special Year*, volume 6 of *Dimacs Series in Discrete Mathematics and Theoretical Computer Science*, pages 111–136. American Mathematical Society and Association for Computing Machinery, 1991.

[GMN+91] A. Giovinni, T. Mora, G. Niesi, L. Robbiano, and C. Traverso. "One sugar cube, please" or selection strategies in the Buchberger algorithm. In *Proc. ISSAC'91*, pages 49–54. ACM Press, 1991.

[Gom92] T. Gomez Diaz. *Quelques applications de l'évaluation dynamique.* Thèse de doctorat, Université de Limoges, 1992.

[GR91] M. Gonzáles-López and T. Recio. The romin inverse geometric model and the dynamic evaluation method. In A.M. Cohen, editor, *Proceedings of the 1991 SCAFI seminar, Computer Algebra in Industry.* Wiley, 1991.

[Grä95] H.G. Gräbe. Triangular systems and factorized Gröbner bases. In G. Cohen, M. Giusti, and T. Mora, editors, *Proc. AAECC'11*, volume 948 of *Lecture Notes in Computer Science*, pages 248–261, Paris, France, 1995. Springer.

[Hen56] P. Henrici. Automatic computations with power series. *JACM*, 3(1):10–15, 1956.

[Huy86] D.T. Huynh. A superexponential lower bound for Gröbner bases and Church Rosser commutative Thue systems. *Information and Control*, 68:196–206, 1986.

[Jeb93] A. Jebli. *Théorie de la dimension.* ScientifikA, 1993.

[JS92] R.D. Jenks and R.S. Sutor. *AXIOM, The Scientific Computation System.* Springer-Verlag, 1992.

[Kal87] M. Kalkbrener. Solving systems of algebraic equations by using Gröbner basis. *Lecture Notes in Computer Science*, 378:282–292, 1987.

[Kal91] M. Kalkbrener. *Three contributions to elimination theory.* Thèse de doctorat, Johannes Kepler University, Linz, 1991.

[Kal93] M. Kalkbrener. A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15:143–167, 1993.

[Kal95] M. Kalkbrener. Algorithmic properties of polynomial rings. Dep. of math., Swiss Federal Institute of Technology, Zurich, 1995. Thèse d'habilitation.

[Kal98] M. Kalkbrener. Algorithmic properties of polynomial rings. *Journal of Symbolic Computation*, 26(5):525–581, 1998.

[Kap74] I. Kaplansky. *Commutative Rings*. The University of Chicago Press, 1974.

[Kot98] I. Kotsireas. *Algorithmes de résolution de systèmes polynomiaux : application aux configurations centrales du problème des n corps en mécanique céleste*. Thèse de doctorat, Université Paris 6, 1998.

[Lag70] J.L. Lagrange. Réflexions sur la résolution algébrique des équations. Mémoires de l'Académie de Berlin, 1770.

[Laz91a] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discr. App. Math*, 33:147–160, 1991.

[Laz91b] D. Lazard. Systems of algebraic equations (algorithms and complexity). In D. Eisenbud and L. Robbiano, editors, *Cortona proceedings*. Cambridge University Press, 1991.

[Laz92] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 15:117–132, 1992.

[Leh97] F. Lehobey. Resolvent computations by resultants without extraneous powers. In Wolfgang Küchlin, editor, *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pages 85–92. ACM, 1997.

[Li95] Z. Li. An implementation of the characteristic set method for solving algebraic equations. In *Proc. PoSSo Workshop on Software*, pages 107–122, 1995.

[Liu89] Z.J. Liu. An algorithm on finding all isolated zeros of polynomial equations. *MM Research Preprints*, 4(63-76), 1989.

[Loo82] R. Loos. Generalized polynomial remainder sequences. In *Symbolic and Algebraic Computation*, pages 115–137. Spinger-Verlag, 1982.

[MM82] E.W. Mayr and A.R. Meyer. The complexity of the word problems for commutative semigroups and ideals. *Advances in Mathematics*, 46:305–329, 1982.

[Möl93] H.M. Möller. On decomposing systems of polynomial equations with finitely many solutions. *Applicable Algebra in Engineering, Communications and Computing*, 4:217–230, 1993.

[Mor97] M. Moreno Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques*. Thèse de doctorat, Université Paris 6, 1997.

[MR95] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In G. Cohen, M. Giusti, and T. Mora, editors, *Proc. AAECC'11*, volume 948 of *Lecture Notes in Computer Science*, pages 365–382, Paris, France, 1995. Springer.

[MS85] J. McKay and L. Soicher. Computing Galois groups over the rationals. *Journal of Number Theory*, 20:273–281, 1985.

[Rit32] J.F. Ritt. *Differential equations from an algebraic standpoint*, volume 14. American Mathematical Society Colloquium Publications, New York, 1932.

[Rit66] J.F. Ritt. *Differential Algebra.* Dover Publications, Inc., New York, 1966.

[Rou96] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux.* Thèse de doctorat, Université de Rennes I, 1996.

[Rou98] F. Rouillier. Solving zero-dimensional polynomial systems through the Rational Univariate Representation. Rapport de recherche INRIA 3426, 1998.

[RV99] N. Rennert and A. Valibouze. Calcul de résolvantes avec les modules de Cauchy. *Experimental Mathematics*, 1999. À paraître.

[Ser65] J. P. Serre. *Algèbre locale. Multiplicités*, volume 11 of *Lectures notes in mathematics.* Springer, 1965.

[Soi81] L. Soicher. *The computations of Galois groups.* Thèse de doctorat, Concordia University, Montreal, 1981.

[Sta73] R.P. Stauduhar. The determination of Galois groups. *Mathematics of computation*, 27:981–996, 1973.

[SZ67] P. Samuel and O. Zariski. *Commutative Algebra*, volume I. Van Nostrand, 1967.

[Tra96] C. Traverso. Hilbert functions and the Buchberger algorithm. *Journal of Symbolic Computation*, 22(4):355–376, 1996.

[Val89] A. Valibouze. Résolvantes et fonctions symétriques. In *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*, pages 390–399. ACM Press, 1989.

[Val95] A. Valibouze. Computation of the Galois group of the resolvent factors for the direct and inverse Galois problems. In G. Cohen, M. Giusti, and T. Mora, editors, *Proc. AAECC'11*, volume 948 of *Lecture Notes in Computer Science*, pages 456–468, Paris, France, 1995. Springer.

[Val97] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bulletin of the Belgian Mathematical Society Simon Stevin*, 1997.

[vdW91] B.L. van der Waerden. *Algebra.* Springer-Verlag, 1991.

[Wan91] D. Wang. On Wu's method for solving systems of algebraic equations. Rapport technique RISC-LINZ Series no 91-52.0, Johannes Kepler University, Austria, 1991.

[Wan92a] D. Wang. An implementation of the characteristic set method in Maple. In *Proc. DISCO'92*, Bath, England, 1992.

[Wan92b] D. Wang. Some improvements on Wu's method for solving systems of algebraic equations. In Wu Wen-Tsün and Cheng Min-De, editors, *Proc. of the Int. Workshop on Math. Mechanisation*, Beijing, China, 1992. Institute of Systems Science, Academia Sinica.

[Wan93a] D. Wang. An elimination method based on Siedenberg's theory and its applications. In F. Eysette and A. Galligo, editors, *Comptutational Algebraic Geometry*, pages 301–328. Birkhäuser Boston, 1993.

[Wan93b] D. Wang. An elimination method for polynomial systems. *Journal of Symbolic Computation*, 16:83–114, 1993.

[Wan95] D. Wang. An implementation of the characteristic set method in Maple. In J. Pfalzgraf and D. Wang, editors, *Automated practical reasoning: algebraic approaches*, pages 187–201. Springer, Wien, 1995.

[Wan96] D. Wang. Solving polynomial equations: characteristic sets and triangular systems. *Mathematics and computers in simulation*, 42:339–351, 1996.

[Wan98] D. Wang. Decomposing polynomial systems into simple systems. *Journal of Symbolic Computation*, 1998.

[Wu84] W. T. Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Scis*, 4:207–235, 1984.

[Wu86] W. T. Wu. On zeros of algebraic equations – an application of Ritt principle. *Kexue Tongbao*, 31(1):1–5, 1986.

[Wu87] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.

[Yok96] K. Yokoyama. A modular method for computing the Galois groups of polynomials. In A. Cohen and M.F. Roy, editors, *special issue of MEGA'96*, pages 617–636. Journal of Pure and Applied Algebra, 1996.

[YZ94] L. Yang and J. Zhang. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. In J. Johnson, S. McKee, and A. Vella, editors, *Artificial intelligence in mathematics*, pages 147–156. Oxford University Press, 1994.

[Zip93] R. Zippel. *Effective polynomial computation.* Kluwer Aca. Pub., 1993.