Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation

Clémence Durvye

Université de Versailles - Saint-Quentin

École Doctorale Société du Futur (n°438)
Laboratoire de Mathématiques de Versailles
Unité Mixte de Recherche CNRS 8100

THÈSE

présentée en vue de l'obtention du grade de

Docteur de l'Université de Versailles - Saint-Quentin
Mention Mathématiques et Applications

par

Clémence DURVYE

Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation

Version préliminaire du 26 mars 2008

Soutenance prévue le 9 juin 2008

Remerciements

Table des matières

Introduction

La résolution de systèmes polynomiaux est l'un des domaines les plus actifs du calcul formel depuis le milieu des années soixante. Il existe de nombreuses manières d'appréhender la question, ce qui explique l'abondance des travaux sur le sujet. Les plus célèbres d'entre eux sont ceux qui proviennent de l'algorithme proposé par Buchberger dans [Buc70] pour le calcul des bases de Gröbner, dans la veine des travaux d'Hironaka ; d'autres s'appuient sur des décompositions triangulaires, des calculs de résultants ou des matrices de Macaulay. De nos jours, tous les systèmes de calcul formel offrent des algorithmes de résolution polynomiale. Ces derniers sont au cœur d'outils de calcul plus sophistiqués en géométrie algébrique ; ils permettent également de résoudre des problèmes classiques provenant de l'ingénierie. Il existe de nombreux ouvrages généralistes traitant de ce sujet, comme par exemple [BW93, Eis95, GP02, GG03, Mor03, Wan04, CLO97, CLO05].

Dans tous les algorithmes mentionnés plus haut, les polynômes sont représentés par le vecteur de leurs coefficients dans la base des monômes. Dans un tel modèle, chaque opération élémentaire peut souvent être interprétée comme une élimination Gaussienne, si bien que les routines d'algèbre linéaire jouent un rôle central. La connaissance d'une base de Gröbner d'un idéal permet de remplacer un monôme par des monômes de plus bas degré ; pour cette raison, cette approche est souvent appelée *méthode de réécriture* comme dans [Dem85].

Plutôt que de développer un polynôme dans la base des monômes, on peut préférer l'encoder comme la fonction qui calcule ses valeurs en tout point ; on parle alors de *méthodes d'évaluation*. Il existe de nombreuses études tirant parti de telles représentations. L'algorithme *Kronecker*, qui fait l'objet de cette thèse, appartient à cette seconde classe de travaux.

En généralisant la méthode du pivot de Gauss aux systèmes polynomiaux, on est amené à "éliminer" des variables. Du point de vue de la complexité, développer des polynômes provenant de processus d'élimination est souvent une mauvaise idée, car le nombre de leurs monômes explose de manière exponentielle. En revanche, les polynômes éliminants se comportent bien dans un modèle en évaluation, comme nous l'illustrons dans ce paragraphe avec trois familles d'exemples. Tout d'abord, considérons le déterminant d'une matrice $n \times n$, qui est un polynôme de degré n en les n^2 coefficients de la matrice. Il est bien connu que le nombre de ses monômes est $n!$, alors qu'il peut être évalué en tout point avec $\mathcal{O}(n^3)$ opérations. Regardons ensuite le résultant de deux polynômes univariés de degré n dont les coefficients sont indéterminés. Ce dernier est un polynôme éliminant à $2(n+1)$ indéterminées. Le nombre de ses monômes croît exponentiellement en n, alors qu'il peut être évalué en un nombre d'opérations arithmétiques quasi-linéaire en n (voir par exemple [GG03, Chapter 11]). Enfin, intéressons-nous à un système de n polynômes denses de degré d en $2n$ variables. De manière informelle, si ces polynômes sont suffisamment génériques, alors l'ensemble de leurs racines communes est de dimension n et de degré d^n. Dans cette situation, les polynômes éliminants en n variables sont de degré d^n, si bien que le nombre de monômes croît en d^{n^2} lorsque d est fixé et n tend vers l'infini. En revanche, les algorithmes présentés dans [Lec03] évaluent de tels polynômes éliminants avec un nombre d'opérations qui croît en d^n seulement.

L'algorithme *Kronecker* proposé par Giusti, Lecerf et Salvy dans [GLS01] résout un système polynomial ayant un nombre fini de solutions avec un coût qui est linéaire en la taille de l'entrée

(donnée par une structure en évaluation) et polynomial en un degré géométrique intrinsèque. Cet algorithme est l'aboutissement d'une longue lignée de travaux, que nous retraçons dans la section suivante. Dans la seconde partie de cette thèse, nous présentons une version concise de cet algorithme, ainsi qu'une preuve autonome de son bon fonctionnement, qui a fait l'objet de la publication [DL07] ; cette nouvelle preuve permet de perfectionner l'algorithme de manière à ce qu'il calcule également les multiplicités des racines sans coût supplémentaire.

Dans le cas univarié, la connaissance d'une racine et de sa multiplicité permet de retrouver le facteur du polynôme qui lui correspond. Dans le cas multivarié, la situation est plus riche, puisque deux racines peuvent avoir la même multiplicité sans avoir la même structure, ou plus précisément sans correspondre au même idéal primaire. La décomposition primaire de l'idéal associé à un système ayant un nombre fini de solutions donne une description des racines tenant compte de la structure de leur multiplicité. Jusqu'à présent, tous les algorithmes de calcul de décomposition primaire procèdent par méthodes de réécriture, et la plupart s'appuient sur des calculs de bases de Gröbner. Nous proposons dans la troisième partie de cette thèse le premier algorithme de décomposition primaire par méthodes d'évaluation ; ce résultat fait l'objet de la prépublication [Dur07].

Historique de l'algorithme "Kronecker"

Les premières études sur les propriétés des polynômes éliminants en évaluation remontent aux travaux de Giusti, Heintz, Morais et Pardo au début des années 90. Un premier algorithme, proposé dans [GH93], calcule la dimension de l'ensemble des solutions d'un système homogène. Les polynômes y sont représentés par des arbres de calcul appelés *straight-line programs* en anglais ; nous utiliserons dans cette introduction l'abréviation SLP, et renvoyons le lecteur à [BCS97, Chapter 4] pour une définition précise. On trouve ensuite dans [GHS93, FGS95, KP96] la preuve que les polynômes impliqués dans le Nullstellensätz ont aussi de bonnes propriétés en évaluation, et peuvent ainsi être calculés efficacement.

Les premiers pas vers un algorithme rapide de résolution polynomiale tirant parti des méthodes d'évaluations apparaissent dans [GHMP95, Par95]. Le but de ces articles était de développer un algorithme de résolution ayant une complexité polynomiale en des invariants géométriques intrinsèques à l'ensemble des solutions, plutôt qu'en des quantités telles que la régularité de Hilbert qui apparaît dans le coût des méthodes de réécriture. L'algorithme proposé dans [GHMP95] est incrémental en le nombre d'équations à résoudre, le système y est donné par un SLP, et la position de Noether (qui fait l'objet du chapitre 2 de cette thèse) en est un ingrédient central. Bien que les polynômes éliminants apparaissant dans cet algorithme soient représentés par des programmes courts, leur coût d'évaluation restait cher.

Comme annoncé à la fin de [GHMP95], ce mauvais comportement pouvait être évité grâce à l'utilisation d'un opérateur de Newton. Cette idée est exploitée dans [GHM+98] pour "comprimer" les SLP calculés lors des étapes intermédiaires de l'algorithme. On trouve dans [GHH+97] une nouvelle version de l'algorithme de [GHMP95], ainsi que de nouvelles bornes inférieures pour l'approximation Diophantienne. Les fibres de relèvement définies dans le chapitre 7 sont alors apparues comme une représentation efficace des variétés de dimension positive.

Ces résultats de complexité ont constitué une percée majeure en théorie de l'élimination. Les différentes versions de l'algorithme mentionnées ci-dessus partagent les caractéristiques suivantes :

- les polynômes donnés en entrée sont encodés par un SLP ;
- la résolution est calculée incrémentalement sur les équations ;
- tous les polynômes apparaissant dans les calculs sont codés par des SLP ;
- le système est supposé n'avoir qu'un nombre fini de solutions, dont l'algorithme calcule une *représentation univariée* (définie au chapitre 4) ;
- la complexité est linéaire en la taille du SLP donné en entrée, et polynomiale en le plus grand des degrés géométriques des systèmes intermédiaires.

On trouve dans [GHMP97] une variante de l'algorithme, dont le coût est polynomial en ces dernières quantités et en la hauteur de l'ensemble des solutions dans le modèle de la machine de Turing.

Les algorithmes décrits dans [GHH+97, GHMP97] ont ensuite été simplifiés dans la thèse de Morais [Mor97]. On trouve dans [Mat99] l'analyse de classe de complexité et des améliorations algorithmiques. Enfin, l'analyse de complexité binaire et d'importantes applications pour la question du Nullstellensätz arithmétique ont été développées dans [Häg98, HMPS00].

Pour implémenter ces algorithmes, il était nécessaire de programmer efficacement des structures d'évaluation. Les premiers pas dans cette direction ont été présentés à la conférence TERA'1996 à Santander par Aldaz et par Castaño, Llovet et Martìnez [CHLM00]. Hägele a ensuite proposé une implantation `C++` des SLP. Enfin, une autre librairie [BHMW02] a été écrite en langage `Haskell`. D'autres expériences ont été réalisées indépendamment pour implanter l'algorithme de [GH93] dans le système `Maple`, qui offrait déjà une base de données pour les structures d'évaluation [GHL+00]. La conclusion de tous ces essais fut que la taille des arbres de calcul intermédiaire nécessitait trop de mémoire pour que l'on puisse observer en pratique les résultats de complexité théorique.

Une solution à ce problème est ensuite venue d'une méthode de transformation utilisée en informatique théorique pour éviter le calcul de données intermédiaires dues à la composition de fonctions ; cette méthode s'appelle la *déforestation*. Dans certains cas, cette transformation peut être effectuée automatiquement, mais elle a nécessité quelques efforts dans le contexte de [GH93]. De manière informelle, la déforestation présentée dans [GHL+00] montre que le calcul et le stockage des SLP intermédiaires est inutile si l'on réécrit les algorithmes de manière appropriée. Ceci a permis d'implémenter avec succès les idées contenues dans [GH93].

Les techniques de déforestation ont été appliquées à l'algorithme de [Mor97] dans [GLS01]. Ce dernier article contient une réécriture complète de l'algorithme, ainsi que des simplifications algorithmiques et des bornes précises de complexité. Les principaux nouveaux ingrédients sont l'introduction de la *représentation de Kronecker* d'une variété, inspirée des travaux de Kronecker [Kro82] (voir le chapitre 4 de cette thèse pour une définition) et l'utilisation de courbes relevées définies dans le chapitre 7. Le nouvel algorithme a été programmé dans le système de calcul formel `Magma` sous le nom de `Kronecker` [Lec], en hommage à Léopold Kronecker. Grâce à la suppression complète des SLP intermédiaires, seul le système en entrée doit être représenté par un SLP. De plus, l'algorithme ne manipule que des polynômes en au plus deux variables sur le corps de base. Des analyses de complexité similaires et l'idée de courbe relevée ont été présentées de manière indépendante dans [HMW01].

Par la suite, ces méthodes ont été généralisées pour le calcul de la décomposition équidimensionnelle d'un système polynomial quelconque. Les algorithmes présentés dans [Lec00, JS00, JPS01, JS02, JKSS04] procèdent à un pré-traitement du système donné en entrée pour éviter l'apparition de composantes multiples dans les étapes intermédiaires, tandis que ceux de Lecerf [Lec02, Lec03] utilisent un opérateur de Newton généralisé pour traiter directement les composantes multiples. Les décompositions irréductibles rationnelle et absolue se déduisent aisément de la décomposition équidimensionelle en factorisant les représentations univariées des différentes composantes, par exemple grâce aux algorithmes proposés dans [BLS+04, Lec06, Lec07, CL07].

Les méthodes d'évaluation ont été utilisées avec succès pour résoudre des systèmes surdéterminés [GS99], des systèmes à paramètres [HKP+00, Sch03, BMWW04], des systèmes de Pham [PSM04], des systèmes creux [JMSW06], et des systèmes sur des corps finis [CM06b, CM06a]. Elles s'appliquent aussi à la géométrie réelle [BGHM97, BGHM01, BGHP04, SS04, Saf05]. Le logiciel `Kronecker` a permis de résoudre des problèmes provenant de la cryptographie [GS05], de construire des modèles pour la réception rétinienne [Mal03], et de concevoir de nouvelles bases d'ondelettes [Leh04] en traitement du signal.

De plus, l'approche incrémentale en le nombre d'équations a été adaptée récemment à la résolution numérique par prolongement homotopique [SVW05]. Des comparaisons théoriques entre les approches numériques et symboliques ont été établies dans [CPHM01, CMPSM02, CPSM03, DLDM05]. Enfin, le lecteur intéressé par les bornes inférieures de complexité pour la résolution polynomiale peut consulter [FGS95, Par95, HMPW98, GH01, CGH+03]. Grossièrement parlant, et sous certaines hypothèses, le résultat principal de [CGH+03] assure que l'algorithme *Kronecker* appartient à une "classe de complexité optimale".

Algorithmes pour la décomposition primaire

Les principaux travaux sur le calcul d'une décomposition primaire d'un idéal polynomial remontent au début des années 90 avec [GTZ88, EHV92, SY96] ; on en trouve quelques améliorations plus récentes comme [CCT97, Mon02]. Ces algorithmes traitent le cas d'idéaux de dimension quelconque sur un corps de caractéristique nulle. Ils sont inspirés des travaux de Seidenberg [Sei74, Sei78, Sei84], et sont résumés et comparés dans [DGP99, GP02].

L'algorithme de [GTZ88] est implémenté dans des systèmes de calcul formel, comme par exemple `Singular` [GPS05, DPS02]. Il se ramène au cas de la dimension nulle grâce à une position de Noether, puis réduit ce dernier cas à une factorisation univariée ; nous le présentons brièvement dans la section 1.5. Les algorithmes de [EHV92, SY96] retrouvent pour leur part la décomposition primaire d'un idéal à partir de celle de son radical par localisations. Enfin, on trouve dans [Ste05] un algorithme semblable à celui de [GTZ88] pour les corps de fonctions algébriques de caractéristique positive, et dans [GWW07] un algorithme original pour les idéaux de dimension nulle sur un corps fini.

Tous ces algorithmes utilisent des calculs de bases de Gröbner, et retournent une famille de générateurs d'un ensemble de primaires. Dans le cas de la dimension nulle, il existe d'autres manières de décrire une décomposition primaire. L'algorithme présenté dans [ABRW96] propose

d'utiliser des outils d'algèbre linéaire pour calculer, à partir d'une base de Gröbner d'un idéal, la décomposition en algèbres locales du quotient de l'anneau des polynômes par l'idéal. Un autre moyen classique d'obtenir l'algèbre locale d'une racine isolée donnée est de calculer une base standard de l'idéal pour un ordre local, ce qui est rendu possible par l'algorithme du cône tangent [Mor91] (généralisé aux ordres mixtes dans [GP96]). On trouve dans [MMM96] une discussion sur les différents moyens de représenter la structure de la multiplicité d'une racine isolée, ainsi que des algorithmes permettant de changer de représentation.

Toutes les approches précédemment citées procèdent par méthode de réécriture. Il faut néanmoins noter que les algorithmes présentés dans [DZ05, Mou97] tiennent compte des propriétés d'évaluation du système à résoudre. Étant donnée une racine p du système polynomial $f_1 = \cdots = f_s = 0$, l'algorithme de Mourrain [Mou97] calcule les matrices de multiplications par les variables dans une base de l'algèbre locale de p en exploitant la dualité entre les polynômes et les séries formelles d'opérateurs différentiels. Néanmoins, la borne sur le coût de l'algorithme donnée dans [Mou97, Proposition 4.1] dépend du "nombre de monômes obtenus par dérivation des monômes de $f_1, \ldots, f_s$", qui peut donner lieu à un nombre combinatoire. Bien que cette borne soit probablement pessimiste, nous n'en connaissons pas de meilleure.

Notre algorithme écrit dans [Dur07] et présenté dans le chapitre 10 de cette thèse est donc le premier à calculer la décomposition primaire d'un idéal de dimension nulle par méthodes d'évaluation avec un coût polynomial en un nombre de Bézout du système (voir le théorème 1 ci-dessous).

Pour étudier une racine multiple, on peut également utiliser des algorithmes de déflation [GLSY05, GLSY07, Lec02, LVZ06], qui produisent un nouveau système pour lequel la racine est simple. L'algorithme de [Lec02] le réalise dans un cadre symbolique, et est un outil central pour la décomposition équidimensionelle dans [Lec03]. Enfin, [Ley08] propose d'utiliser la déflation pour calculer tous les premiers associés à un idéal à partir de décompositions équidimensionelles. Une de nos motivations est de calculer la décomposition primaire dans le même esprit que [Lec03] sans avoir recours à la déflation.

Plan de la thèse

Pour rendre ce texte accessible à un plus grand nombre de lecteurs, nous résumons dans le premier chapitre la théorie classique de la décomposition primaire ; nous terminons par une présentation rapide de l'algorithme de [GTZ88], qui permet de familiariser le lecteur avec l'utilisation de formes séparantes.

La position de Noether présentée dans le deuxième chapitre est un ingrédient essentiel pour l'algorithme *Kronecker* ; elle permet également le calcul de la dimension d'un idéal. Un résultat classique de généricité (Theorem 2.4.3) permet d'assurer qu'un changement de variables aléatoire fournit une position de Noether avec grande probabilité ; ceci permet un processus d'élimination probabiliste, mais efficace. À partir de ce second chapitre, toutes les preuves présentées dans cette thèse sont constructives. Nous extrayons ainsi de la preuve du théorème 2.4.3 un algorithme déterministe classique pour le calcul d'une position de Noether.

Nous terminons la première partie de cette thèse par des considérations générales sur les idéaux de dimension nulle. La décomposition primaire d'un tel idéal peut être représentée par la donnée de ses racines et de leurs algèbres locales ; c'est sous cette forme que nous la calculerons dans la troisième partie. Après avoir rappelé quelques résultats classiques sur la décomposition en algèbres locales qui nous seront utiles par la suite, nous présentons dans le troisième chapitre un algorithme inspiré de [FGLM93] qui permet de retrouver une base de Gröbner du primaire associé à chacune des racines à partir de son algèbre locale.

La deuxième partie de ce texte est consacrée à la présentation de l'algorithme *Kronecker*, qui procède incrémentalement sur les équations. Chaque étape incrémentale se divise en trois opérations, appelées *relèvement*, *intersection* et *nettoyage*. Nous dédions un chapitre à chacun de ces algorithmes, puis nous réservons un chapitre à l'algorithme de résolution.

Nous définissons dans le quatrième chapitre les *représentations univariées* d'un idéal. Ces représentations sont de bons outils algorithmiques, puisqu'elles permettent de se ramener au cas de polynômes à une variable. Nous en déduisons ainsi aisément l'algorithme de nettoyage, qui permet de supprimer d'un ensemble de points ceux qui annulent un polynôme g.

La clé incrémentale de l'algorithme de résolution est la méthode d'intersection, qui fait l'objet du cinquième chapitre. Plus précisément, il s'agit de calculer une représentation univariée d'un idéal $\mathcal{I}+(f)$ de dimension nulle à partir de celle d'un idéal $\mathcal{I}$ de dimension 1. Le résultat de la proposition 5.3.1 permet de présenter un algorithme d'intersection qui calcule les éventuelles multiplicités des racines de $\mathcal{I}+(f)$. C'est un isomorphisme mis en évidence lors de la preuve de la proposition 5.3.1 qui est à l'origine du calcul des algèbres locales dans la troisième partie.

La bonne complexité de l'algorithme *Kronecker* est en partie due au fait qu'il ne manipule que des courbes et des ensembles finis de points. Ceci est rendu possible par des procédés de spécialisation et de relèvement qui sont présentés dans le sixième chapitre.

Nous terminons la deuxième partie de la thèse par une présentation complète d'un algorithme *Kronecker* avec multiplicités. L'algorithme présenté dans [GLS01] permet de calculer les solutions du système $f_1 = \cdots = f_n = 0,\ g \neq 0$ sous l'hypothèse que la suite $f_1, \ldots, f_n$ forme une *suite régulière réduite dans l'ouvert* $\{g \neq 0\}$. Cette hypothèse assure en particulier que le système ne présente pas de multiplicités avant la dernière étape d'intersection, ce qui permet entre autres l'utilisation de l'algorithme de relèvement. Dans le cas où le système a des racines multiples, l'algorithme présenté dans le cinquième chapitre permet d'en calculer les multiplicités lors de la dernière intersection. Enfin, un lemme de Bertini (Proposition 7.1.6) permet de lever l'hypothèse de régularité et ainsi de traiter tous les systèmes carrés zéro-dimensionels.

En plus de ses conséquences algorithmiques, l'énoncé de la proposition 5.3.1 permet de retrouver quelques résultats classiques de la théorie du degré, comme un théorème de Bézout, qui intervient dans l'étude de complexité de nos algorithmes. Les preuves de ces résultats sont rassemblées dans la seconde section du septième chapitre.

La troisième partie de cette thèse est consacrée au calcul des algèbres locales. L'algorithme présenté dans la seconde partie traite le système de manière globale. Pour trouver la structure d'une racine multiple, nous allons intervenir de manière locale lors de la dernière intersection. Nous sommes ainsi ramenés à l'étude d'un point à l'intersection d'une courbe et d'une hypersurface.

Dans ce contexte local, nous aurons besoin d'algorithmes pour la réduction de matrices à coefficients dans un anneau de séries formelles. Bien que cette question ait été abondamment étudiée dans le cas de matrices à coefficients entiers ou polynomiaux, il ne semble pas exister de travaux traitant le cas des séries. Nous proposons dans le huitième chapitre des algorithmes adaptés à nos applications, ainsi que l'étude de leur complexité.

Dans le neuvième chapitre, nous introduisons un module de germe de courbe en la racine à étudier, et nous donnons un algorithme pour calculer ce module à partir d'une représentation univariée de la courbe.

Le calcul de l'algèbre locale se limite ensuite à une réduction de Smith, qui est détaillée dans le dixième chapitre ; un raisonnement analogue permet de traiter les systèmes surdéterminés. Nous terminons le dixième chapitre par une présentation générale de l'algorithme de décomposition primaire, ainsi que par son étude de coût.

Contributions originales de la thèse

La première contribution de cette thèse est une présentation concise de l'algorithme *Kronecker*, ainsi qu'une preuve entièrement autonome de son bon fonctionnement. Les simplifications apportées aux preuves de [GLS01] permettent d'éviter le recours à des outils extérieurs à l'algorithme, comme par exemple les séries de Hilbert. Nos preuves suivent en effet des idées géométriques directement liées aux algorithmes ; à l'exception de celles du premier chapitre, elles sont toutes constructives. Nous retrouvons ainsi dans la section 7.2 des résultats classiques de la théorie du degré, comme un théorème de Bézout, qui intervient dans les études de coût des algorithmes. À l'exception des considérations de complexités consignées dans le paragraphe précédant le théorème 1, les seuls prérequis pour la lecture de cette thèse sont quelques résultats sur les modules sur un anneau principal, que l'on peut trouver par exemple dans [Lan02, Chapter X, Section 3], et un résultat classique sur les extensions de corps, dont une preuve peut être trouvée dans [Lan02, Chapter VII, Section 1, Theorem 1.1], et qui n'est utilisé que dans le second chapitre.

Au delà de leur intérêt pédagogique, ces nouvelles preuves permettent de lever certaines hypothèses de régularité : le théorème 4.2.1, puis la proposition 5.3.1 généralisent [GLS01, Corollary 2 and Proposition 8] aux idéaux équidimensionels. Ces nouveaux énoncés nous permettent de présenter dans le chapitre 7 un algorithme qui calcule les multiplicités des racines sans coût supplémentaire.

Dans la troisième partie de la thèse, nous aurons besoin d'algorithmes pour la réduction de matrices à coefficients dans un anneau de séries formelles ; cette question ne semble pas avoir été étudiée jusqu'à présent. Nous proposons dans le chapitre 8 un algorithme de calcul de forme de Smith avec multiplicateurs inspiré de [Vil93], ainsi que son analyse de coût.

Enfin, nous tirons parti de l'aspect algorithmique de la preuve de la proposition 5.3.1 pour présenter au chapitre 10 un nouvel algorithme de décomposition primaire. Dans la section 10.3, nous proposons également une première estimation de sa complexité.

Plus précisément, étant donnés $n+1$ polynômes $f_1, \ldots, f_n, g$ à n variables sur un corps $\mathbb{K}$

de caractéristique zéro, l'algorithme *Kronecker* calcule les racines du système $f_1 = \cdots = f_n = 0,\ g \neq 0$ sous l'hypothèse que la suite $f_1, \ldots, f_n$ est *régulière réduite* dans l'ouvert $\{g \neq 0\}$; ceci implique en particulier que l'ensemble des solutions du système dans une clôture algébrique $\bar{\mathbb{K}}$ de $\mathbb{K}$ est fini. L'algorithme retourne une suite $q, v_1, \ldots, v_n \in \mathbb{K}[T]$ de polynômes univariés telle que les solutions du système dans $\bar{\mathbb{K}}^n$ sont les n-uplets $(v_1(\alpha), \ldots, v_n(\alpha))$ lorsque α parcourt l'ensemble des racines de q dans $\bar{\mathbb{K}}$; une telle suite est appelée *représentation univariée* de l'ensemble des solutions.

L'algorithme présenté au chapitre 7 calcule également un polynôme $\chi \in \mathbb{K}[T]$ ayant les mêmes facteurs irréductibles que q et tel que la multiplicité de $(v_1(\alpha), \ldots, v_n(\alpha))$ comme solution du système est égale à celle de α comme racine de χ. La suite $\chi, q, v_1, \ldots, v_n$ est appelée *représentation univariée avec multiplicités* de l'idéal associé au système. De plus, reprenant l'idée de [GH93, KP96], nous utilisons un lemme de Bertini pour traiter tous les systèmes $g_1 = \cdots = g_n = 0, g \neq 0$ ayant un nombre fini de solutions dans $\bar{\mathbb{K}}^n$.

Étant donnés $s+1$ polynômes $g_1, \ldots, g_s, g$, nous notons $(g_1, \ldots, g_s)$ l'idéal de $\mathbb{K}[x_1, \ldots, x_n]$ engendré par $g_1, \ldots, g_s$; l'idéal associé au système $g_1 = \cdots = g_s = 0, g \neq 0$ est le *saturé* par g

$$(g_1, \ldots, g_s) : g^\infty = \{h \in \mathbb{K}[x_1, \ldots, x_n], \exists N \in \mathbb{N}, g^N h \in (g_1, \ldots, g_s)\}$$

(la signification géométrique de la saturation est présentée dans la section 1.3). Sous l'hypothèse que le système n'a qu'un nombre fini de solutions dans $\bar{\mathbb{K}}^n$, l'algorithme présenté dans la section 10.3 calcule :

- une représentation univariée avec multiplicités $\chi, Q, V_1, \ldots, V_n$ de $(g_1, \ldots, g_s) : g^\infty$;
- une suite $\mu_1, \ldots, \mu_\rho$ d'entiers non nuls et des polynômes deux à deux premiers entre eux $Q_1, \ldots, Q_\rho \in \mathbb{K}[T]$ tels que $\chi = Q_1^{\mu_1} \cdots Q_\rho^{\mu_\rho}$;
- pour tout $\ell \in \{1, \ldots, \rho\}$, une suite $M_{x_1}^{(\ell)}, \ldots, M_{x_n}^{(\ell)}$ de matrices $\mu_\ell \times \mu_\ell$ à coefficients dans $\mathbb{K}[T]$, telles que pour toute racine $\alpha \in \bar{\mathbb{K}}$ de Q_ℓ, les matrices $M_{x_1}^{(\ell)}, \ldots, M_{x_n}^{(\ell)}$ évaluées en $T = \alpha$ soient les matrices des endomorphismes de multiplication par $x_1, \ldots, x_n$ dans une base commune de l'algèbre locale de $(V_1(\alpha), \ldots, V_n(\alpha))$ comme racine de $(g_1, \ldots, g_s) : g^\infty$.

La suite $(\mu_\ell, Q_\ell, M_{x_1}^{(\ell)}, \ldots, M_{x_n}^{(\ell)})_{1 \leq \ell \leq \rho}$ décrit ainsi la structure des différentes algèbres locales ; nous l'appelons *représentation univariée locale*, et nous en donnons des exemples dans la section 10.3. Les polynômes $Q_1, \ldots, Q_\rho$ proviennent d'un processus d'*évaluation dynamique* qui permet d'éviter la factorisation du polynôme χ (voir section 10.3).

Nous résumons dans ce paragraphe les résultats classiques de complexité qui sont utiles pour l'étude de coût de notre algorithme. Nous nous plaçons dans un modèle d'arbres de calcul défini dans [BCS97, Section 4.4], et le système en entrée est donné par un SLP ([BCS97, Section 4.1]). Au cours des calculs, nous ne manipulons que des SLP sans division. Pour tout couple de fonctions (f, g), nous écrivons $f \in \tilde{\mathcal{O}}(g)$ lorsqu'il existe $\beta > 0$ tel que f/g appartient à $\mathcal{O}(\log(g)^\beta)$. Pour tout anneau unitaire A, une opération arithmétique entre deux polynômes de $A[T]$ de degré au plus d (addition, multiplication ou division euclidienne par un polynôme unitaire) coûte $\tilde{\mathcal{O}}(d)$ opérations arithmétiques dans A. Sommer ou multiplier des matrices $n \times n$ à coefficients dans A coûte $\mathcal{O}(n^3)$ opérations arithmétiques dans A ; le déterminant ou l'inverse d'une telle matrice peuvent être calculés en $\mathcal{O}(n^4)$ opérations, ou en $\mathcal{O}(n^3)$ opérations si A est un corps (de tels résultats peuvent être trouvés dans [BCS97, Chapters 15 and 16]). Il est connu que les opérations usuelles en algèbre linéaire peuvent être effectuées plus rapidement ; nous nous restreignons volontairement aux algorithmes naifs à ce stade de notre travail. Par

exemple, évaluer un SLP de taille L en une matrice $n \times n$ à coefficients dans $\mathbb{K}$ coûte $L\mathcal{O}(n^3)$ opérations arithmétiques dans $\mathbb{K}$.

Notre résultat de complexité principal est le suivant :

Théorème 1. *Soit $\mathbb{K}$ un corps de caractéristique zéro, et $g_1, \ldots, g_s, g \in \mathbb{K}[x_1, \ldots, x_n]$ des polynômes donnés par un SLP de taille L tels que le système $g_1 = \cdots = g_s = 0, g \neq 0$ a un nombre fini de solutions dans la clôture algébrique de $\mathbb{K}$. Soient $d_1, \ldots, d_s$ les degrés respectifs de $g_1, \ldots, g_s$. On suppose que $d_1 \geq d_2 \geq \cdots \geq d_s > 1$, et on pose $D = d_1 \cdots d_n$. Alors l'algorithme 14 du chapitre 10 calcule une représentation univariée avec multiplicités et une représentation locale de l'idéal $(g_1, \ldots, g_s) : g^\infty$ en*

$$\tilde{\mathcal{O}}(D^{11} + (L + ns)D^6)$$

opérations arithmétiques dans $\mathbb{K}$. L'algorithme est probabiliste et dépend du choix de $\mathcal{O}(ns)$ éléments de $\mathbb{K}$; les mauvais choix sont inclus dans un fermé algébrique propre.

Notre algorithme est probabiliste de type Monte Carlo : il est amené à choisir des paramètres aléatoires, et de mauvais choix peuvent en altérer le résultat. Néanmoins, le fait que ces mauvais choix soient inclus dans des fermés algébriques stricts rend la probabilité d'erreur très faible. Nous n'estimons pas dans cette thèse la probabilité d'erreur, qui est voisine de celle de l'algorithme *Kronecker*. Nous renvoyons le lecteur interessé par ce genre de questions à des travaux tels que [HMW01, Mat99, KPS01].

L'exposant obtenu dans le théorème 1 n'est pas optimal. Nous donnons quelques pistes pour l'améliorer à la fin du chapitre 10.

Enfin, les extensions [Lec00, Lec03] de l'algorithme *Kronecker* permettent le calcul de la décomposition équidimensionelle d'une variété. Nous espérons que des idées similaires permettent d'étendre nos techniques au calcul des primaires isolés en dimension positive.

Notations

Here, we gather together the notations defined all along the thesis, so that this section can be used as an index of notations.

As usual, we let $\mathbb{N}$ denote the integer ring. For any subsets $\mathcal{E}, \mathcal{F}$, we write $\mathcal{E} \subseteq \mathcal{F}$ if any element x of $\mathcal{E}$ belongs to $\mathcal{F}$, we write $\mathcal{E} \subsetneq \mathcal{F}$ if $\mathcal{E} \subseteq \mathcal{F}$ with $\mathcal{E} \neq \mathcal{F}$, and $\mathcal{E} \nsubseteq \mathcal{F}$ if there exists $x \in \mathcal{E}$ that does not belong to $\mathcal{F}$. We let $\emptyset$ denote the empty set. For our complexity measurement, we use the classical notation $f \in \tilde{\mathcal{O}}(g)$ when there exists $\beta > 0$ such that $f/g \in \mathcal{O}(\log(g)^\beta)$.

In all the thesis, $\mathbb{K}$ denotes a field of characteristic zero with algebraic closure $\bar{\mathbb{K}}$, and $\bar{\mathbb{K}}^n$ denotes the affine space with dimension n over $\bar{\mathbb{K}}$. Apart from the beginning of Chapter 1, $\mathcal{I}$ denotes an ideal of the ring $\mathbb{K}[x_1, \ldots, x_n]$ of polynomials in n variables over $\mathbb{K}$; we write $\mathcal{V}(\mathcal{I})$ for the set of zeros of $\mathcal{I}$ in $\bar{\mathbb{K}}^n$. Given polynomials $f_1, \ldots, f_i \in \mathbb{K}[x_1, \ldots, x_n]$, we write $(f_1, \ldots, f_i)$ for the ideal generated by $f_1, \ldots, f_i$ in $\mathbb{K}[x_1, \ldots, x_n]$, or in a formal series ring in Part III. We write $\mathcal{I} + \mathcal{J}$ for the ideal generated by all the elements of the ideals $\mathcal{I}$ and $\mathcal{J}$ in $\mathbb{K}[x_1, \ldots, x_n]$, and $\mathcal{I} : g^\infty$ for the *saturation* of the ideal $\mathcal{I}$ by the polynomial g (see Definition 1.3.1).

For any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, we write $\deg(f)$, respectively, $\deg_{x_j}(f)$, for the total degree of f, respectively, its partial degree in x_j. The polynomial f is said to be *monic* in x_j when the coefficient of the greatest power of x_j in f is a unit of $\mathbb{K}$.

For any $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, we let $\mathrm{Res}_{x_j}(f, g)$ denote the resultant of f and g with respect to x_j, which is the determinant of the Sylvester matrix of f and g seen as polynomials in the variable x_j; the discriminant $\mathrm{Disc}_{x_j}(f)$ of f with respect to x_j is $\mathrm{Res}_{x_j}(f, \partial f/\partial x_j)$. Two polynomials f, g are *pairwise coprime* if their only common divisors are the units of $\mathbb{K}[x_1, \ldots, x_n]$, and the polynomial f is *square-free* if there does not exist a polynomial g with positive degree such that g^2 divides f.

In Part II, for any ideal $\mathcal{I} \neq (1)$ in $\mathbb{K}[x_1, \ldots, x_n]$ of dimension r, we use the following notation:

$$\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r], \quad \mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I},$$

$$\mathbb{A}' = \mathbb{K}(x_1, \ldots, x_r), \quad \mathbb{B}' = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}',$$

where $\mathcal{I}'$ denotes the extension of $\mathcal{I}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$; let us remark that in Chapter 2, $\mathbb{A}$ denotes any subring of $\mathbb{K}[x_1, \ldots, x_n]$ with unity. If $\mathcal{I}$ is any ideal in Noether position, then $\mathbb{B}'$ is a $\mathbb{A}'$-vector space of finite dimension, so that, for any f in $\mathbb{K}[x_1, \ldots, x_n]$, we can define $\chi \in \mathbb{A}'[T]$ (respectively, μ) as the characteristic (respectively, minimal) polynomial of the endomorphism of multiplication by f in $\mathbb{B}'$; we write χ_0, respectively μ_0, for the constant coefficient of χ, respectively μ.

The sequences $q, v_{r+1}, \ldots, v_n$, respectively $q, w_{r+1}, \ldots, w_n$, refer to a univariate, respectively Kronecker, representation of $\mathcal{I}$ (see Definition 4.3.2). In the case when $\mathcal{I}$ is radical unmixed in Noether position, we let δ denote the dimension of $\mathbb{B}'$, that equals the degree of q. In Chapter 7, we are given $f_1, \ldots, f_n, g \in \mathbb{K}[x_1, \ldots, x_n]$, and for $i \in \{1, \ldots, n\}$, we set

$$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty, \mathcal{J}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i})}, \text{ and } \mathcal{K}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})}.$$

We say that $f_1, \ldots, f_n$ is a *reduced regular sequence in the open subset* $\{g \neq 0\}$ when for all $i \in \{0, \ldots, n-1\}$, f_{i+1} is a nonzerodivisor modulo $\mathcal{I}_i$, and $\mathcal{I}_i$ is radical.

In Part III, we are led to deal with the ring $\mathbb{K}[[x_1, \ldots, x_n]]$ of formal power series in $x_1, \ldots, x_n$ over $\mathbb{K}$. We say that we compute in $\mathbb{K}[[x_1]]$ *to precision* η when we calculate in $\mathbb{K}[[x_1]]/(x_1^\eta)$. For any ring R, we let $(\mathrm{R})_{r\times s}$ denote the algebra of matrices with r rows, s columns and entries in R. We let $M_{k,\ell}$, respectively $M_{\cdot,\ell}$, denote the (k,ℓ)-th entry, respectively the ℓ-th column, of the element M of $(\mathrm{R})_{r\times s}$; we let M^t denote the transpose of M. In the case when R is the formal power series ring $\mathbb{K}[[t]]$, M to precision η is the matrix whose entries are those of M to precision η.

In Chapters 9 and 10, we are given the Kronecker representation $q, w_2, \ldots, w_n$ with respect to x_2 of an unmixed one-dimensional radical ideal $\mathcal{I}$. We let q_0 be the product of all irreducible factors of $q \in \mathbb{K}[[x_1]][x_2]$ that vanish in $(0,0)$. We let $\mathcal{I}_0$ denote the ideal $\mathcal{I}$ extended to $\mathbb{K}[[x_1]][x_2, \ldots, x_n]$, and we set $\mathcal{J}_0 = \mathcal{I}_0 + (q_0)$ and $\mathbb{B}_0 = \mathbb{K}[[x_1]][x_2, \ldots, x_n]/\mathcal{J}_0$. The degree of q_0 is denoted by δ_0, when m_0 denotes half the valuation of $\mathrm{Disc}_{x_2}(q_0)$. We set

$$\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \mathbb{K}[[x_1]]x_2 \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0-1}$$

and

$$\mathbb{L}_0 = \mathbb{K}[[x_1]]\frac{1}{x_1^{m_0}} \oplus \mathbb{K}[[x_1]]\frac{x_2}{x_1^{m_0}} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{\delta_0-1}}{x_1^{m_0}}.$$

We are also given a polynomial f such that $\mathcal{I} + (f)$ is zero-dimensional. We denote by

$$\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, \ldots, x_n]]/(\mathcal{I}_0 + (f))$$

the local algebra of the origin as a root of $\mathcal{I} + (f)$ (see Definition 3.1.4). The integer μ_0 is the dimension of $\mathbb{D}_0$. The central ingredent of the computations of Part III is the isomorphism

$$\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f) \simeq \mathbb{D}_0,$$

where $\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f)$ stands for the quotient of $\bar{\mathbb{K}}[[x_1]][x_2, \ldots, x_n]$ by the extension of $\mathcal{J}_0 + (f)$ to $\bar{\mathbb{K}}[[x_1]][x_2, \ldots, x_n]$.

Part I

Prerequisite on Primary Decomposition

Let Q be a polynomial in one variable over an algebraically closed field of characteristic zero. Its factorization $Q = \prod_{\ell=1}^{s}(T-\alpha_\ell)^{\nu_\ell}$ gives a complete description of its roots: the irreducible factors give the roots α_ℓ, when their multiplicities can be read from the exponents ν_ℓ. In Part I, we summarize the classical theory of primary decomposition, which generalizes this description for polynomial systems with several variables.

We begin Chapter 1 with the definition of an algebraic variety, which gives a geometrical meaning to a polynomial system. Then we present the irreducible decomposition of radical ideals, and give a geometric interpretation of the saturation of an ideal, which traduces inequalities. Finally, primary decompositions give an exact description of the roots of an ideal. There are not so many known algorithms for computing primary decompositions in the general case. We end Chapter 1 by giving a quick presentation of the famous one designed by Gianni, Trager and Zacharias in [GTZ88], which computes primary decompositions by reducing to the univariate case. Though we will have no need of this algorithm in the rest of the thesis, it is a first incursion in the univariate philosophy.

The notions introduced in Chapter 1 permit us to define the dimension of an ideal as the maximal dimension of its components. A classical way to compute the dimension is to choose variables such that the ideal is in *Noether position*. Such a situation will be essential in Part II since it allows to perform linear algebra in the quotient of the polynomial ring by the ideal. Moreover, it can be used to reduce the dimension of any ideal by specializations, which will permit us to deal with curves and finite set of points. In Chapter 2, we first give the definition of the dimension of an ideal *via* transcendence degree. We then present Noether positions and give a genericity result, together with an algorithm for computing a Noether position.

We end Part I with the particular case of zero-dimensional ideals, whose computation is the purpose of this thesis. We recall the definition of a local algebra at a zero of an ideal. Then we reformulate the primary decomposition in terms of local algebras; as a consequence, we remind a classical result on characteristic polynomials that will be intensively used in Part II since it gives a first piece of information on the multiplicities. Our main Algorithm 14 in Part III returns the primary decomposition of any zero-dimensional ideal under the form of the local algebras of its different roots. We give in Section 3.3 an algorithm ispired from [FGLM93] to recover a Gröbner basis of the primary ideal of a root from its local algebra.

All the proofs given throughout this thesis are tightly connected to our algorithms. The only exception is Chapter 1, in which we give the classical presentation of the primary decomposition theory using Noetherianity.

Chapter 1

Theory of Primary Decomposition

In this chapter, we study the roots of a polynomial system from a geometrical point of view. First we associate to any system a geometric object called an affine variety; two systems define the same variety if and only if the ideals generated by the equations have the same radical. In a second section, we recall that any variety can be decomposed in irreducible components; this corresponds to write any radical ideal as an intersection of prime ideals. A primary decomposition of an ideal is then a refinement of the decomposition of its radical. The classical proofs of the existence of latter decompositions rely on the noetherianity of the polynomial ring. In the last section of this chapter, we give an overview of the existing algorithms to compute primary decomposition of any ideal, and present the well known one designed by Gianni, Trager and Zacharias in 1988, in the particular case of zero-dimensional systems.

1.1 Radical Ideals and Varieties

Let $\mathbb{K}$ be a field of characteristic zero with algebraic closure $\bar{\mathbb{K}}$. In this section, we recall the geometric meaning of some properties of ideals in $\mathbb{K}[x_1, \ldots, x_n]$. We refer the reader interested in more details on this *algebra-geometry dictionary* to [CLO97, Chapter 4].

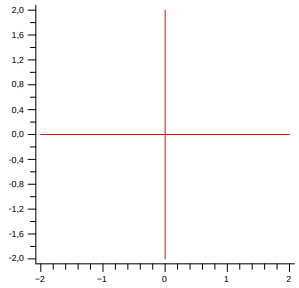
Definition 1.1.1. Let $\mathcal{I}$ be a non empty subset of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The *affine variety of* $\bar{\mathbb{K}}^n$ *defined by* $\mathcal{I}$ is the set

$$\mathcal{V}(\mathcal{I}) = \{(a_1, \ldots, a_n) \in \bar{\mathbb{K}}^n \text{ such that } \forall f \in \mathcal{I}, f(a_1, \ldots, a_n) = 0\}.$$

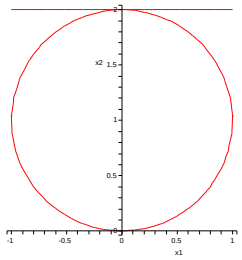
We adopt the convention that $\mathcal{V}(\emptyset) = \bar{\mathbb{K}}^n$.

The variety $\mathcal{V}(\mathcal{I})$ is thus the set of points in $\bar{\mathbb{K}}^n$ that vanish all the polynomials of $\mathcal{I}$; for examples in the affine plane $\bar{\mathbb{K}}^2$, $\mathcal{V}(x_1x_2)$ is the union of both axes and $\mathcal{V}((x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2))$ is the union of a circle and an line (see Figure 1.1.2 below). One easily deduces from the definition that the intersection of two varieties remains a variety: indeed, we have $\mathcal{V}(\mathcal{I}_1) \cap \mathcal{V}(\mathcal{I}_2) = \mathcal{V}(\mathcal{I}_1 \cup \mathcal{I}_2)$ for any subsets $\mathcal{I}_1, \mathcal{I}_2$ of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Thus the three points at the intersection of the previous circle $\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1)$ with the parabola $\mathcal{V}(x_1 - x_1^2)$ form the variety $\mathcal{V}(\{x_1^2 + (x_2 - 1)^2 - 1, x_1 - x_1^2\})$.

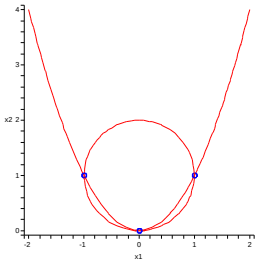
Figure 1.1.2.



$\mathcal{V}(x_1x_2)$



$\mathcal{V}((x_1^2+(x_2-1)^2-1)(x_2-2))$



$\mathcal{V}(x_1^2+(x_2-1)^2-1)\cap\mathcal{V}(x_1-x_1^2)$

It is not true in general that $\mathcal{V}(\mathcal{I}_1)\cup\mathcal{V}(\mathcal{I}_2)=\mathcal{V}(\mathcal{I}_1\cap\mathcal{I}_2)$ for any subsets $\mathcal{I}_1,\mathcal{I}_2$ of polynomials in $\mathbb{K}[x_1,\ldots,x_n]$, as shows the example $\mathcal{V}(x_1)\cup\mathcal{V}(x_2)\subsetneq\mathcal{V}(\{x_1\}\cap\{x_2\})=\bar{\mathbb{K}}^n$. Nevertheless, the previous equality is true as soon as $\mathcal{I}_1$ and $\mathcal{I}_2$ are ideals in $\mathbb{K}[x_1,\ldots,x_n]$. Indeed for the non-trivial inclusion, if a is a point in $\mathcal{V}(\mathcal{I}_1\cap\mathcal{I}_2)$ that does not belong to $\mathcal{V}(\mathcal{I}_1)$, then there exists $f\in\mathcal{I}_1$ such that $f(a)\neq 0$. For any polynomials $g\in\mathcal{I}_2$, we have $fg(a)=0$ with $f(a)\neq 0$, so that $g(a)=0$ and $a\in\mathcal{V}(\mathcal{I}_2)$, which proves that $\mathcal{V}(\mathcal{I}_1\cap\mathcal{I}_2)\subseteq\mathcal{V}(\mathcal{I}_1)\cup\mathcal{V}(\mathcal{I}_2)$. Now if $\mathcal{I}$ is any set of polynomials in $\mathbb{K}[x_1,\ldots,x_n]$, then any element of $\mathcal{V}(\mathcal{I})$ vanishes all the polynomials of the ideal $(\mathcal{I})$ generated by the elements of $\mathcal{I}$ in $\mathbb{K}[x_1,\ldots,x_n]$. We thus have $\mathcal{V}(\mathcal{I}_1)\cup\mathcal{V}(\mathcal{I}_2)=\mathcal{V}((\mathcal{I}_1)\cap(\mathcal{I}_2))$ for any sets $\mathcal{I}_1,\mathcal{I}_2$ of polynomials; for instance $\mathcal{V}(x_1)\cup\mathcal{V}(x_2)=\mathcal{V}((x_1)\cap(x_2))=\mathcal{V}(x_1x_2)$. The intersection of two varieties remains a variety.

Given any subset $\mathcal{E}$ of $\bar{\mathbb{K}}^n$, the set of polynomials that are vanished by all the elements of $\mathcal{E}$, that is

$$\mathcal{I}(\mathcal{E})=\{f\in\mathbb{K}[x_1,\ldots,x_n]\text{ such that }\forall(a_1,\ldots,a_n)\in\mathcal{E},f(a_1,\ldots,a_n)=0\},$$

is an ideal of $\mathbb{K}[x_1,\ldots,x_n]$. One easily check that the smallest variety that contains $\mathcal{E}$ is $\mathcal{V}(\mathcal{I}(\mathcal{E}))$, which is called *Zariski closure of* $\mathcal{E}$. For instance, the Zariski closure of $\mathcal{E}=\{(0,\alpha)\in\bar{\mathbb{K}}^2\text{ such that }\alpha\neq 0\}$ is the line $\mathcal{V}(x_1)$: writing $p\in\mathcal{I}(\mathcal{E})$ as $p=x_1h_1+h_2$ with $h_2\in\mathbb{K}[x_2]$, we obtain $h_2(\alpha)=0$ for all $\alpha\neq 0$, so that $h_2=0$ and $p\in(x_1)$.

For any variety $\mathcal{V}$ of $\bar{\mathbb{K}}^n$, we clearly have $\mathcal{V}(\mathcal{I}(\mathcal{V}))=\mathcal{V}$. Conversely, if $\mathcal{I}$ is an ideal, it is not true in general that $\mathcal{I}(\mathcal{V}(\mathcal{I}))$ equals $\mathcal{I}$: indeed the set of roots of a polynomial f equals the one of any power f^m of f, and $(f)\neq(f^m)$. This yields the following definition:

Definition 1.1.3. Let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1,\ldots,x_n]$.

(a) The *radical ideal of* $\mathcal{I}$ is the set

$$\sqrt{\mathcal{I}}=\{f\in\mathbb{K}[x_1,\ldots,x_n]\text{ such that }\exists m\in\mathbb{N},f^m\in\mathcal{I}\}.$$

(b) The ideal $\mathcal{I}$ is *radical* if $\mathcal{I}=\sqrt{\mathcal{I}}$.

Since we consider varieties in $\bar{\mathbb{K}}^n$, the Hilbert's Nullstellensatz theorem (see [CLO97, Chapter 4, Â§ 1, Theorem 2] for instance) ensures that for any ideal $\mathcal{I}$ in $\mathbb{K}[x_1,\ldots,x_n]$, we have $\mathcal{I}(\mathcal{V}(\mathcal{I}))=\sqrt{\mathcal{I}}$; thus the radical ideal of (x_1^2,x_2), that is (x_1,x_2), equals $\mathcal{I}(\{(0,0)\})$.

The radical ideal of $\mathcal{I}$ describes the set of common roots of all the polynomial of $\mathcal{I}$, but with a loss of information, as for (x_1^2,x_2). This lost information will be studied in Section 1.4. The subject of this thesis is to compute the roots of a system without losing this information.

1.2 Irreducible Decomposition

To study an object, for instance a variety or an ideal, one often "break" it into "simpler" objects. For example, the circle $\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1)$ seems to be "unbreakable", whereas $\mathcal{V}((x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2)) = \mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1) \cup \mathcal{V}(x_2 - 2)$ is not. We now define the "unbreakable" varieties and ideals.

Definition 1.2.1. (a) A variety $\mathcal{V}$ in $\bar{\mathbb{K}}^n$ is said to be *irreducible* if for all varieties $\mathcal{V}_1, \mathcal{V}_2$ in $\bar{\mathbb{K}}^n$, the equality $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$ implies that $\mathcal{V} = \mathcal{V}_1$ or $\mathcal{V} = \mathcal{V}_2$.

(b) An ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$ is said to be *irreducible* if for any couple $(\mathcal{I}_1, \mathcal{I}_2)$ of ideals in $\mathbb{K}[x_1, \ldots, x_n]$ such that $\mathcal{I} = \mathcal{I}_1 \cap \mathcal{I}_2$, then either $\mathcal{I} = \mathcal{I}_1$ or $\mathcal{I} = \mathcal{I}_2$.

For instance, the ideals $(x_1^2 + (x_2 - 1)^2 - 1)$ and $(x_2 - 2)$ are irreducible in $\mathbb{K}[x_1, x_2]$, when $((x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2))$ is not. The Noetherianity of the polynomial ring ensures that any ideal can be "broken" into "unbreakable" ideals, that is:

Theorem 1.2.2. *Any ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is a finite intersection of irreducible ideals.*

Proof. Let $\mathcal{I}$ be an ideal that cannot be written as an intersection of finitely many irreducible ideals. Then there exists two ideals $\mathcal{I}_1 \supsetneq \mathcal{I}$ and $\mathcal{I}_1' \supsetneq \mathcal{I}$ such that $\mathcal{I} = \mathcal{I}_1 \cap \mathcal{I}_1'$ and that $\mathcal{I}_1$ cannot be written as an intersection of finitely many irreducible ideals. By a recursive use of this method, we construct an ascending chain $\mathcal{I} \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$ of ideals in the Noetherian ring $\mathbb{K}[x_1, \ldots, x_n]$, which is impossible. Thus any ideal is an intersection of finitely many irreducible ideals. □

A similar proof for decomposition of varieties can be found in [CLO97, Chapter 4, Â§6, Theorem 2]; we prefer here to translate Theorem 1.2.2 on varieties. We expect irreducible ideals to define irreducible varieties. This leads to consider radical irreducible ideals, which actually are the following ones:

Definition 1.2.3. An ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$ is said to be *prime* if for any couple (f, g) of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ such that fg belongs to $\mathcal{I}$, either f belongs to $\mathcal{I}$ or g belongs to $\mathcal{I}$.

Lemma 1.2.4. *Let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. Then $\mathcal{I}$ is prime if and only if $\mathcal{I}$ is radical and irreducible. Moreover, the radical ideal of any irreducible ideal is prime.*

Proof. It directly follows from the definition that any prime ideal is radical. Let $\mathcal{I}$ be an ideal which is not irreducible; there exist $\mathcal{I}_1 \supsetneq \mathcal{I}$ and $\mathcal{I}_2 \supsetneq \mathcal{I}$ such that $\mathcal{I} = \mathcal{I}_1 \cap \mathcal{I}_2$. Then taking $f \in \mathcal{I}_1 \backslash \mathcal{I}$ and $g \in \mathcal{I}_2 \backslash \mathcal{I}$, we have $fg \in \mathcal{I}$ with $f \notin \mathcal{I}$ and $g \notin \mathcal{I}$, so that $\mathcal{I}$ is not prime. We thus obtain that any prime ideal is irreducible.

Conversely, let $\mathcal{I}$ be a radical ideal which is not prime. There exist $f \notin \mathcal{I}$ and $g \notin \mathcal{I}$ such that $fg \in \mathcal{I}$. Then we claim that $\mathcal{I} = (\mathcal{I} + (f)) \cap (\mathcal{I} + (g))$: for the non-trivial inclusion, if $h = h_1 + h_2 f = h_3 + h_4 g$ with $h_1, h_3 \in \mathcal{I}$, then $h^2 = h_1(h_3 + h_4 g) + (h_2 f)h_3 + h_2 h_4 (fg)$ belongs to $\mathcal{I}$, and so does h since $\mathcal{I}$ is radical. We thus obtain that $\mathcal{I}$ is not irreducible: any irreducible radical ideal is prime.

We will see in Lemma 1.4.2 that any irreducible ideal $\mathcal{I}$ is primary (see Definition 1.4.1); this ensures that the radical ideal of $\mathcal{I}$ is prime. □

Following Lemma 1.2.5 gives the geometric meaning of the notion of prime ideal.

Lemma 1.2.5. *Let $\mathcal{V}$ be an affine variety of the affine space $\bar{\mathbb{K}}^n$. Then $\mathcal{V}$ is irreducible if and only if $\mathcal{I}(\mathcal{V})$ is prime.*

Proof. On the one hand, let us assume that $\mathcal{V}$ is an irreducible variety, and let f, g be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ such that $fg \in \mathcal{I}(\mathcal{V})$. Any point of $\mathcal{V}$ vanishes either f or g, so that $\mathcal{V}$ equals the union of the two varieties $(\mathcal{V} \cap \mathcal{V}(f))$ and $(\mathcal{V} \cap \mathcal{V}(g))$. Then since $\mathcal{V}$ is irreducible, either $\mathcal{V}$ equals $\mathcal{V} \cap \mathcal{V}(f)$, and so $f \in \mathcal{I}(\mathcal{V})$, or $\mathcal{V}$ equals $\mathcal{V} \cap \mathcal{V}(g)$, and $g \in \mathcal{I}(\mathcal{V})$. We just proved that the ideal $\mathcal{I}(\mathcal{V})$ is prime.

On the other hand, assume that $\mathcal{I}(\mathcal{V})$ is prime, and let $\mathcal{V}_1, \mathcal{V}_2$ be varieties such that $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, with $\mathcal{V} \neq \mathcal{V}_1$. Since $\mathcal{V}_2 \subseteq \mathcal{V}$, we have $\mathcal{I}(\mathcal{V}) \subseteq \mathcal{I}(\mathcal{V}_2)$; the same way, we have $\mathcal{I}(\mathcal{V}) \subsetneq \mathcal{I}(\mathcal{V}_1)$. Now let $g \in \mathcal{I}(\mathcal{V}_2)$, and $f \in \mathcal{I}(\mathcal{V}_1) \backslash \mathcal{I}(\mathcal{V})$. Then since $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, fg belongs to the prime ideal $\mathcal{I}(\mathcal{V})$. Thus g belongs to $\mathcal{I}(\mathcal{V})$, that implies that $\mathcal{I}(\mathcal{V}) = \mathcal{I}(\mathcal{V}_2)$, and so that $\mathcal{V} = \mathcal{V}_2$. □

This yields the following geometric translation of Theorem 1.2.2:

Theorem 1.2.6. *(a) Any radical ideal $\mathcal{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$ is a finite intersection $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathfrak{p}_\ell$ of prime ideals. Moreover the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ is uniquely determined by $\mathcal{I}$ as soon as we assume that $\mathfrak{p}_\ell \not\subseteq \mathfrak{p}_k$ for $\ell \neq k$; $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathfrak{p}_\ell$ is then called the* reduced prime decomposition *of $\mathcal{I}$.*

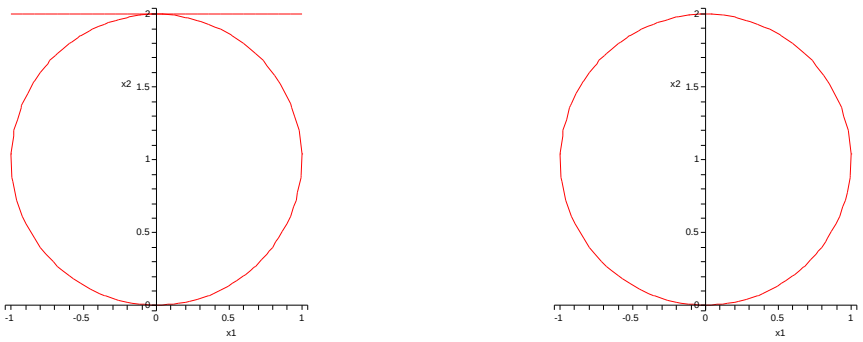
(b) Any variety $\mathcal{V}$ in $\bar{\mathbb{K}}^n$ is a finite union $\mathcal{V} = \bigcup_{\ell=1}^{s} \mathcal{V}_\ell$ of irreducible varieties. Moreover the set $\{\mathcal{V}_1, \ldots, \mathcal{V}_s\}$ is uniquely determined by $\mathcal{V}$ as soon as we assume that $\mathcal{V}_\ell \not\subseteq \mathcal{V}_k$ for $\ell \neq k$; $\mathcal{V} = \bigcup_{\ell=1}^{s} \mathcal{V}_\ell$ is then called the reduced decomposition *of $\mathcal{V}$, and $\mathcal{V}_1, \ldots, \mathcal{V}_s$ are the* irreducible components *of $\mathcal{V}$.*

Proof. Let $\mathcal{I}$ be radical ideal. Theorem 1.2.2 ensures the existence of some irreducible ideals $\mathcal{I}_1, \ldots, \mathcal{I}_s$ such that $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{I}_\ell$. Then $\mathcal{I} = \sqrt{\mathcal{I}} = \bigcap_{\ell=1}^{s} \sqrt{\mathcal{I}_\ell}$, which proves the existence of a decomposition as in part (a) by Lemma 1.2.4. Then for any variety $\mathcal{V}$ in $\bar{\mathbb{K}}^n$, there exist some prime ideals $\mathcal{I}_1, \ldots, \mathcal{I}_s$ such that $\mathcal{I}(\mathcal{V}) = \bigcap_{\ell=1}^{s} \mathcal{I}_\ell$. Thus $\mathcal{V} = \bigcup_{\ell=1}^{s} \mathcal{V}(\mathcal{I}_\ell)$, which yields the existence of the decomposition as in part (b) by Lemma 1.2.5 since $\mathcal{I}(\mathcal{V}(\mathcal{I}_\ell)) = \mathcal{I}_\ell$ is prime.

Let $\mathcal{V}$ be any variety in $\bar{\mathbb{K}}^n$. One easily deduce from a decomposition of $\mathcal{V}$ in irreducible varieties a reduced one $\mathcal{V} = \bigcup_{\ell=1}^{s} \mathcal{V}_\ell$. Let $\mathcal{V} = \bigcup_{\ell=1}^{s'} \mathcal{V}'_\ell$ be another reduced decomposition of $\mathcal{V}$. Then for $\ell \in \{1, \ldots, s\}$, we have $\mathcal{V}_\ell = \mathcal{V}_\ell \cap \mathcal{V} = \bigcup_{k=1}^{s'} (\mathcal{V}_\ell \cap \mathcal{V}'_k)$. Since $\mathcal{V}_\ell$ is irreducible, this yields $\mathcal{V}_\ell = \mathcal{V}_\ell \cap \mathcal{V}'_k$ for some $k \in \{1, \ldots, s'\}$, that is, $\mathcal{V}_\ell \subseteq \mathcal{V}'_k$. Proceeding the same way, one obtains that $\mathcal{V}'_k \subseteq \mathcal{V}_j$ for some $j \in \{1, \ldots, s\}$. We thus have $\mathcal{V}_\ell \subseteq \mathcal{V}'_k \subseteq \mathcal{V}_j$, which implies $\ell = j$ and $\mathcal{V}_\ell = \mathcal{V}'_k$ thanks to the hypothesis on the decomposition. Hence $\{\mathcal{V}_1, \ldots, \mathcal{V}_s\}$ is a subset of $\{\mathcal{V}'_1, \ldots, \mathcal{V}'_{s'}\}$. A similar argument gives the opposite inclusion, so that we have $\{\mathcal{V}_1, \ldots, \mathcal{V}_s\} = \{\mathcal{V}'_1, \ldots, \mathcal{V}'_{s'}\}$: we are done with part (b).

For any ideals $\mathcal{I}, \mathcal{J}$, we have the equivalence $\mathcal{I} \subseteq \mathcal{J} \Leftrightarrow \mathcal{V}(\mathcal{J}) \subseteq \mathcal{V}(\mathcal{I})$. Thus the uniqueness of the reduced prime decomposition of a radical ideal directly follows from the one of a variety by Lemma 1.2.5. □

Figure 1.3.2.



$\mathcal{V}((x_1^2+(x_2-1)^2-1)(x_2-2))$ $\mathcal{V}(((x_1^2+(x_2-1)^2-1)(x_2-2)) : (x_2-2)^\infty)$

Example 1.2.7. The variety $\mathcal{V}((x_1^2+(x_2-1)^2-1)(x_2-2))$ is the union of a circle and a line in $\bar{\mathbb{K}}^2$ (see Figure 1.1.2); this corresponds to the radical decomposition

$$\sqrt{((x_1^2+(x_2-1)^2-1)(x_2-2))} = (x_1^2+(x_2-1)^2-1) \cap (x_2-2).$$

The three points at the intersection of the circle $\mathcal{V}(x_1^2+(x_2-1)^2-1)$ and the parabola $\mathcal{V}(x_2-x_1^2)$ are given by

$$\sqrt{(x_1^2+(x_2-1)^2-1, x_2-x_1^2)} = (x_1-1, x_2-1) \cap (x_1+1, x_2-1) \cap (x_1, x_2).$$

1.3 Saturation of Ideals: Removing of Components

We present here a notion that can be used as an algorithmic tool to compute decompositions of ideals.

Definition 1.3.1. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1,\ldots,x_n]$, g be a polynomial, and m be an integer.

(a) The *quotient ideal* $\mathcal{I} : g^m$ *of* $\mathcal{I}$ *by* g^m is

$$\mathcal{I} : g^m = \{f \in \mathbb{K}[x_1,\ldots,x_n], \text{ such that } g^m f \in \mathcal{I}\}.$$

(b) The *saturation* $\mathcal{I} : g^\infty$ *of* $\mathcal{I}$ *with respect to* g is the ideal $\mathcal{I} : g^\infty = \bigcap_{m=0}^{\infty} \mathcal{I} : g^m$.

For instance, the quotient ideal of $\mathcal{I} = ((x_1^2+(x_2-1)^2-1)(x_2-2)^2)$ by $g = x_2-2$ is the ideal $((x_1^2+(x_2-1)^2-1)(x_2-2))$, when the saturation of $\mathcal{I}$ with respect to g is the ideal $(x_1^2+(x_2-1)^2-1)$ (see Figure 1.3.2 above). Following Proposition 1.3.3 highlights the geometric meaning of the saturation of an ideal $\mathcal{I}$ with respect to a polynomial g: it corresponds to remove the components of $\mathcal{V}(\mathcal{I})$ that are included in $\mathcal{V}(g)$.

Proposition 1.3.3. *Let* $\mathcal{I}$ *be an ideal of* $\mathbb{K}[x_1,\ldots,x_n]$*, and* g *be a polynomial in* $\mathbb{K}[x_1,\ldots,x_n]$*. Then* $\mathcal{V}(\mathcal{I} : g^\infty)$ *is the Zariski closure of* $\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I}) \cap \mathcal{V}(g))$.

Proof. Let a be an point in $\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I})\cap\mathcal{V}(g))$, and f be a polynomial in $\mathcal{I}:g^\infty$. There exists an integer m such that $g^m f$ belongs to $\mathcal{I}$; then a vanishes $g^m f$ without vanishing g. Thus $f(a)=0$, and so $a\in\mathcal{V}(\mathcal{I}:g^\infty)$: the Zariski closure of $\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I})\cap\mathcal{V}(g))$ is included in the variety $\mathcal{V}(\mathcal{I}:g^\infty)$.

Conversely, if h is a polynomial of $\mathcal{I}(\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I})\cap\mathcal{V}(g)))$, then gh belongs to $\mathcal{I}(\mathcal{V}(\mathcal{I}))=\sqrt{\mathcal{I}}$, and so h belongs to $\sqrt{\mathcal{I}:g^\infty}$. The ideal inclusion $\mathcal{I}(\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I})\cap\mathcal{V}(g)))\subseteq\sqrt{\mathcal{I}:g^\infty}$ implies the opposite variety inclusion $\mathcal{V}(\sqrt{\mathcal{I}:g^\infty})\subseteq\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathcal{I})\backslash(\mathcal{V}(\mathcal{I})\cap\mathcal{V}(g))))$, which ends the proof since $\mathcal{V}(\sqrt{\mathcal{I}:g^\infty})=\mathcal{V}(\mathcal{I}:g^\infty)$. □

One finds in [GP02, Sections 1.8.8 and 1.8.9] algorithms to compute quotient ideals and saturation by the use of Gröbner bases. In the univariate case, that is, when the number of variables n equals one, computing saturation reduces to gcd calculations; the latter case will be exploited in Section 4.4.

1.4 Primary Decomposition

In this section, we define the primary decompositions of any ideal $\mathcal{I}$ as decompositions that are compatible with the reduced decomposition of $\sqrt{\mathcal{I}}$. We begin with an extension of the notion of prime ideal:

Definition 1.4.1. An ideal $\mathcal{Q}$ in $\mathbb{K}[x_1,\ldots,x_n]$ is *primary* if for any couple (f,g) of polynomials in $\mathbb{K}[x_1,\ldots,x_n]$ such that fg belongs to $\mathcal{Q}$, either f belongs to $\mathcal{Q}$ or there exists $m\in\mathbb{N}$ such that g^m belongs to $\mathcal{Q}$.

One easily deduces from the definition that the radical of any primary ideal $\mathcal{Q}$ is prime, so that $\mathcal{V}(\mathcal{Q})$ is irreducible. For instance, the ideal (x_1^2,x_1x_2,x_2^2) is primary with radical ideal (x_1,x_2); primary ideals thus permit us to describe the multiplicity of an irreducible component.

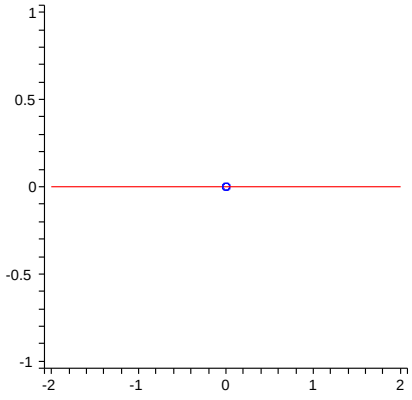
Let us notice that an ideal whose radical is prime is not always primary: by considering $f=x_2$ and $g=x_1$, one easily get convinced that the ideal (x_2^2,x_1x_2) is not primary, while its radical ideal $\sqrt{(x_2^2,x_1x_2)}=(x_2)$ is prime. Actually, the ideal $(x_2^2,x_1x_2)=(x_2)\cap(x_1^2,x_1x_2,x_2^2)$ consists of the polynomials vanishing along the line $\mathcal{V}(x_2)$ and vanishing to order at least two at the point $(0,0)$, that belongs to $\mathcal{V}(x_2)$ (see Figure 1.4.6). Considering primary ideals yields to distinguish both "components".

The irreducibility of $\mathcal{V}(\mathcal{Q})$ for any primary ideal $\mathcal{Q}$ suggests the following lemma:

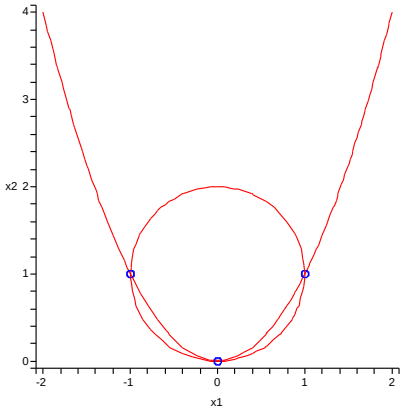
Lemma 1.4.2. *Let $\mathcal{I}$ be an irreducible ideal of $\mathbb{K}[x_1,\ldots,x_n]$. Then $\mathcal{I}$ is primary.*

Proof. Let f,g be polynomials such that $fg\in\mathcal{I}$ and $f\notin\mathcal{I}$. Then $\mathcal{I}\subseteq\mathcal{I}:g\subseteq\mathcal{I}:g^2\subseteq\cdots$ is an ascending chain of ideals in the Noetherian ring $\mathbb{K}[x_1,\ldots,x_n]$, so that there exists an integer N such that $\mathcal{I}:g^N=\mathcal{I}:g^{N+1}$. We claim that $\mathcal{I}$ equals $(\mathcal{I}+(g^N))\cap(\mathcal{I}+(f))$: for the non-trivial inclusion, if $h=h_1+h_2g^N=h_3+h_4f$ with $h_1,h_3\in\mathcal{I}$, we have $h_2g^{N+1}=h_3g+h_4fg-h_1g\in\mathcal{I}$, so that $h_2\in\mathcal{I}:g^{N+1}=\mathcal{I}:g^N$ and thus $h\in\mathcal{I}$. Then $\mathcal{I}=\mathcal{I}+(g^N)$ since $\mathcal{I}$ is irreducible with $f\notin\mathcal{I}$: the polynomial g^N belongs to $\mathcal{I}$, and $\mathcal{I}$ is primary. □

Figure 1.4.6.



(x_2^2, x_1x_2)



$\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1, x_1 - x_1^2)$

Here again, the converse does not hold, as shown by the primary ideal $(x_1^2, x_1x_2, x_2^2) = (x_1^2, x_2) \cap (x_1, x_2^2)$.

Definition 1.4.3. Let $\mathcal{Q}$ be a primary ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and let $\mathfrak{p}$ denote $\sqrt{\mathcal{Q}}$. We say that $\mathcal{Q}$ is $\mathfrak{p}$-*primary*, and we call $\mathfrak{p}$ *the prime belonging to* $\mathcal{Q}$.

If $\mathcal{Q}$ is a primary ideal, then $\sqrt{\mathcal{Q}}$ is the smallest prime ideal containing $\mathcal{Q}$; from a geometric point of view, $\mathcal{Q}$ is $\mathfrak{p}$-primary if and only if $\mathcal{V}(\mathcal{Q}) = \mathcal{V}(\mathfrak{p})$. If $\mathcal{Q}$ and $\mathcal{Q}'$ are two $\mathfrak{p}$-primary ideals for the same prime ideal $\mathfrak{p}$, then $\mathcal{Q} \cap \mathcal{Q}'$ is also a $\mathfrak{p}$-primary ideal. Reduced primary decompositions of an ideal $\mathcal{I}$ are then a refinement of the reduced decomposition in prime ideals of $\sqrt{\mathcal{I}}$:

Definition 1.4.4. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

(a) A *primary decomposition of* $\mathcal{I}$ is an expression of $\mathcal{I}$ as an intersection of primary ideals $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$.

(b) A primary decomposition $\bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$ of $\mathcal{I}$ is said to be *reduced* if the prime ideals belonging to $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ are all distinct, and if $\mathcal{I}$ cannot be expressed as an intersection of a proper subset of $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_s\}$.

Example 1.4.5. The reduced primary decomposition

$$(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2) = (x_1 - 1, x_2 - 1) \cap (x_1 + 1, x_2 - 1) \cap (x_1^2, x_2)$$

is a refinement of the radical decomposition given in Example 1.2.7, in which the tangency of the x_1-axis at the origin is not forgotten (see Figure 1.4.6).

As a consequence of Theorem 1.2.2, we obtain:

Theorem 1.4.7. *Any ideal* $\mathcal{I}$ *in* $\mathbb{K}[x_1, \ldots, x_n]$ *admits a reduced primary decomposition.*

Proof. Let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. Theorem 1.2.2 and Lemma 1.4.2 ensure the existence of a primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$ of $\mathcal{I}$. If $\mathcal{Q}_\ell$ and $\mathcal{Q}_k$ have the same radical ideal, we

can replace them with the single ideal $\mathcal{Q}_\ell \cap \mathcal{Q}_k$. Continuing in this way, we can assume that the prime ideals belonging to $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ are all distinct. Then even if it means omitting some of the $\mathcal{Q}_\ell$, we can also easily assume that $\mathcal{I}$ cannot be expressed as an intersection of a proper subset of $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_s\}$. □

A reduced primary decomposition may not be unique, as shows the example

$$(x_2^2, x_1x_2) = (x_2) \cap (x_1^2, x_1x_2, x_2^2) = (x_2) \cap (x_1, x_2^2).$$

Nevertheless, the radical ideals of (x_1^2, x_1x_2, x_2^2) and (x_1, x_2^2) are equals. This fact suggests to study the set of primes belonging to the primary ideals of a decomposition. In a sense, these prime ideals represent components of the set of zeros of the ideal (here the line $\mathcal{V}(x_2)$ and the origin), which yields the following terminology:

Definition 1.4.8. Let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. A prime ideal $\mathfrak{p} \subsetneq \mathbb{K}[x_1, \ldots, x_n]$ is called *associated prime of* $\mathcal{I}$ if there exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $\mathfrak{p} = \sqrt{\mathcal{I} : g}$.

For instance, the associated primes of $\mathcal{I} = (x_2^2, x_1x_2)$ are $(x_2) = \mathcal{I} : (x_1)$ and $(x_1, x_2) = \mathcal{I} : (x_2)$, whose radical ideals describe the x_1-axis and the origin.

Theorem 1.4.9. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, let $\bigcap_{\ell=1}^s \mathcal{Q}_\ell$ be a reduced primary decomposition of $\mathcal{I}$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ denote the primes belonging to $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$. Then the set of associated primes of $\mathcal{I}$ is exactly $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.*

Proof. On one hand, let $\mathfrak{p}$ be an associated prime of $\mathcal{I}$. There exists $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $\mathfrak{p} = \sqrt{\mathcal{I} : g} = \bigcap_{\ell=1}^s \sqrt{\mathcal{Q}_\ell : g}$. Since a prime ideal is irreducible, we thus have $\mathfrak{p} = \sqrt{\mathcal{Q}_\ell : g}$ for some $\ell \in \{1, \ldots, s\}$. Now since $\mathcal{Q}_\ell$ is primary either $\sqrt{\mathcal{Q}_\ell : g}$ equals $\sqrt{\mathcal{Q}_\ell}$ or $g \in \mathcal{Q}_\ell$. Since $\mathfrak{p} \neq \mathbb{K}[x_1, \ldots, x_n]$, the second alternative cannot occur, and we have $\mathfrak{p} = \sqrt{\mathcal{Q}_\ell}$.

On the other hand, since the primary decomposition is reduced, there exists $g_\ell \notin \mathcal{Q}_\ell$ in $\bigcap_{k \neq \ell} \mathcal{Q}_k$ for any $\ell \in \{1, \ldots, s\}$. Then $\sqrt{\mathcal{I} : g_\ell} = \bigcap_{k=1}^s \sqrt{\mathcal{Q}_k : g_\ell} = \sqrt{\mathcal{Q}_\ell : g_\ell} = \sqrt{\mathcal{Q}_\ell}$ since $g_\ell \notin \mathcal{Q}_\ell$. We thus have $\mathfrak{p}_\ell = \sqrt{\mathcal{I} : g_\ell}$, which proves that $\mathfrak{p}_\ell$ is an associated prime of $\mathcal{I}$. □

Remark 1.4.10. An ideal is primary if and only if it admits a unique associated prime.

In this thesis, we shall focus on the following particular class of ideals:

Definition 1.4.11. An ideal $\mathcal{I}$ is *zero-dimensional* if all its associated primes are maximal with respect to the inclusion of ideals.

For instance, the ideal of Example 1.4.5 is zero-dimensional, when (x_2^2, x_1x_2) is not. Since we consider varieties in $\bar{\mathbb{K}}^n$, an ideal $\mathcal{I}$ is zero-dimensional if and only if $\mathcal{V}(\mathcal{I})$ is a finite set of points in $\bar{\mathbb{K}}^n$, which justifies the terminology.

Overlying ideal (x_2^2, x_1x_2) consists of the polynomials vanishing along the line $\mathcal{V}(x_2)$ and vanishing to order at least two at the point $(0, 0)$, that belongs to $\mathcal{V}(x_2)$; this suggests to distinguish two kinds of associated primes:

Definition 1.4.12. Let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ with associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, and let ℓ be an element of $\{1, \ldots, s\}$.

(a) The ideal $\mathfrak{p}_\ell$ is an *isolated prime of* $\mathcal{I}$ if $\mathfrak{p}_k \not\subseteq \mathfrak{p}_\ell$ for all $k \neq \ell$.

(b) If $\mathfrak{p}_\ell$ is not isolated, it is said to be an are the *embedded prime of* $\mathcal{I}$.

This terminology takes root in the geometric point of view: for instance, the only isolated prime of (x_2^2, x_1x_2) is (x_2) when its unique embedded prime is (x_1, x_2), which corresponds to the origin. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the isolated primes of an ideal $\mathcal{I}$, then $\sqrt{\mathcal{I}} = \bigcap_{\ell=1}^{r} \mathfrak{p}_\ell$ is the reduced decomposition of $\sqrt{\mathcal{I}}$: by considering the radical of an ideal, we "kill" the embedded primes. The next proposition deals with the uniqueness of primary decompositions:

Proposition 1.4.13. *Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ with reduced primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$. Let $\mathfrak{p}$ be an associated prime of $\mathcal{I}$, and let $\mathcal{Q}_{\ell_1}, \ldots, \mathcal{Q}_{\ell_r}$ denote the ideals of $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_s\}$ that are included in $\mathfrak{p}$. Then $\mathcal{Q}_{\ell_1} \cap \cdots \cap \mathcal{Q}_{\ell_r}$ is independent of the decomposition.*

Proof. We let $\mathbb{K}[x_1, \ldots, x_n]_\mathfrak{p}$ denote the localization of the ring of polynomials in $\mathfrak{p}$, that is, the set of rational fractions f/g with $g \notin \mathfrak{p}$. For any ℓ such that $\mathcal{Q}_\ell \not\subseteq \mathfrak{p}$, we have

$$\mathcal{Q}_\ell \mathbb{K}[x_1, \ldots, x_n]_\mathfrak{p} \cap \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[x_1, \ldots, x_n].$$

For $\ell \in \{\ell_1, \ldots, \ell_r\}$, we claim that $\mathcal{Q}_\ell \mathbb{K}[x_1, \ldots, x_n]_\mathfrak{p} \cap \mathbb{K}[x_1, \ldots, x_n] = \mathcal{Q}_\ell$. For the non trivial inclusion, if $f \in \mathcal{Q}_\ell \mathbb{K}[x_1, \ldots, x_n]_\mathfrak{p} \cap \mathbb{K}[x_1, \ldots, x_n]$, then there exists $a \notin \mathfrak{p}$ such that $af \in \mathcal{Q}_\ell$. If $f \notin \mathcal{Q}_\ell$, then $a \in \sqrt{\mathcal{Q}_\ell}$ since $\mathcal{Q}_\ell$ is primary; this yields a contradiction since $\mathcal{Q}_\ell \subseteq \mathfrak{p}$. Thus

$$\mathcal{I}\mathbb{K}[x_1, \ldots, x_n]_\mathfrak{p} \cap \mathbb{K}[x_1, \ldots, x_n] = \bigcap_{k=1}^{r} \mathcal{Q}_{\ell_k},$$

and $\bigcap_{k=1}^{r} \mathcal{Q}_{\ell_k}$ is independent for the decomposition. □

In the case when $\mathfrak{p}$ is an isolated prime of $\mathcal{I}$, the corresponding $\mathfrak{p}$-primary ideal does not depend on the reduced primary decomposition of $\mathcal{I}$. This yields the following corollary of Proposition 1.4.13:

Corollary 1.4.14. *Let $\mathcal{I}$ be an ideal whose all associated primes are isolated. Then $\mathcal{I}$ admits a unique reduced primary decomposition. In particular, any zero-dimensional ideal admits a unique primary decomposition.*

Proof. It is a direct consequence of Proposition 1.4.13 and Definition 1.4.11. □

Example 1.4.16. Let

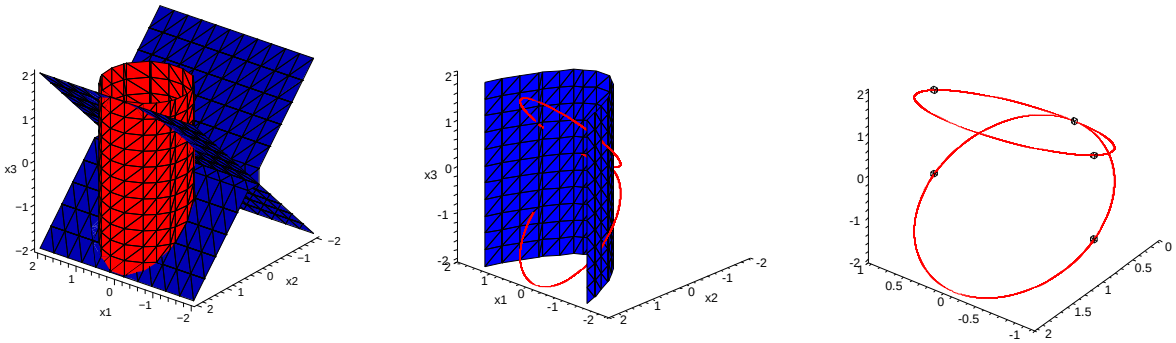
$$\begin{cases} f_1 &= x_1^2 + (x_2 - 1)^2 - 1 \\ f_2 &= x_3^2 - x_2^2 \\ f_3 &= x_2 - x_1^2. \end{cases}$$

The variety $\mathcal{V}(f_1, f_2, f_3)$ consists in the five points $(0, 0, 0), (-1, 1, \pm 1), (1, 1, \pm 1)$ (see Figure 1.4.15 below). In Chapter 10, we compute the primary decomposition

$$\begin{aligned}(x_1^2, x_1x_3, x_3^2, x_2) \cap (x_1 + 1, x_2 - 1, x_3 - 1) \cap (x_1 + 1, x_2 - 1, x_3 + 1) \\ \cap (x_1 - 1, x_2 - 1, x_3 - 1) \cap (x_1 - 1, x_2 - 1, x_3 + 1)\end{aligned}$$

of the ideal (f_1, f_2, f_3).

Figure 1.4.15.



$\mathcal{V}(f_1), \mathcal{V}(f_2)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_3)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_1, f_2, f_3)$

1.5 Algorithms for Primary Decomposition

There exist several known algorithms for computing a primary decomposition in the general case: the algorithms of [EHV92, GTZ88, SY96] for polynomial ideals over a field of characteristic zero all take root in the work of Seidenberg [Sei74, Sei78, Sei84]; they are summarized and compared in [DGP99, GP02]. Some variants of [GTZ88] are given in [CCT97, Mon02]. The algorithm of [GTZ88] reduces to the zero dimensional case thanks to a general position, whereas the algorithms of [EHV92, SY96] deduce the primary decomposition of a given ideal $\mathcal{I}$ from the one of its radical ideal $\sqrt{\mathcal{I}}$ by localizations. Finally, the algorithm of [Ste05] extends the one of [GTZ88] to algebraic function fields of positive characteristic, when [GWW07] contains an original algorithm for zero-dimensional polynomial ideals over a finite field.

We present here the core of the algorithm of [GTZ88] for zero-dimensional ideals. This algorithm is based on the following remark: in the univariate case, any ideal is generated by a single polynomial, say f. If $f = f_1^{\nu_1} \cdots f_s^{\nu_s}$ is the factorization of the univariate polynomial f in irreducible factors of $\mathbb{K}[x_1]$, then $(f) = (f_1^{\nu_1}) \cap \cdots \cap (f_s^{\nu_s})$ is a reduced primary decomposition of the ideal (f). In the univariate case, primary decomposition calculations thus corresponds to polynomial factorizations.

The main idea of Gianni, Trager and Zacharias is to reduce any zero-dimensional ideal to a univariate ideal, using the fact that for any maximal ideal $\mathfrak{p}$, we have $\mathfrak{p} \cap \mathbb{K}[x_1] \neq \emptyset$:

Definition 1.5.1. A zero-dimensional ideal $\mathcal{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$ with associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ is *in general position* if $\mathfrak{p}_\ell \cap \mathbb{K}[x_1] \neq \mathfrak{p}_k \cap \mathbb{K}[x_1]$ for $\ell \neq k$.

For instance, the ideal of Example 1.4.5 is in general position; geometrically speaking, a zero-dimensional ideal $\mathcal{I}$ is in general position when two points of $\mathcal{V}(\mathcal{I})$ are distinct if and only if their first coordinates differ. General positions permit us to exploit the univariate case towards the following proposition:

Proposition 1.5.2. *Let $\mathcal{I}$ be a zero-dimensional ideal in general position, let f be the monic polynomial that generates $\mathcal{I} \cap \mathbb{K}[x_1]$, and let $f = f_1^{\nu_1} \cdots f_s^{\nu_s}$ be its irreducible factorization in $\mathbb{K}[x_1]$. Then $\bigcap_{\ell=1}^{s} (\mathcal{I} + (f_\ell^{\nu_\ell}))$ is a primary decomposition of $\mathcal{I}$.*

Proof. Let us remark that we can assume without loss of generality that $f_1, \ldots, f_s$ are monic. First we prove that $\mathcal{I} = \bigcap_{\ell=1}^{s}(\mathcal{I} + (f_\ell^{\nu_\ell}))$. For $\ell \in \{1, \ldots, s\}$, we let $f^{(\ell)}$ denote the polynomial $f/f_\ell^{\nu_\ell}$. Then there exists a Bézout relation $\sum_{\ell=1}^{s} a_\ell f^{(\ell)} = 1$ with $a_1, \ldots, a_s$ in $\mathbb{K}[x_1]$. Now, let g belong to $\bigcap_{\ell=1}^{s}(\mathcal{I} + (f_\ell^{\nu_\ell}))$; for any $\ell \in \{1, \ldots, s\}$, there exist $g_\ell \in \mathcal{I}$ and $b_\ell \in \mathbb{K}[x_1, \ldots, x_n]$ such that $g = g_\ell + b_\ell f_\ell$. Then $g = \sum_{\ell=1}^{s} a_\ell f^{(\ell)} g = \sum_{\ell=1}^{s} a_\ell f^{(\ell)}(g_\ell + b_\ell f_\ell) = \sum_{\ell=1}^{s}(a_\ell f^{(\ell)} g_\ell + a_\ell b_\ell f)$ belongs to $\mathcal{I}$. Since the other inclusion is obvious, we have $\mathcal{I} = \bigcap_{\ell=1}^{s}(\mathcal{I} + (f_\ell^{\nu_\ell}))$.

It remains to prove that for $\ell \in \{1, \ldots, s\}$, the ideal $\mathcal{I} + (f_\ell^{\nu_\ell})$ is primary, that is, to prove that its set of associated primes $\mathcal{A}_\ell$ contains exactly one element. First we claim that $\mathcal{I} + (f_\ell^{\nu_\ell}) \neq \mathbb{K}[x_1, \ldots, x_n]$: otherwise one could find $g \in \mathcal{I}$ and $h \in \mathbb{K}[x_1, \ldots, x_n]$ such that $1 = g + h f_\ell^{\nu_\ell}$, which would imply $f^{(\ell)} = g f^{(\ell)} + h f \in \mathcal{I}$. Thus the set $\mathcal{A}_\ell$ is not empty. Now any ideal in $\mathcal{A}_\ell$ is an associated prime of $\mathcal{I}$ since $(\mathcal{I} + (f_\ell^{\nu_\ell})) : g = \mathcal{I} : (f_\ell^{(\ell)} g)$ for any g in $\mathbb{K}[x_1, \ldots, x_n]$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ denote the associated primes of $\mathcal{I}$, and let p_k be the monic generator of the ideal $\mathfrak{p}_k \cap \mathbb{K}[x_1]$. The general position of $\mathcal{I}$ ensures that the univariate irreducible polynomials p_k are pairwise coprime. Then we have $(f_1 \cdots f_s) = \sqrt{\mathcal{I} \cap \mathbb{K}[x_1]} = \bigcap_{k=1}^{r}(\mathfrak{p}_k \cap \mathbb{K}[x_1]) = (p_1 \cdots p_r)$, so that $s = r$ and we can assume that $f_k = p_k$ for $k \in \{1, \ldots, s\}$. Finally, since an ideal is always contained in any of its associated prime, we obtain $\mathcal{A}_\ell = \{\mathfrak{p}_\ell\}$. The ideal $\mathcal{I} + (f_\ell^{\nu_\ell})$ is primary. □

Proposition 1.5.2 yields the following algorithm, which is the core of the algorithm presented in [GTZ88].

Algorithm 1. *Gianni Trager Zacharias zero-dimensional primary decomposition*

Input: a zero-dimensional ideal $\mathcal{I}$ in general position.

Output: a set of pairs $(\mathcal{Q}_\ell, \mathfrak{p}_\ell)$ of ideals in $\mathbb{K}[x_1, \ldots, x_n]$ with $\mathfrak{p}_\ell = \sqrt{\mathcal{Q}_\ell}$ such that $\bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$ is a primary decomposition of $\mathcal{I}$.

1. Compute $f \in \mathbb{K}[x_1]$ such that $\mathcal{I} \cap \mathbb{K}[x_1] = (f)$.
2. Compute the factorization $f = f_1^{\nu_1} \cdots f_s^{\nu_s}$ of f in irreducible factors in $\mathbb{K}[x_1]$.
3. For ℓ from 1 to s,
   a. $\mathcal{Q}_\ell := \mathcal{I} + (f_\ell^{\nu_\ell})$;
   b. $\mathfrak{p}_\ell := \sqrt{\mathcal{Q}_\ell}$.
4. Return $(\mathcal{Q}_1, \mathfrak{p}_1), \ldots, (\mathcal{Q}_s, \mathfrak{p}_s)$.

Example 1.5.3. Let $\mathcal{I}$ be the zero-dimensional ideal $(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$, that is in general position in $\mathbb{K}[x_1, x_2]$. Then we have $\mathcal{I} \cap \mathbb{K}[x_1] = (x_1^2(x_1 - 1)(x_1 + 1))$. The algorithm returns $(\mathcal{Q}_1 = (x_1^2, x_2), \mathfrak{p}_1 = (x_1, x_2))$, $(\mathcal{Q}_2 = \mathfrak{p}_2 = (x_1 - 1, x_2 - 1))$ and $(\mathcal{Q}_3 = \mathfrak{p}_3 = (x_1 + 1, x_2 - 1))$.

Our presentation of the algorithm is quite schematic; more details can be found in the original paper [GTZ88] or in [GP02, Section 4.2]. Step 1 rely on a Gröbner basis computation with respect to a monomial ordering that eliminates $x_2, \ldots, x_n$. For step 3.b we need an

algorithm that, given a set of generators of an ideal $\mathcal{I}$, computes a set of generators of $\sqrt{\mathcal{I}}$; one can for instance use the algorithm presented by Krick and Logar in [KL91] (see also [GP02, Section 4.5]), which is based on the same idea of univariate reduction.

The general position hypothesis is not really restrictive: one can prove that for any zero-dimensional ideal, most of the linear change of variables put the ideal in general position (see [GTZ88, Proposition 7.1], [GP02, Proposition 4.2.2] or Corollary 4.3.12 below). The zero-dimensional hypothesis can also be removed by the use of a Noether position (see [GTZ88, Section 8] or [GP02, Section 4.3]).

Chapter 2

Dimension and Noether Position

The idea of the dimension of a variety in $\bar{\mathbb{K}}^n$ is quite intuitive; for instance, we would like to say that the parabola $\mathcal{V}(x_1 - x_2^2)$ has dimension 1 in the affine plane $\bar{\mathbb{K}}^2$. We recall in Section 2.1 the algebraic definition of dimension *via* transcendence degree. Noether positions are then a way to highlight the geometric meaning of this algebraic dimension, and a practical ingredient to compute it. General Noether positions, that correspond to Noether positions for projective varieties, will be an important tool to control the degree of Kronecker representations in Part II. We finish this chapter with genericity results on Noether positions that will be a key for Algorithm 7 in Part II.

In the whole chapter, $\mathbb{A}$ denotes a subring of $\mathbb{K}[x_1, \ldots, x_n]$ with unity.

2.1 Transcendence Degree and Dimension

The projection in the affine plane of the parabola $\mathcal{V}(x_2 - x_1^2)$ on the x_1-axis $\mathcal{V}(x_2)$ is finite and surjective; for that reason, we would like to say that the dimension of the parabola is one. Algebraic dependencies permit us to express this situation.

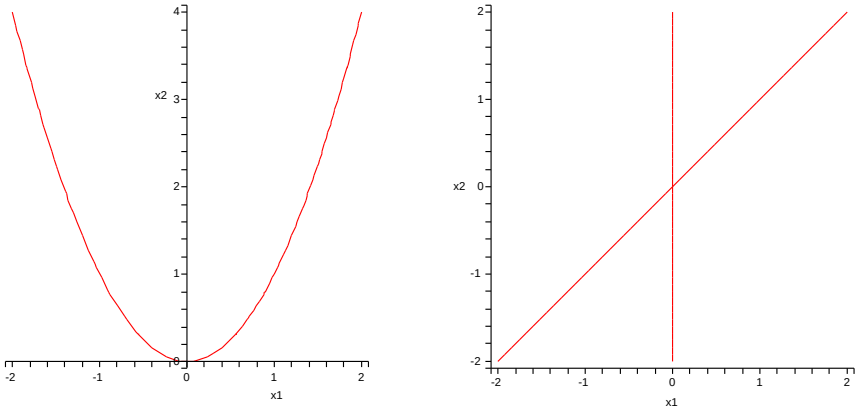
Definition 2.1.1. (a) Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are *algebraically dependent modulo* $\mathcal{I}$ if there exists a nonzero polynomial E with s variables over $\mathbb{K}$ such that $E(e_1, \ldots, e_s)$ belongs to $\mathcal{I}$. Otherwise they are *algebraically independent modulo* $\mathcal{I}$.

(b) A polynomial $e \in \mathbb{K}[x_1, \ldots, x_n]$ is *algebraic* over $\mathbb{A}$ modulo $\mathcal{I}$ if there exists a nonzero polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$.

(c) Such a polynomial e is *integral over* $\mathbb{A}$ *modulo* $\mathcal{I}$ if there exists a nonzero *monic* (*i.e.* with leading coefficient 1) polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$.

Example 2.1.2. In $\mathbb{K}[x_1, x_2]$, x_1 is algebraically independent modulo $(x_2 - x_1^2)$ and x_2 is integral over $\mathbb{K}[x_1]$ modulo $(x_2 - x_1^2)$. Geometrically speaking, the independency of x_1 ensures that to any value α of x_1 in $\bar{\mathbb{K}}$ corresponds a non empty set $\mathcal{V}_\alpha$ of points in $\mathcal{V}(x_2 - x_1^2)$, when the integrality of x_2 over x_1 ensures the finiteness of this set $\mathcal{V}_\alpha$ for any $\alpha \in \bar{\mathbb{K}}$ (here a single point).

Figure 2.1.3.



$\mathcal{V}(x_1 - x_2^2)$ $\mathcal{V}(x_1x_2 - x_1^2)$

The polynomial x_2 is not integral over $\mathbb{K}[x_1]$ modulo $(x_1x_2 - x_1^2)$: the variety $\mathcal{V}(x_1x_2 - x_1^2)$ contains the whole line $\mathcal{V}(x_1)$ over $x_1 = 0$ (see Figure 2.1.3).

Algebraic and integral dependencies are preserved when passing to the radical of $\mathcal{I}$, as detailed in the following proposition:

Proposition 2.1.4. *Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are algebraically independent modulo $\mathcal{I}$ if, and only if, they are algebraically independent modulo $\sqrt{\mathcal{I}}$. A polynomial e in $\mathbb{K}[x_1, \ldots, x_n]$ is algebraic (respectively, integral) over $\mathbb{A}$ modulo $\mathcal{I}$ if, and only if, it is algebraic (respectively, integral) over $\mathbb{A}$ modulo $\sqrt{\mathcal{I}}$.*

Proof. The proof is straightforward from the definitions. □

We will use the following classical properties several times:

Proposition 2.1.5. *Let e_1, e_2 be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.*

(a) If e_1 and e_2 are integral over $\mathbb{A}$ modulo $\mathcal{I}$ then so are $e_1 + e_2$ and e_1e_2.

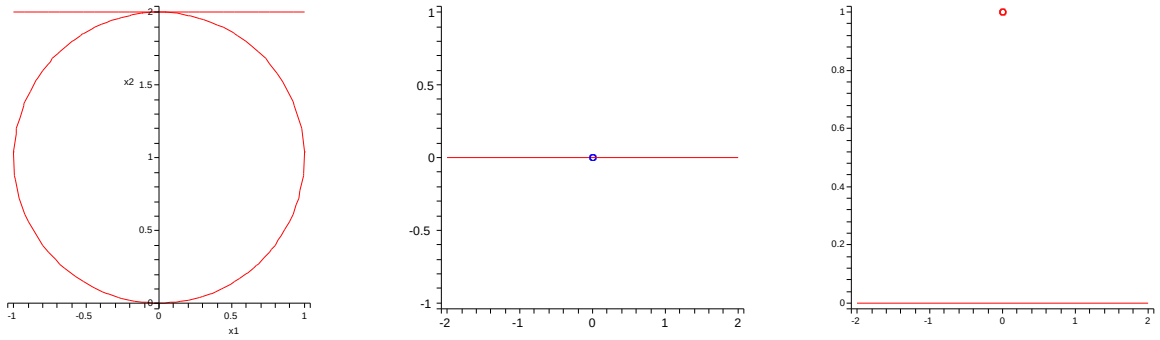
(b) If e_1 is integral over $\mathbb{A}$ modulo $\mathcal{I}$, and if e_2 is integral over $\mathbb{A}[e_1]$ modulo $\mathcal{I}$, then e_2 is integral over $\mathbb{A}$ modulo $\mathcal{I}$.

Proof. In both cases, $\mathbb{A}[e_1, e_2]$ is finitely generated as a free $\mathbb{A}$-module. Now, by the Cayley Hamilton theorem one obtains a relation of integral dependency over $\mathbb{A}$ for any $e \in \mathbb{A}[e_1, e_2]$ by evaluating in e the characteristic polynomial of the morphism of multiplication by e in $\mathbb{A}[e_1, e_2]$. □

The last algebraic tool that we need to define the dimension of an ideal is the following:

Definition 2.1.6. Let $\mathbb{F}$ be a field extension of $\mathbb{K}$. The *transcendence degree of $\mathbb{F}$ over $\mathbb{K}$* is the maximal number of elements in $\mathbb{F}$ that are algebraically independent.

Figure 2.1.9.



$\mathcal{V}((x_1^2+(x_2-1)^2-1)(x_2-2))$ $\mathcal{V}(x_2^2, x_1x_2)$ $\mathcal{V}((x_2)\cap(x_1, x_2-1))$

The computation of the transcendence degree of a field is made easier by the following classical result:

Proposition 2.1.7. *Let $\mathbb{F}$ be a field extension of $\mathbb{K}$ with finite transcendence degree r. Then any maximal (with respect to the inclusion ordering) subset of elements of $\mathbb{F}$ that are algebraically independent has cardinality r. Moreover, if Γ is a set of generators of $\mathbb{F}$ over $\mathbb{K}$ and if S is a subset of Γ whose elements are algebraically independents over $\mathbb{K}$, then there exists a subset $\mathcal{B}$ of Γ with cardinality r such that $S \subseteq \mathcal{B}$ and the elements of $\mathcal{B}$ are algebraically independent over $\mathbb{K}$.*

Proof. See for instance [Lan02, Chapter VIII, Section 1, Theorem 1.1]. □

Thus $\mathbb{K}[x_1, x_2]/(x_1 - x_2^2)$ is a field extension with degree 1 over $\mathbb{K}$ since x_1 is a maximal subset of algebraically independent elements in the set of generators $\{x_1, x_2\}$. This example suggests the following definition:

Definition 2.1.8. (a) If $\mathcal{I}$ is a prime ideal then the *dimension* $\dim(\mathcal{I})$ *of* $\mathcal{I}$ is the transcendence degree of the quotient field of $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ over $\mathbb{K}$.

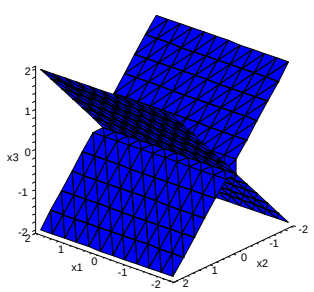
(b) In general, the dimension of $\mathcal{I} \neq (1)$ is the maximum of the dimensions of its associated primes. By convention, the ideal (1) has dimension -1.

(c) An ideal $\mathcal{I}$ is *unmixed* if the dimensions of its associated primes are all equal.

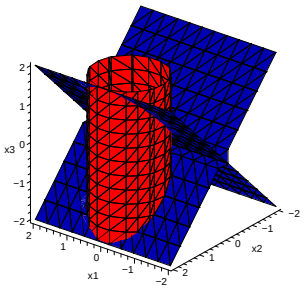
From a geometrical point of view, the dimension of an ideal $\mathcal{I}$ is thus the maximal dimension of the components of $\mathcal{V}(\mathcal{I})$, and $\mathcal{I}$ is unmixed when all the irreducible components of $\mathcal{V}(\mathcal{I})$ have same dimension. The ideals $(x_1 - x_2^2)$ and $((x_1^2+(x_2-1)^2-1)(x_2-2))$ are thus unmixed with dimension one, when $(x_2^2, x_1x_2) = (x_2) \cap (x_1, x_2^2)$ and $(x_1x_2, x_2^2 - x_2) = (x_2) \cap (x_1, x_2 - 1)$ have dimension one without being unmixed (see Figure 2.1.9).

Of course, any zero-dimensional ideal as defined in 1.4.11 is unmixed with dimension zero. Since all the associated primes of an unmixed ideal are isolated, Corollary 1.4.14 ensures that any unmixed ideal $\mathcal{I}$ admits a unique reduced primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$; in this case, the ideals $\mathcal{Q}_1, \ldots, \mathcal{Q}_\ell$ are called *primary components of* $\mathcal{I}$.

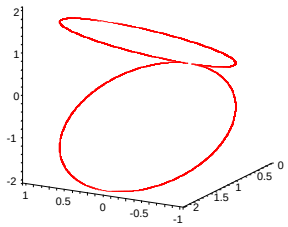
Figure 2.2.4.



$\mathcal{V}(x_3^2 - x_2^2)$



$\mathcal{V}(x_3^2 - x_2^2), \mathcal{V}((x_2-1)^2 + x_1^2 - 1)$



$\mathcal{V}(x_3^2 - x_2^2, (x_2-1)^2 + x_1^2 - 1)$

2.2 Noether Position

In this section, we generalize the situation observed in Example 2.1.2:

Definition 2.2.1. An ideal $\mathcal{I}$ is in *Noether position* if there exists $r \in \{0, \ldots, n\}$ such that the variables $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$, and such that $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

Example 2.2.2. The ideal $(x_2 - x_1^2)$ of Example 2.1.2 is in Noether position in $\mathbb{K}[x_1, x_2]$ with $r = 1$, when $(x_1 x_2 - x_1^2)$ is not. The ideals $(x_3^2 - x_2^2)$ and $(x_3^2 - x_2^2, (x_2-1)^2 + x_1^2 - 1)$ are in Noether position in $\mathbb{K}[x_1, x_2, x_3]$ with $r = 2$, respectively $r = 1$ by Proposition 2.1.5 (see Figure 2.2.4).

Remark 2.2.3. Any zero-dimensional ideal is in Noether position, with $r = 0$.

By Proposition 2.1.5, if $\mathcal{I}$ is in Noether position then any $e \in \mathbb{K}[x_1, \ldots, x_n]$ is integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, so that another way to say that $\mathcal{I}$ is in Noether position is to say that $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is an integral ring extension of $\mathbb{K}[x_1, \ldots, x_r]$. Geometrically speaking, as announced in Example 2.1.2, the algebraic independency of $x_1, \ldots, x_r$ modulo $\mathcal{I}$, respectively the integrality of $x_{r+1}, \ldots, x_n$ over $x_1, \ldots, x_r$, ensures that the projection of $\mathcal{V}(\mathcal{I})$ on $\mathcal{V}(x_{r+1}, \ldots, x_n)$ is surjective, respectively finite.

When $\mathcal{I} \neq (1)$, we are to show that the integer r in Definition 2.2.1 coincides with the dimension of $\mathcal{I}$. Of course, when $\mathcal{I} = (1)$, $\mathcal{I}$ is in Noether position with $r = 0$ while $\dim(\mathcal{I}) = -1$.

Theorem 2.2.5. *Assume that* $\mathcal{I} \neq (1)$.

(a) Assume that $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$. Then $\dim(\mathcal{I}) \leq r$. The latter inequality is an equality if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$.

(b) Assume that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$. Then we have $\dim(\mathcal{I}) \geq r$. If the latter inequality is an equality then $x_{r+1}, \ldots, x_n$ are algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$. The converse holds if $\mathcal{I}$ is unmixed.

Proof. In order to prove part (a), let us first assume that $\mathcal{I}$ is prime. Since any maximal subset of algebraically independent elements of $\{x_1, \ldots, x_r\}$ modulo $\mathcal{I}$ is also maximal in $\{x_1, \ldots, x_n\}$, part (a) follows from Proposition 2.1.7. If $\mathcal{I}$ is not prime, then we can assume that $\mathcal{I}$ is radical with prime decomposition $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ by Proposition 2.1.4. Since $x_{r+1}, \ldots, x_n$ remain integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo each $\mathfrak{p}_\ell$, we deduce that $\dim(\mathfrak{p}_\ell) \leq r$ for all $\ell \in \{1, \ldots, s\}$, whence $\dim(\mathcal{I}) \leq r$. If $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathcal{I}$ then they are also algebraically dependent modulo each $\mathfrak{p}_\ell$, for all $\ell \in \{1, \ldots, s\}$, whence $\dim(\mathcal{I}) < r$. Conversely, if $\dim(\mathcal{I}) < r$, then there exists $E_\ell \in \mathfrak{p}_\ell \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$ for all ℓ. Therefore $E_1 \cdots E_s$ belongs to $\mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$, whence the algebraically dependence of $x_1, \ldots, x_r$ over $\mathbb{K}$ modulo $\mathcal{I}$, which ends part (a).

Let us now deal with part (b). If $\mathcal{I}$ is prime then part (b) straightforwardly follows from Proposition 2.1.7. If $\mathcal{I}$ is not prime then we can assume again that $\mathcal{I}$ is radical with prime decomposition $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$. If $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$, then there necessarily exists $\ell \in \{1, \ldots, s\}$ such that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathfrak{p}_\ell$, whence $\dim(\mathcal{I}) \geq r$. If $x_{r+1}, \ldots, x_n$ are algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, then they are also algebraic modulo $\mathfrak{p}_\ell$, whence $\dim(\mathcal{I}) = \dim(\mathfrak{p}_\ell) = r$ whenever $\mathcal{I}$ is unmixed. Conversely, assume that $\dim(\mathcal{I}) = r$ holds, and let $i \in \{r+1, \ldots, n\}$. For each $\ell \in \{1, \ldots, s\}$, if $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathfrak{p}_\ell$ then we take $E_\ell \in \mathfrak{p}_\ell \cap \mathbb{K}[x_1, \ldots, x_r] \setminus \{0\}$; otherwise we take $E_\ell \in \mathfrak{p}_\ell \cap \mathbb{K}[x_1, \ldots, x_r, x_i] \setminus \{0\}$. Since $E_1 \cdots E_s \in \mathcal{I}$, it follows that x_i is algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$, which ends part (b). □

Example 2.2.6. If $n = 3$ and $\mathcal{I} = (x_1x_2 - 1, x_3) \cap (x_1)$ then x_1 is algebraically independent modulo $\mathcal{I}$, and x_2, x_3 are algebraic over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$. Since $\dim(\mathcal{I}) = 2$, this shows that we can not discard the unmixedness hypothesis in Theorem 2.2.5(b). This example also shows that Theorem 2.2.5(a) does not hold if $x_{r+1}, \ldots, x_n$ are only supposed to be algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

Example 2.2.7. If $n = 2$ and $\mathcal{I} = (x_1x_2-1) \cap (x_1, x_2)$ then x_1 is algebraically independent modulo $\mathcal{I}$, x_2 is algebraic over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, and $\dim(\mathcal{I}) = 1$. This shows that the unmixedness hypothesis in Theorem 2.2.5(b) is too strong.

Remark 2.2.8. It can be observed that the Noether position is preserved when extending the ground field. Therefore if $\mathcal{I}$ is in Noether position then Theorem 2.2.5 implies that $\dim(\mathcal{I})$ does not depend on the ground field $\mathbb{K}$.

Remark 2.2.9. Noether positions can be used as a tool for reducing dimension by specializing the independent variables. For instance, if we let $\mathcal{I} = (x_1 - x_2^2)$, the ideal $\mathcal{I} + (x_1)$ has dimension zero when $\mathcal{I}$ has dimension one. This method is a key of the good cost of the Kronecker solver since it permits us to deal only with ideals with dimension zero or one.

2.3 General Noether Position

In this section, we extend the notion of Noether position to projective varieties. This stronger Noether position will allow us to control the degrees of Kronecker representations of ideals in Part II.

For any $e \in \mathbb{K}[x_1, \ldots, x_n]$, we denote by $e^\sharp \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ the *homogenization* of e with respect to the new variable x_0, and by $\mathcal{I}^\sharp \subseteq \mathbb{K}[x_0, x_1, \ldots, x_n]$ the ideal generated by the homogenized polynomials of $\mathcal{I}$. For any $e \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ we write $e^\flat$ for $e(1, x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$.

Algebraic independencies are preserved by homogenizing:

Lemma 2.3.1. *Some polynomials $e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are algebraically dependent modulo $\mathcal{I}$ if, and only if, $x_0, e_1^\sharp, \ldots, e_s^\sharp$ are algebraically dependent modulo $\mathcal{I}^\sharp$.*

Proof. If $e_1, \ldots, e_s$ are algebraically dependent modulo $\mathcal{I}$ then, by homogenizing, we directly obtain that $x_0, e_1^\sharp, \ldots, e_s^\sharp$ are algebraically dependent modulo $\mathcal{I}^\sharp$. Conversely, let E be a nonzero polynomial over $\mathbb{K}$ such that $E(x_0, e_1^\sharp, \ldots, e_s^\sharp) \in \mathcal{I}^\sharp$. Since $\mathcal{I}^\sharp$ is homogeneous, we can assume that E is homogeneous for the weighted degree $(1, \deg(e_1), \ldots, \deg(e_s))$. The conclusion thus follows by substituting 1 for x_0 in $E(x_0, e_1^\sharp, \ldots, e_s^\sharp) \in \mathcal{I}^\sharp$. □

The same property is not true for integral dependencies, which yields the following definition:

Definition 2.3.2. A polynomial $e \in \mathbb{K}[x_1, \ldots, x_n]$ is *generally integral* over $\mathbb{A}$ modulo $\mathcal{I}$ if there exists a nonzero monic polynomial $q \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$, and such that

$$\deg(q(x_1, \ldots, x_n, T^{\deg(e)})) = \deg_T(q(x_1, \ldots, x_n, T^{\deg(e)})), \tag{2.3.1}$$

where q is seen in $\mathbb{K}[x_1, \ldots, x_n, T]$.

Example 2.3.3. The monomial x_2 is generally integral over $\mathbb{K}[x_1]$ modulo $(x_2^2 - x_1)$ whereas it is not modulo $(x_2 - x_1^2)$.

For any subring $\mathbb{A}$ of $\mathbb{K}[x_1, \ldots, x_n]$, we write $\mathbb{A}^\sharp$ for the subring of $\mathbb{K}[x_0, x_1, \ldots, x_n]$ generated by x_0 and by the homogenized polynomials of $\mathbb{A}$. For example, if $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r]$ then $\mathbb{A}^\sharp$ is $\mathbb{K}[x_0, x_1, \ldots, x_r]$. The following properties are direct consequences of the definition:

$$\forall e \in \mathbb{A}^\sharp,\ e^\flat \in \mathbb{A}, \tag{2.3.2}$$

$$\forall e \in \mathbb{A}^\sharp,\ \text{any homogeneous component of } e \text{ belongs to } \mathbb{A}^\sharp. \tag{2.3.3}$$

Assertion (2.3.3) is equivalent to saying that $\mathbb{A}^\sharp$ inherits the usual graduation of $\mathbb{K}[x_0, x_1, \ldots, x_n]$.

Lemma 2.3.4. *Let $e \in \mathbb{K}[x_1, \ldots, x_n]$. The following assertions are equivalent:*

(a) e is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$.

(b) $e^\sharp$ is generally integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$.

(c) $e^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$.

Proof. If (a) holds then there exists a polynomial $q = T^\alpha + a_1 T^{\alpha-1} + \cdots + a_\alpha \in \mathbb{A}[T]$ such that $q(e) \in \mathcal{I}$, and such that equality (2.3.1) holds. It thus follows that

$$(e^\sharp)^\alpha + x_0^{\deg(e)-\deg(a_1)} a_1^\sharp (e^\sharp)^{\alpha-1} + \cdots + x_0^{\alpha\deg(e)-\deg(a_\alpha)} a_\alpha^\sharp \in \mathcal{I}^\sharp,$$

which leads to (b). Of course (b) implies (c). If (c) holds then there exists a polynomial $q = T^\alpha + a_1 T^{\alpha-1} + \cdots + a_\alpha \in \mathbb{A}^\sharp[T]$ such that $q(e^\sharp) \in \mathcal{I}^\sharp$. By property (2.3.3), we can take all the a_i homogeneous of degree $i\deg(e)$, so that we obtain (a) from property (2.3.2). □

Proposition 2.1.5 does not extend nicely to generally integral dependencies. Nevertheless, we have the following weaker properties:

Proposition 2.3.5. *Let e_1, e_2 be in $\mathbb{K}[x_1, \ldots, x_n]$.*

(a) If e_1 and e_2 are generally integral over $\mathbb{A}$ modulo $\mathcal{I}$, then so is always $e_1 e_2$, and so is $e_1 + e_2$ whenever $\deg(e_1 + e_2) = \max(\deg(e_1), \deg(e_2))$.

(b) If $\mathbb{A}$ inherits the usual graduation of $\mathbb{K}[x_1, \ldots, x_n]$, if e_1 is homogeneous and generally integral over $\mathbb{A}$ modulo $\mathcal{I}$, and if e_2 is generally integral over $\mathbb{A}[e_1]$ modulo $\mathcal{I}$, then e_2 is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$.

Proof. We start with part (a). Without loss of generality we can assume that $\deg(e_1) \geq \deg(e_2)$. We know from Lemma 2.3.4 that $e_1^\sharp$ and $e_2^\sharp$ are integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$; so are $(e_1 + e_2)^\sharp = e_1^\sharp + x_0^{\deg(e_1)-\deg(e_2)} e_2^\sharp$ and $(e_1 e_2)^\sharp = e_1^\sharp e_2^\sharp$ by Proposition 2.1.5(a). Part (a) thus follows from Lemma 2.3.4.

As for part (b), we proceed in a similar manner: $e_1^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$, and $e_2^\sharp$ is integral over $(\mathbb{A}[e_1])^\sharp$ modulo $\mathcal{I}^\sharp$. Thanks to the hypotheses on $\mathbb{A}$ and e_1, we obtain that $(\mathbb{A}[e_1])^\sharp = \mathbb{A}^\sharp[e_1^\sharp]$, so that Proposition 2.1.5(b) implies that $e_2^\sharp$ is integral over $\mathbb{A}^\sharp$ modulo $\mathcal{I}^\sharp$. Part (b) thus follows from Lemma 2.3.4 again. □

Example 2.3.6. Let $\mathbb{K} = \mathbb{Q}[\imath]$, with $\imath = \sqrt{-1}$, let $\mathcal{I} = (x_2 - x_1^2)$, $e_1 = x_2 + \imath x_1^2$, and $e_2 = -\imath x_1^2$. Of course e_2 is generally integral over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, and since $e_1^2 - 2\imath x_1^2 e_1 - 2x_1^4 \in \mathcal{I}$ so is e_1. Because $e_1 + e_2 = x_2$ is not generally integral over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$, the hypothesis $\deg(e_1 + e_2) = \max(\deg(e_1), \deg(e_2))$ is necessary in Proposition 2.3.5(a). In addition, since $x_2 - e_1/(1+\imath) \in \mathcal{I}$, we have that x_2 is generally integral over $\mathbb{K}[x_1, e_1]$ modulo $\mathcal{I}$, which shows that the homogeneity of e_1 is necessary in Proposition 2.3.5(b). Finally, from $x_1^2 - e_1/(1+\imath) \in \mathcal{I}$ we obtain that x_1 is homogeneous and generally integral over $\mathbb{K}[e_1]$ modulo $\mathcal{I}$. Since we have already seen that x_2 is generally integral over $\mathbb{K}[x_1, e_1]$ modulo $\mathcal{I}$, this shows that the graduation hypothesis on $\mathbb{A}$ is necessary in Proposition 2.3.5(b).

In general the Noether position of $\mathcal{I}$ does not imply the Noether position of $\mathcal{I}^\sharp$ (consider $(x_2 - x_1^2)$ in $\mathbb{K}[x_1, x_2]$). In order for $\mathcal{I}^\sharp$ to be in Noether position, we need to strengthen the definition.

Definition 2.3.7. An ideal $\mathcal{I}$ of dimension r is in *general Noether position* if $\mathcal{I}$ is in Noether position, and if the variables $x_{r+1}, \ldots, x_n$ are generally integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.

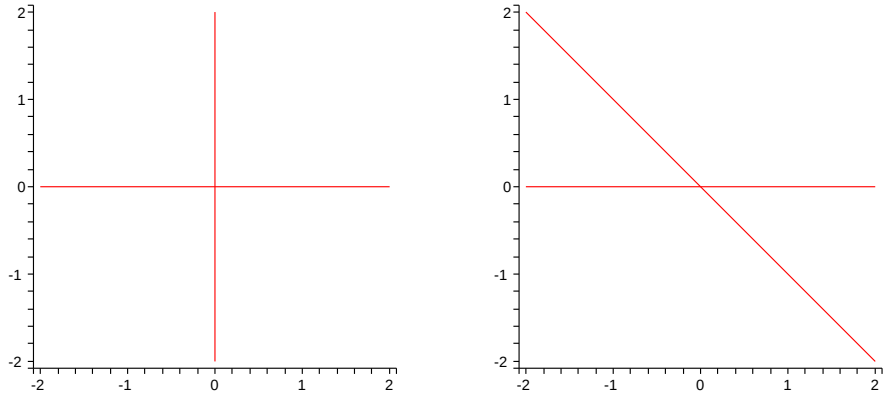
Since $\mathbb{K}[x_1, \ldots, x_r]$ inherits the usual graduation of $\mathbb{K}[x_1, \ldots, x_n]$, Lemma 2.3.4 implies that the Noether and the general Noether positions coincide whenever $\mathcal{I}$ is homogeneous.

Example 2.3.8. The ideal $(x_2^2 - x_1)$ is in general Noether position in $\mathbb{K}[x_1, x_2]$, when $(x_2 - x_1^2)$ is not.

Proposition 2.3.9. *If $\mathcal{I}$ has dimension r and is in general Noether position then any $e \in \mathbb{K}[x_1, \ldots, x_n]$ is generally integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.*

Proof. This property is a direct consequence of Proposition 2.3.5(a). □

Figure 2.4.1.



$\mathcal{V}(x_1x_2)$ $\mathcal{V}(x_2^2 + x_1x_2)$

2.4 Genericity and Noether Positions

Given an ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$, there is *a priori* no reason that it is in Noether position even after a permutation of the variables. For example, (x_1x_2) is not in Noether position when seen in $\mathbb{K}[x_1, x_2]$ nor in $\mathbb{K}[x_2, x_1]$. In fact, we are to prove that almost all linear changes of the variables in $\mathcal{I}$ produces a new ideal in Noether position. For example, by substituting x_1+x_2 for x_1 in (x_1x_2), we obtain the new ideal $(x_2^2 + x_1x_2)$ which is Noether position (see Figure 2.4.1).

For any $n \times n$ matrix M over $\mathbb{K}$, we write $\mathcal{I} \circ M$ for the ideal $\{f \circ M(x_1, \ldots, x_n)^t \mid f \in \mathcal{I}\}$. The existence of a general Noether position will follow from a repeated use of the following lemma:

Lemma 2.4.2. *Let $i \in \{1, \ldots, n\}$ and assume that $x_{i+1}, \ldots, x_n$ are integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_i]$ modulo $\mathcal{I}$, and that $x_1, \ldots, x_i$ are algebraically dependent modulo $\mathcal{I}$. Then, for any nonzero polynomial $a \in \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_i]$, and for any point $(\alpha_1, \ldots, \alpha_{i-1}, 1) \in \mathbb{K}^i$ that does not annihilate the homogeneous component h of highest degree of a, the variables $x_i, \ldots, x_n$ are integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_{i-1}]$ modulo $\mathcal{I} \circ M$, where M is defined by*

$$M(x_1, \ldots, x_n)^t = (x_1 + \alpha_1 x_i, \ldots, x_{i-1} + \alpha_{i-1}x_i, x_i, \ldots, x_n)^t.$$

In addition, we have that $\deg_{x_i}(a \circ M) = \deg(a \circ M)$.

Proof. By a straightforward calculation we obtain that the coefficient of $x_i^{\deg(a)}$ in $a(x_1 + \alpha_1 x_i, \ldots, x_{i-1} + \alpha_{i-1}x_i, x_i)$ is $h(\alpha_1, \ldots, \alpha_{i-1}, 1)$. Therefore, if the latter quantity is nonzero then x_i is generally integral over $\mathbb{K}[x_1, \ldots, x_{i-1}]$ modulo $\mathcal{I} \circ M$. Since $x_{i+1}, \ldots, x_n$ remain integral (respectively, generally integral) over $\mathbb{K}[x_1, \ldots, x_i]$, the conclusion follows from Proposition 2.1.5(b) (respectively, Proposition 2.3.5(b)). □

Theorem 2.4.3. *Let $\mathcal{I}$ be any proper ideal in $\mathbb{K}[x_1, \ldots, x_n]$. There exists a Zariski dense subset of upper triangular $n \times n$ matrices M with 1 on their diagonal such that $\mathcal{I} \circ M$ is general Noether position.*

Proof. Let M be an upper triangular matrix with 1 on its diagonal, written in the following form:

$$M = \begin{pmatrix} 1 & \alpha_{1,2} & \dots & \alpha_{1,n} \\ 0 & 1 & \dots & \alpha_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

For all $i \in \{1, \dots, n\}$ we define the $n \times n$ matrix M_i by:

$$M_i(x_1, \dots, x_n)^t = (x_1 + \alpha_{1,i}x_i, \dots, x_{i-1} + \alpha_{i-1,i}x_i, x_i, \dots, x_n)^t.$$

A straightforward calculation shows that $M = M_n \cdots M_1$. Let $r = \dim(\mathcal{I})$. Since $M_r \cdots M_1$ only affects the variables $x_1, \dots, x_r$, we see that $\mathcal{I} \circ M$ is in general Noether position if, and only if, $\mathcal{I} \circ M_n \cdots M_{r+1}$ is in general Noether position. Therefore the theorem follows from the following stronger claim: for any $i \in \{r, \dots, n\}$, there exists a Zariski dense subset of values for $(\alpha_{k,l} | i+1 \leq l \leq n, 1 \leq k \leq l-1)$ such that $x_{i+1}, \dots, x_n$ are generally integral over $\mathbb{K}[x_1, \dots, x_i]$ modulo $\mathcal{I} \circ M_n \cdots M_{i+1}$.

The proof of the claim is done by descending induction on i. If $i = n$ then the claim holds trivially. Assume that the claim is true for some $i \in \{r+1, \dots, n\}$. Since $i \geq r+1$, Theorem 2.2.5(a) implies that $x_1, \dots, x_i$ can not be algebraically independent modulo $\mathcal{I} \circ M_n \cdots M_{i+1}$. Then Lemma 2.4.2 asserts that there exists a Zariski dense subset of values for $(\alpha_{k,i} | 1 \leq k \leq i-1)$ for which $x_i, \dots, x_n$ are generally integral over $\mathbb{K}[x_1, \dots, x_{i-1}]$ modulo $\mathcal{I} \circ M_n \cdots M_i$, which completes the proof of the claim. □

Corollary 2.4.4. *Theorem 2.4.3 holds if we replace the space of the upper triangular matrices with 1 on their diagonal by the whole space of the invertible matrices.*

Proof. The set of matrices M such that all their principal minors are nonzero is dense. It is classical that such a matrix M can be uniquely written as the product of a lower triangular matrix L by an upper triangular matrix U with 1 on its diagonal. Since $\mathcal{I} \circ L$ is in general Noether position if, and only if, $\mathcal{I}$ is itself in general Noether position, the conclusion follows from Theorem 2.4.3. □

From the existence of general Noether positions, we can now deduce:

Corollary 2.4.5. *If* $\mathcal{I} \neq (1)$ *then* $\dim(\mathcal{I}^\sharp) = \dim(\mathcal{I}) + 1$.

Proof. Thanks to Theorem 2.4.3, we can assume that $\mathcal{I}$ is in general Noether position. Therefore the conclusion follows from Lemmas 2.3.1 and 2.3.4, and Theorem 2.2.5(a). □

The proof of Theorem 2.4.3 directly gives an algorithm to compute general Noether position for an ideal $\mathcal{I}$ (which is similar to [GP02, Algorithm 3.4.5]):

Algorithm 2. *Noether Position*

Input: an ideal $\mathcal{I}$.

Output: a matrix M such that $\mathcal{I} \circ M$ is in general Noether position, and the dimension r of $\mathcal{I}$.

1. Initialize i with n and M with the identity matrix.
2. While $(\mathcal{I} \circ M) \cap \mathbb{K}[x_1, \ldots, x_i] \neq \emptyset$ do
   a. choose $a \in \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_i]$;
   b. let h be the homogeneous component of highest degree of a;
   c. choose $(\alpha_1^{(i)}, \ldots, \alpha_{i-1}^{(i)}, 1) \in \mathbb{K}^i$ that does not annihilate h;
   d. for k from 1 to $i-1$ replace $M_{i,k}$ with $\alpha_k^{(i)}$;
   e. decrease i by 1.
3. Return i and M.

The test of step 2 together with step 2.a can be performed *via* a Gröbner basis computation with a monomial ordering that eliminates $x_{i+1}, \ldots, x_n$. Evaluating a non constant polynomial h on randomly chosen points, one should quickly find a point that does not annihilate h, which permits to perform step 2.c. When considering complexity, notice that we only need to find out a point that does not vanish a polynomial; the polynomial itself does not need to be explicity written down. This observation led to the first breakthrough with evaluation techniques due to Giusti and Heintz in [GH93].

Chapter 3

Primary Decomposition of Zero-dimensional Ideals

In this chapter, we focus on zero-dimensional ideals. As announced in Corollary 1.4.14 of Chapter 1, such ideals have a unique primary decomposition, whose computation is the purpose of Part III. In the whole chapter, we deal with $\bar{\mathbb{K}}^n$, so that the maximal ideals in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ are exactly the ideals $(x_1 - p_1, \ldots, x_n - p_n)$ with $p = (p_1, \ldots, p_n) \in \bar{\mathbb{K}}^n$. The variety defined by any zero-dimensional ideal is thus a finite set of points, whose multiplicity structures are described by the corresponding primary ideals.

We first present localizations as a way to isolate primary ideals, and define multiplicities as the dimensions of local algebras. Then we traduce the primary decomposition of an ideal in terms of local algebras. In Section 3.3, we propose an algorithm to recover a primary ideal from its local algebra; this algorithm is inspired from [FGLM93].

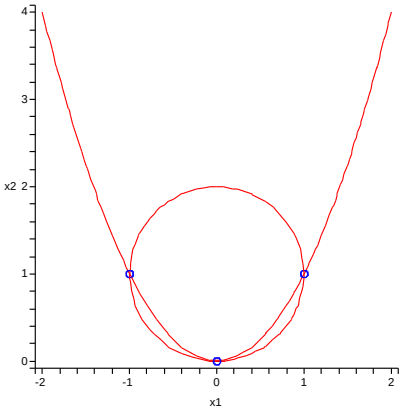
3.1 Local Algebra of a Root

A classical way to study a variety $\mathcal{V} \subseteq \bar{\mathbb{K}}^n$ is to examine the coordinate ring $\bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I}(\mathcal{V})$, which can be thought of as the ring of polynomial functions on $\mathcal{V}$. To focus on the information in a neighborhood of p, one often considers rational functions defined at the point, that is, whose denominator does not vanish when evaluated in p. Using the Taylor formula, one easily get convinced that it is equivalent to deal with the ring $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$ of formal power series in $x_1 - p_1, \ldots, x_n - p_n$. For computational motivation, we will prefer the second ring: it may be easier to control the size of truncated series than to estimate the degrees of numerators and denominators of rational fractions.

Definition 3.1.1. Let $p = (p_1, \ldots, p_n)$ be an element in $\bar{\mathbb{K}}^n$, and $\mathcal{I}$ be any ideal of $\bar{\mathbb{K}}[x_1, \ldots, x_n]$. The *localization* $\mathcal{I}_p$ *of* $\mathcal{I}$ *in* p is the ideal $\mathcal{I}$ extended to the ring $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$ of formal power series over $\bar{\mathbb{K}}$.

The units of $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$ are exactly the polynomials that do not vanish in p.

Figure 3.1.2.



$\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$

For instance, if

$$\mathcal{I} = (x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2) = (x_1^2(x_1 - 1)(x_1 + 1), x_2 - x_1^2),$$

then we have $\mathcal{I}_{(0,0)} = (x_1^2, x_2)$. The latter ideal describes the structure of the origin at the intersection of the circle and the parabola, namely, the tangency of the x_1-axis (see Figure 3.1.2). Let us recall from Example 1.4.5 in Chapter 1 that the primary decomposition of $\mathcal{I}$ is

$$\mathcal{I} = (x_1^2, x_2) \cap (x_1 + 1, x_2 - 1) \cap (x_1 - 1, x_2 - 1).$$

By localizing in $(0, 0)$, we just keep the primary ideal with associated prime (x_1, x_2). Localizations can thus be seen as a way to "isolate" primary ideals:

Proposition 3.1.3. *Let $\mathcal{I}$ be a zero-dimensional ideal in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ with reduced primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$. For $\ell \in \{1, \ldots, s\}$, let $p^{(\ell)}$ denote the only point in $\mathcal{V}(\mathcal{Q}_\ell)$. Then for any $\ell \in \{1, \ldots, s\}$, we have $\mathcal{I}_{p^{(\ell)}} = (\mathcal{Q}_\ell)_{p^{(\ell)}}$. In addition, we have that $\mathcal{I}_{p^{(\ell)}} \cap \bar{\mathbb{K}}[x_1, \ldots, x_n] = \mathcal{Q}_\ell$.*

Proof. For $k \neq \ell$, there exists $i_k \in \{1, \ldots, n\}$ such that $p_{i_k}^{(k)} \neq p_{i_k}^{(\ell)}$. Then since $\sqrt{\mathcal{Q}_k} = (x_1 - p_1^{(k)}, \ldots, x_n - p_n^{(k)})$, the ideal $\mathcal{Q}_k$ contains a power of $x_{i_k} - p_{i_k}^{(k)}$, that is a unit in $\bar{\mathbb{K}}[[x_1 - p_1^{(\ell)}, \ldots, x_n - p_n^{(\ell)}]]$. We thus have $(\mathcal{Q}_k)_{p^{(\ell)}} = \bar{\mathbb{K}}[[x_1 - p_1^{(\ell)}, \ldots, x_n - p_n^{(\ell)}]]$ for any $k \neq \ell$, so that $\mathcal{I}_{p^{(\ell)}} = \bigcap_{k=1}^{s} (\mathcal{Q}_k)_{p^{(\ell)}} = (\mathcal{Q}_\ell)_{p^{(\ell)}}$. Let $f \in (\mathcal{Q}_\ell)_{p^{(\ell)}} \cap \mathbb{K}[x_1, \ldots, x_n]$. There exists $g \notin \sqrt{\mathcal{Q}_\ell}$ such that $fg \in \mathcal{Q}_\ell$, so that f belongs to the primary ideal $\mathcal{Q}_\ell$. The result straightforwardly follows from the equality $\mathcal{I}_{p^{(\ell)}} = (\mathcal{Q}_\ell)_{p^{(\ell)}}$. □

We now define local algebras and multiplicities:

Definition 3.1.4. Let $p = (p_1, \ldots, p_n) \in \bar{\mathbb{K}}^n$ and $\mathcal{I}$ be an ideal of $\bar{\mathbb{K}}[x_1, \ldots, x_n]$.

(a) The *local algebra of p as a root of $\mathcal{I}$* is the $\bar{\mathbb{K}}$-algebra

$$\mathbb{D}_p = \bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]/\mathcal{I}_p.$$

(b) The *multiplicity μ_p of p as a root of $\mathcal{I}$* is the dimension of the $\bar{\mathbb{K}}$-algebra $\mathbb{D}_p$.

Example 3.1.5. The algebra of the origin $(0,0)$ as a root of $\mathcal{I} = (x_1^2 + (x_2-1)^2 - 1, x_2 - x_1^2)$ is $\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, x_2]]/(x_1^2, x_2)$, and the one of $(-1,1)$ is $\mathbb{D}_{(-1,1)} = \bar{\mathbb{K}}[[x_1+1, x_2-1]]/(x_1+1, x_2-1)$. The origin thus has multiplicity two, and $(-1,1)$ has multiplicity one.

If $f = \alpha \prod_{\ell=1}^{s} (x - p^{(\ell)})^{\nu_\ell}$ is a univariate polynomial in $\bar{\mathbb{K}}[x]$, then for any $\ell \in \{1, \ldots, s\}$, we have $(f)_{p^{(\ell)}} = (x - p^{(\ell)})^{\nu_\ell}$, so that Definition 3.1.4(b) coincide with the usual definition of the multiplicity of a root.

In the multivariate case, that is when $n \geq 2$, two zeros may have same multiplicities with distinct structures, as shown by the primary ideals (x_1^3, x_2), (x_1^2, x_1x_2, x_2^2). In Part II, we focus on the computation of the roots together with their multiplicities. The calculation of the local algebras is the purpose of Part III.

Remark 3.1.6. If $\mathcal{I}$ is a zero-dimensional ideal with reduced primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$, if $p^{(\ell)}$ denote the only point in $\mathcal{V}(\mathcal{Q}_\ell)$ for some $\ell \in \{1, \ldots, s\}$, then Proposition 3.1.3 ensures that $\mathbb{D}_{p^{(\ell)}}$ equals $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]/(\mathcal{Q}_\ell)_{p^{(\ell)}}$.

Remark 3.1.7. Let $\mathcal{I}$ be a zero-dimensional ideal, g be a polynomial in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$, and $p \in \bar{\mathbb{K}}^n$ be a root of $\mathcal{I}$. Then p is a root of $\mathcal{I} : g^\infty$ if and only if g does not vanish when evaluated in p. In the latter case, g is a unit of $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$, so that the local algebras of p as a root of $\mathcal{I}$ and $\mathcal{I} : g^\infty$ coincide.

3.2 Decomposition in Local Algebras

In this section, we traduce the primary decomposition of a zero-dimensional ideal $\mathcal{I}$ in terms of local algebras, and give some classic consequences of this new representation of primary decomposition.

Theorem 3.2.1. *Let $\mathcal{I}$ be a zero-dimensional ideal with reduced primary decomposition $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$, and for $\ell \in \{1, \ldots, s\}$, let $p^{(\ell)}$ be the only point in $\mathcal{V}(\mathcal{Q}_\ell)$. Then the following isomorphism of $\bar{\mathbb{K}}$-algebras holds:*

$$\bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I} \simeq \mathbb{D}_{p^{(1)}} \times \cdots \times \mathbb{D}_{p^{(s)}}.$$

Proof. For $\ell \in \{1, \ldots, s\}$, for any polynomial $f \in \bar{\mathbb{K}}[x_1, \ldots, x_n]$, we let $[f]_\ell$ denote the coset of f in $\mathbb{D}_{p^{(\ell)}}$. We let Φ be the morphism of algebras

$$\Phi : \left\{ \begin{array}{ccc} \bar{\mathbb{K}}[x_1, \ldots, x_n] & \longrightarrow & \mathbb{D}_{p^{(1)}} \times \cdots \times \mathbb{D}_{p^{(s)}} \\ f & \longmapsto & ([f]_1, \ldots, [f]_s) \end{array} \right. .$$

The ideal $\mathcal{I}$ is obviously included in the kernel of Φ. Now, if f is an element that vanishes Φ, then for any $\ell \in \{1, \ldots, s\}$, f belongs to $(\mathcal{Q}_\ell)_{p^{(\ell)}} \cap \bar{\mathbb{K}}[x_1, \ldots, x_n] = \mathcal{Q}_\ell$ by Proposition 3.1.3. The kernel of Φ thus equals $\mathcal{I} = \bigcap_{\ell=1}^{s} \mathcal{Q}_\ell$. □

Example 3.2.2. For the ideal $\mathcal{I} = (x_1^2 + (x_2-1)^2 - 1, x_2 - x_1^2)$ in $\bar{\mathbb{K}}^2$, we thus have

$$\bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I} \simeq \mathbb{D}_{(0,0)} \times \mathbb{D}_{(-1,1)} \times \mathbb{D}_{(1,1)}.$$

The degree of a univariate polynomial equals the sum of the multiplicities of all its distinct roots, which generalizes in:

Corollary 3.2.3. *Let $\mathcal{I}$ be a zero-dimensional ideal, and let $p^{(1)}, \ldots, p^{(s)}$ denote the elements of $\mathcal{V}(\mathcal{I})$. For $\ell \in \{1, \ldots, s\}$, let μ_ℓ denote the multiplicity of $p^{(\ell)}$ as a root of $\mathcal{I}$. Then $\bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I}$ is a finite dimensional $\bar{\mathbb{K}}$-algebra with dimension $\sum_{\ell=1}^{s} \mu_{p^{(\ell)}}$.*

Proof. It directly follows from Theorem 3.2.1 by considering dimensions. □

The following consequence of Theorem 3.2.1 will be widely used in Part II for the representation of multiplicities; it is sometimes refered as the *Stickelberger Theorem*.

Proposition 3.2.4. *Let $\mathcal{I}$ be a zero-dimensional ideal in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$, and let $p^{(1)}, \ldots, p^{(s)}$ denote the distinct zeros of $\mathcal{I}$, with multiplicities $\mu_{p^{(1)}}, \ldots, \mu_{p^{(s)}}$. For $f \in \bar{\mathbb{K}}[x_1, \ldots, x_n]$, let $\chi \in \bar{\mathbb{K}}[T]$ denote the characteristic polynomial of the morphism m_f of multiplication by f in $\mathbb{B} = \bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I}$. Then we have*

$$\chi(T) = \prod_{\ell=1}^{s} (f(p^{(\ell)}) - T)^{\mu_{p^{(\ell)}}}.$$

Proof. Let us first examine the case when $\mathcal{I}$ is a primary ideal $\mathcal{Q}$, with only root p in $\bar{\mathbb{K}}^n$. Then Corollary 3.2.3 ensures that the dimension of the $\bar{\mathbb{K}}$-vector space $\mathbb{B} = \bar{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{Q}$ equals the multiplicity μ_p of p as a root of $\mathcal{Q}$. Thus we just have to prove that the only eigenvalue of m_f is $f(p)$. For $\lambda \in \bar{\mathbb{K}}$, let g_λ be the polynomial $f - \lambda$: if λ is an eigenvalue of m_f, then there exists a polynomial $h \notin \mathcal{Q}$ such that $g_\lambda h \in \mathcal{Q}$: g_λ is a zerodivisor in $\mathbb{B}$. Now if $\lambda \neq f(p)$, then $1 - g_\lambda/g_\lambda(p)$ belongs to $\mathcal{I}(\{p\}) = \mathcal{I}(\mathcal{V}(\mathcal{Q})) = \sqrt{\mathcal{Q}}$, so that $(1 - g_\lambda/g_\lambda(p))^N$ belongs to $\mathcal{Q}$ for some positive integer N. By expanding $(1 - g_\lambda/g_\lambda(p))^N$, one obtains that g_λ is a unit of $\mathbb{B}$. Therefore any $\lambda \neq f(p)$ cannot be an eigenvalue of m_f. This ends the proof in the case when $\mathcal{I} = \mathcal{Q}$ is primary.

If the ideal $\mathcal{I}$ is not primary, Theorem 3.2.1 allows us to consider χ as the characteristic polynomial of its image $[m_f]$ in $\mathbb{D}_{p^{(1)}} \times \cdots \times \mathbb{D}_{p^{(s)}}$. Now for any $\ell \in \{1, \ldots, s\}$, Theorem 3.2.1 again ensures that $\mathbb{D}_{p^{(\ell)}}$ is isomorphic to $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{Q}_\ell$, so that the restriction of $[m_f]$ to $\mathbb{D}_{p^{(\ell)}}$ has characteristic polynomial $(f(p^\ell) - T)^{\mu_\ell}$. □

Example 3.2.5. The characteristic polynomial of the morphism of multiplication by x_1 in $\mathbb{K}[x_1, x_2]/(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ is $T^2(T - 1)(T + 1)$.

3.3 From Local Algebras to Primary Ideals

To any primary ideal $\mathcal{Q}$ in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ with only root p, we can associate the local algebra $\mathbb{D}_p$ of p as a root of $\mathcal{Q}$. Conversely, to any local algebra $\mathbb{D}_p$ corresponds a unique primary ideal $\mathcal{Q}$ with associated prime $(x_1 - p_1, \ldots, x_n - p_n)$. In this section, we provide the reader with an algorithm to recover $\mathcal{Q}$ from p and $\mathbb{D}_p$.

Firstly, we have to say how we encode the different objects. It is quite natural to depict an ideal as a set of generators. One often compute a local algebra $\mathbb{D}_p$ under the form of the matrices $M_{x_1}, \ldots, M_{x_n}$ of the morphisms of multiplication by the variables $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}_p$: indeed, these matrices allow all the computations in $\mathbb{D}_p$. For instance, $\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, x_2]]/(x_1^2, x_2)$ will be represented by

$$M_{x_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } M_{x_2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

which are the matrices of multiplication by x_1, x_2 in the basis $1, x_1$ of $\mathbb{D}_0$.

We now give an algorithm inspired from [FGLM93] to recover the primary ideal corresponding to a given local algebra. For that purpose, we let *lex* denote the lexicographic ordering on the monomials of $\mathbb{K}[x_1, \ldots, x_n]$, for which $x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n}$ if the first nonzero entry of the vector $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) \in \mathbb{Z}^n$ is positive. The *leading monomial* of a polynomial is the greatest monomial with nonzero coefficient.

Algorithm 3. *FGLM*

Input: the matrices $M_{x_1}, \ldots, M_{x_n}$ of the morphisms of multiplication by the variables $x_1, \ldots, x_n$ with respect to a basis of a local algebra $\mathbb{D}$.

Output: a Gröbner basis of the $(x_1, \ldots, x_n)$-primary ideal $\mathcal{Q}$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $\mathbb{D} \simeq \mathbb{K}[[x_1, \ldots, x_n]]/\mathcal{Q}$.

1. Initialize G and LG with the empty set.
2. Initialize $\mathcal{B}$ with the empty set.
3. Initialize m with 1.
4. While LG does not contain a positive power of x_1,
   a. let $\tilde{m}$ be the monomial m evaluated in $(M_{x_1}, \ldots, M_{x_n})$;
   b. if the elements of $\mathcal{B} \cup \{\tilde{m}\}$ are linearly independent, then add $\tilde{m}$ to $\mathcal{B}$;
   c. else
      i. let g be a relation of linear dependency,
      ii. add g to G and m to LG;
   d. replace m with the next monomial in lexicographic order that is not a multiple of an element of LG.
5. Return G.

Proposition 3.3.1. *Algorithm 3 is correct.*

Proof. See for instance [FGLM93] or [CLO05, Chapter 2, Section 3]. □

Example 3.3.2. Let us run Algorithm 3 on the matrices

$$M_{x_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } M_{x_2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

At the end of the first round through the while loop, $\mathcal{B}$ contains the identity matrix Id, $G = LG = \emptyset$ and $m = x_2$. The second round yields $\mathcal{B} = \{\mathrm{Id}\}$, $G = LG = \{x_2\}$ and $m = x_1$. Finally the third round leads to $\mathcal{B} = \{\mathrm{Id}, M_{x_1}\}$, $G = LG = \{x_2, x_1^2\}$. We thus recover the (x_1, x_2)-primary ideal (x_1^2, x_2).

Example 3.3.3. In Example 10.3.5, we will obtain the matrices

$$M_{x_1} = \begin{pmatrix} 0 & -4\frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & 1+4\frac{1}{16} & 0 \end{pmatrix}, \; M_{x_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } M_{x_3} = \begin{pmatrix} 0 & \frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{1}{16} & 0 \end{pmatrix}.$$

Algorithm 3 applied to $M_{x_1}, M_{x_2}, M_{x_3}$ returns the primary ideal $(x_1^2, x_1x_3, x_3^2, x_2)$.

Computing zero-dimensional primary decompositions as pairs of roots and local algebras is quite classical. One finds in [ABRW96] an algorithm that calculates the decomposition of the quotient ring into local algebras by linear algebra from a Gröbner basis of the ideal. Another classical way to obtain the local algebra of a given isolated root is to compute a standard basis with respect to a local ordering by using the tangent cone algorithm of [Mor91]; a discussion on the different ways to represent the multiplicity structure of an isolated root can be found in [MMM96]. The algorithms of [DZ05, Mou97] take advantage of the evaluation property of the input system. Indeed, given a polynomial system $f_1 = \cdots = f_s = 0$ together with an isolated root $p \in \mathbb{K}^n$, this algorithm computes the matrices of multiplication by the variables with respect to a basis of the local algebra of p as a root of $(f_1, \ldots, f_s)$ thanks to the duality between polynomials and formal power series in differential operators. But the bound on the cost of the algorithm given in [Mou97, Proposition 4.1] still depends on *the number of monomials obtained by derivation of the monomials of* $f_1, \ldots, f_s$, which can yield to a combinatorial number; although we believe that the latter cost is pessimistic, we did not found a better estimate in the literature. For the first time, our algorithm underlying in Part III computes the primary decomposition of a zero-dimensional ideal by pure evaluation techniques, with a cost that does not involve a number of monomials up to a certain regularity.

Part II

Computation of the Radical: Global Solving

The purpose of this thesis is the computation of the roots of a zero-dimensional system together with the structure of their local algebras. In this part, we present the Kronecker solver designed in [GLS01, Lec01], which computes the roots of a zero-dimensional system. For the first time, we give a self contained proof of the good working of the solver, and we extend it so that it further calculates the multiplicities of the roots without an extra cost. Most of the proofs presented in this part can also be found in [DL07].

The input polynomial system is given by a sequence of equations $f_1 = \cdots = f_n = 0$ and an inequation $g \neq 0$, where $f_1, \ldots, f_n$ and g belong to $\mathbb{K}[x_1, \ldots, x_n]$. In practice these polynomials are expected to be represented by an evaluation data structure (a straight-line program, for instance). The Kronecker solver designed in [GLS01] computes the roots of the system $f_1 = \cdots = f_n = 0, g \neq 0$ in the form

$$q(T) = 0, \begin{cases} x_1 &= v_1(T), \\ &\vdots \\ x_n &= v_n(T), \end{cases}$$

where $q, v_1, \ldots, v_n \in \mathbb{K}[T]$; we call such a sequence $q, v_1, \ldots, v_n$ *univariate representation* of the radical ideal $\sqrt{(f_1, \ldots, f_n) : g^\infty}$. If the ideal $\mathcal{I}_n = (f_1, \ldots, f_n) : g^\infty$ is not radical, we prove that the algorithm also computes a polynomial $\chi \in \mathbb{K}[T]$ which square-free part is q, and such that for any root α of q in $\bar{\mathbb{K}}$, the multiplicity of $(v_1(\alpha), \ldots, v_n(\alpha))$ as a root of $\mathcal{I}_n$ equals the one of α as a root of χ. We will refer to such a sequence $\chi, q, v_1, \ldots, v_n$ as *univariate representation of $\mathcal{I}_n$ with multiplicities*.

The Kronecker algorithm solves the equations $f_1, \ldots, f_n$ in sequence. To be more precise, let us introduce the intermediate ideals

$$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty, \text{ for } i \in \{1, \ldots, n\};$$

by convention we let $\mathcal{I}_0 = (0)$. The version considered in [GLS01] requires the following hypotheses:

$$f_{i+1} \text{ is a nonzerodivisor modulo } \mathcal{I}_i, \text{ and } \mathcal{I}_i \text{ is radical, for all } i \in \{0, \ldots, n-1\};$$

in this case, we say that $f_1, \ldots, f_n$ is a *reduced regular sequence in the open subset* $\{g \neq 0\}$. These requirements imply in particular that the dimension of $\mathcal{I}_i$ is $n - i$.

Using genericity results as the one proved in Chapter 2 for Noether positions, we will see that, after performing a random affine change of the variables in the input system, the algorithm can safely compute the finite sets of zeros of the ideals

$$\mathcal{J}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i})}$$

in sequence for i from 1 to n, with a high probability of success. The set of zeros of $\mathcal{J}_i$ is represented by i univariate polynomials $q, w_{n-i+2}, \ldots, w_n$ in $\mathbb{K}[x_{n-i+1}]$ such that

$$\mathcal{J}_i = (q, q'x_{n-i+2} - w_{n-i+2}, \ldots, q'x_n - w_n) + (x_1, \ldots, x_{n-i}).$$

We call such a representation *Kronecker representation* of $\mathcal{J}_i$.

The computation of a Kronecker representation of $\mathcal{J}_{i+1}$ from a representation of $\mathcal{J}_i$ divides into the following three steps:

1. *Lifting step.* Compute a Kronecker representation of $\mathcal{K}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})}$.

2. *Intersection step.* Compute a representation of $\sqrt{\mathcal{K}_i + (f_{i+1})}$.

3. *Cleaning step.* Compute a representation of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$.

Of course the algorithm stops as soon as it encounters an empty set of solutions, that is as soon as $\mathcal{I}_i = (1)$. Geometrically speaking, $\mathcal{K}_i$ is a one-dimensional ideal whose set of zeros is a solution curve of the ith first equations. Then, during the intersection step, we compute the intersection of the latter curve with the hypersurface defined by $f_{i+1} = 0$. This intersection is made of a finite set of points, from which we remove the ones contained in the hypersurface defined by $g = 0$ during the cleaning step.

In Chapter 4, we define the different representations of ideals. We take advantage of their univariate character to reduce the cleaning step to a gcd computation.

The cornerstone of the Kronecker solver is the intersection step presented in Chapter 5. It consists in computing a univariate representation of a zero-dimensional ideal $\mathcal{I} + (f)$ from the one of a one-dimensional radical ideal $\mathcal{I}$. This calculation is made possible by Proposition 5.3.1. Moreover, the formula that follows from this proposition permits to give a global intersection algorithm that computes a univariate representation of $\mathcal{I} + (f)$ with multiplicities. Proposition 5.3.1 is also the starting point of the local intersection algorithm presented in Part III.

In Chapter 6, we explain how to specialize the representations, and how to recover the whole representation from a specialized one. This lifting operation relies on the good properties of Kronecker representations: we can easily recover polynomials in $\mathbb{K}[x_1, \ldots, x_r][T]$ from their specializations at $x_1 = \cdots = x_r = 0$ by a Newton-Hensel lifting as soon as we have a bound on their degrees. This specialization and lifting process permit to deal with ideals of dimension zero and one.

We finish Part II with a complete presentation of the Kronecker solver. In the case when $f_1, \ldots, f_n$ is a reduced regular sequence in the open subset $\{g \neq 0\}$, all the intermediate ideals $\mathcal{I}_i$ are radical, so that multiplicities do not appear until the last intersection step. Applying our new intersection algorithm to $\mathcal{K}_{n-1} = \mathcal{I}_{n-1}$ and f_n, we can obtain a univariate representation of $(f_1, \ldots, f_n) : g^\infty$ with multiplicities. These ideas are developped in Chapter 7, together with a Bertini lemma that permits us to discard hypotheses on the input: by taking random linear combinations of the generators of any square zero-dimensional system, one can safely assume that the equations form a reduced regular sequence.

Chapter 4

Univariate Representations and Cleaning Step

In this chapter, we properly define the representations announced in the introduction for ideals in Noether position. For that purpose, we let $\mathcal{I}$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ with $\mathcal{I} \neq (1)$, and we write $r \geq 0$ for the dimension of $\mathcal{I}$. In addition we will use the following notation:

$$\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r], \quad \mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I},$$

$$\mathbb{A}' = \mathbb{K}(x_1, \ldots, x_r), \quad \mathbb{B}' = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}',$$

where $\mathcal{I}'$ denotes the extension of $\mathcal{I}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$.

The ring $\mathbb{B}$ can naturally be seen as an $\mathbb{A}$-module, whose torsion-freeness is related to the unmixedness of $\mathcal{I}$. If $\mathcal{I}$ is in Noether position, then $\mathbb{B}'$ is a $\mathbb{A}'$-vector space of finite dimension. Some suitable characteristic and minimal polynomials in $\mathbb{B}'$ will lead to define univariate representations. We conclude this chapter with the *cleaning step* algorithm.

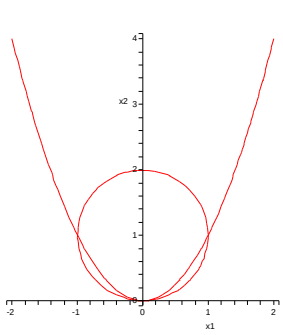
4.1 Unmixedness and Torsion

The following proposition gives us a useful criterion for testing the unmixedness of $\mathcal{I}$:

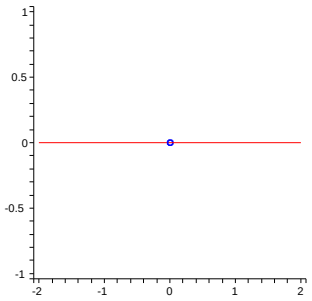
Proposition 4.1.1. *Assume that $\mathcal{I}$ is in Noether position. Then $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module if, and only if, $\mathcal{I}$ is unmixed.*

Proof. Let $\mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_s$ represent a reduced primary decomposition of $\mathcal{I}$, with associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. By Theorem 2.2.5(a), the ideal $\mathcal{I}$ is unmixed if, and only if, $\mathbb{A} \cap \mathfrak{p}_\ell = (0)$, for all $\ell \in \{1, \ldots, s\}$. On the other hand, the fact that $\mathbb{B}$ has torsion reformulates into the following property: there exist $a \in \mathbb{A} \setminus \{0\}$ and $b \notin \mathcal{I}$ such that $ab \in \mathcal{I}$. If $\mathbb{B}$ has torsion then there exist $a \in \mathbb{A} \setminus \{0\}$, $\ell \in \{1, \ldots, s\}$, and b such that $ab \in \mathcal{Q}_\ell$ and $b \notin \mathcal{Q}_\ell$. Therefore we must have $a \in \mathfrak{p}_\ell$, hence $\mathcal{I}$ is not unmixed. Conversely, if $\mathcal{I}$ is not unmixed then there exists $a \in (\mathbb{A} \cap \mathfrak{p}_\ell) \setminus \{0\}$ for some ℓ, hence some power of a is a torsion element for $\mathbb{B}$. □

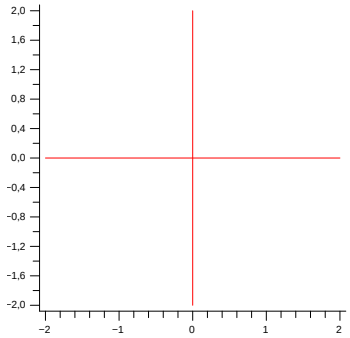
Figure 4.1.2.



$\mathcal{V}((x_1^2+(x_2-1)^2-1)(x_2-x_1^2))$



$\mathcal{V}((x_2)\cap(x_1^2,x_1x_2,x_2^2))$



$\mathcal{V}(x_1x_2)$

Example 4.1.3. The $\mathbb{K}[x_1]$-module $\mathbb{K}[x_1,x_2]/((x_1^2+(x_2-1)^2-1)(x_2-2))$ is torsion-free, when x_1 is a torsion element in $\mathbb{K}[x_1,x_2]/((x_2)\cap(x_1^2,x_1x_2,x_2^2))$.

Example 4.1.4. If $\mathcal{I}=(x_1x_2)\subseteq\mathbb{K}[x_1,x_2]$ then $\mathcal{I}$ is unmixed with dimension 1 but $\mathbb{B}$ has torsion. This example shows that the Noether position is necessary in Proposition 4.1.1.

Corollary 4.1.5. *If $\mathcal{I}$ is radical, then $\mathcal{I}'$ is radical. The converse holds if $\mathcal{I}$ is unmixed.*

Proof. Let $b\in\mathbb{A}'[x_{r+1},\ldots,x_n]$, and assume that b^m belongs to $\mathcal{I}'$ for some positive integer m. There exists $a\in\mathbb{A}$ such that ab^m belongs to $\mathcal{I}$. Then ab belongs to the radical ideal $\mathcal{I}$, so that b belong to $\mathcal{I}'$: the ideal $\mathcal{I}'$ is radical. Conversely, let $f\in\mathbb{K}[x_1,\ldots,x_n]$ be such that f^m belongs to $\mathcal{I}$ for some positive integer m. Then f belongs to the radical ideal $\mathcal{I}'$, so that there exists $a\in\mathbb{A}$ such that af belongs to $\mathcal{I}$. The unmixedness of $\mathcal{I}$ ensures that f belongs to $\mathcal{I}$ by Proposition 4.1.1, which proves the radicality of $\mathcal{I}$. □

Example 4.1.6. If $\mathcal{I}=(x_2)\cap(x_1^2,x_1x_2,x_2^2)$, then $\mathcal{I}'=(x_2)$ but $\mathcal{I}$ is not radical. This example shows that the unmixedness of $\mathcal{I}$ is in general necessary in Corollary 4.1.5.

If $\mathcal{I}$ is an unmixed ideal, removing primary components of $\mathcal{I}$ does not affect the unmixed nature of $\mathcal{I}$, as says the following corollary of Proposition 4.1.1:

Corollary 4.1.7. *Assume that $\mathcal{I}$ is unmixed, and let g in $\mathbb{K}[x_1,\ldots,x_n]$ be such that $\mathcal{I}:g^\infty\neq(1)$. Then $\mathcal{I}:g^\infty$ is unmixed with dimension r. If $\mathcal{I}$ is in Noether position or in general Noether position then so is $\mathcal{I}:g^\infty$.*

Proof. Without loss of generality we can assume that $\mathcal{I}$ is in Noether position (respectively, general Noether position), by Theorem 2.4.3. From Proposition 4.1.1 we know that $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module. Therefore the assumption $\mathcal{I}:g^\infty\neq(1)$ implies that $x_1,\ldots,x_r$ are algebraically independent modulo $\mathcal{I}:g^\infty$. On the other hand, the inclusion $\mathcal{I}\subseteq\mathcal{I}:g^\infty$ gives us that $x_{r+1},\ldots,x_n$ are integral (respectively, generally integral) over $\mathbb{A}$ modulo $\mathcal{I}:g^\infty$. It follows that $\mathcal{I}:g^\infty$ inherits the Noether position of $\mathcal{I}$ (respectively, general Noether position), whence $\dim(\mathcal{I}:g^\infty)=r$ by Theorem 2.2.5(a). Finally, the torsion-freeness of $\mathbb{B}$ implies the one of $\mathbb{K}[x_1,\ldots,x_n]/(\mathcal{I}:g^\infty)$, and Proposition 4.1.1 completes the proof. □

Example 4.1.8. Let $\mathcal{I}=((x_1^2+(x_2-1)^2-1)(x_2-2))$. The ideal $\mathcal{I}:(x_2-2)^\infty=(x_1^2+(x_2-1)^2-1)$ is unmixed in general Noether position in $\mathbb{K}[x_1,x_2]$ with same dimension one as $\mathcal{I}$.

4.2 Characteristic and Minimal Polynomials

In the case of an unmixed curve in Noether position, that is when $\mathcal{I}$ is unmixed in Noether position with dimension 1, then $\mathbb{A} = \mathbb{K}[x_1]$ is a principal ideal domain, and the torsion-free module $\mathbb{B}$ is a finitely generated free module (see [Lan02, Chapter III, Theorem 7.3]). In this situation, one can naturally speak about the characteristic and minimal polynomials of the endomorphism of multiplication by any f in $\mathbb{B}$. In this section, we study polynomials with similar properties under the only hypothesis that $\mathbb{B}$ is torsion-free.

If $\mathcal{I}$ is any ideal in Noether position, then $\mathbb{B}'$ is a $\mathbb{A}'$-vector space of finite dimension, so that, for any f in $\mathbb{K}[x_1, \ldots, x_n]$, we can define $\chi \in \mathbb{A}'[T]$ (respectively, μ) as the characteristic (respectively, minimal) polynomial of the endomorphism of multiplication by f in $\mathbb{B}'$. In short, we will respectively call them the *characteristic* and the *minimal* polynomials of f modulo $\mathcal{I}$.

Theorem 4.2.1. *Assume that $\mathcal{I}$ is in Noether position, and let $d = \deg(f)$.*

(a) χ and μ belong to $\mathbb{A}[T]$. In addition, if $\mathcal{I}$ and f are homogeneous, then $\chi(T^d)$ and $\mu(T^d)$ are homogeneous when seen in $\mathbb{K}[x_1, \ldots, x_r, T]$.

(b) If the Noether position is general then the total degrees of $\chi(T^d)$ and $\mu(T^d)$ seen in $\mathbb{K}[x_1, \ldots, x_r, T]$ equal their respective partial degree in T.

(c) If $\mathcal{I}$ is unmixed then $\chi(f)$ and $\mu(f)$ belong to $\mathcal{I}$.

Proof. Since f is integral over $\mathbb{A}$ modulo $\mathcal{I}$ by Proposition 2.1.5, there exists a monic polynomial $q \in \mathbb{A}[T]$ such that $q(f) \in \mathcal{I}$. Since $q(f) = 0$ holds in $\mathbb{B}'$, the minimal polynomial μ divides q in $\mathbb{A}'[T]$. In particular, all the irreducible factors of μ divide q. Since q and these factors are monic in T, the classical Gauss lemma [Lan02, Chapter IV, Theorem 2.1] implies that all these factors actually belong to $\mathbb{A}[T]$, so do μ and χ. If $\mathcal{I}$ and f are homogeneous then q can be chosen so that $q(T^d)$ is homogeneous. Therefore all the irreducible factors of $\mu(T^d)$ are homogeneous, which concludes part (a).

If the Noether position is general then Proposition 2.3.9 implies that f is generally integral over $\mathbb{A}$ modulo $\mathcal{I}$. We can thus take q such that equality (2.3.1) holds. This equality between the degrees hold for any irreducible factor of q, hence for μ and χ, which concludes part (b).

Since $\mu(f) \in \mathcal{I}'$, there exist $a \in \mathbb{A} \setminus \{0\}$ and $b \in \mathcal{I}$ such that $\mu(f) = b/a$. Thus we have $a\mu(f) = 0$ in $\mathbb{B}$. By Proposition 4.1.1, $\mathbb{B}$ is torsion-free, whence $\mu(f) \in \mathcal{I}$. The same proof holds for χ, which concludes part (c). □

Example 4.2.2. With $\mathcal{I} = (x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ and $f = x_1$ in $\mathbb{K}[x_1, x_2]$, we have $\chi = \mu = T^2(T-1)(T+1)$. With the ideal $\mathcal{I} = (x_1^2 + (x_2 - 1)^2 + 1, x_3^2 - x_2^2)$ (see Figure 2.2.4) and $f = x_2$ in $\mathbb{K}[x_1, x_2, x_3]$, we have $\chi = \mu^2 = (x_2^2 - 2x_2 + x_1^2)^2$.

Example 4.2.3. With $\mathcal{I} = (x_2) \cap (x_1^2, x_1x_2, x_2^2) = (x_2^2, x_1x_2)$ and $f = x_2 + 1$, we have $\mathcal{I}' = (x_2)$ and $\mu = T - 1$ but $\mu(f) = x_2 \notin \mathcal{I}$. Therefore it is necessary to assume that $\mathcal{I}$ is unmixed in Theorem 4.2.1(c).

Example 4.2.4. Theorem 4.2.1(b) does not hold if the Noether position is not general as exemplified by taking $\mathcal{I} = (x_2 - x_1^2)$ and $f = x_2$ so that $\mu = T - x_1^2$.

4.3 Univariate Representation

In this section, we assume that $\mathcal{I}$ is in Noether position, and we let δ denote the dimension of the $\mathbb{A}'$-vector space $\mathbb{B}'$. To define a univariate representation of a zero-dimensional ideal as announced in the introduction of Part II, we need a function that takes different values on the distinct roots of the ideal. For a radical unmixed ideal, we search such a "separating function" as a linear form in the independent variables:

Proposition 4.3.1. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Let $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ be a $\mathbb{K}$-linear form. Then, $\mathcal{I}'$ is radical, and the following assertions are equivalent:*

(a) The powers of u generate $\mathbb{B}'$.

(b) The degree of the minimal polynomial of u in $\mathbb{B}'$ equals δ.

(c) There exist unique polynomials $q, v_{r+1}, \ldots, v_n$ in $\mathbb{A}'[T]$ such that $\mathcal{I}' = (q(u), x_{r+1} - v_{r+1}(u), \ldots, x_n - v_n(u))$, q is monic, and $\deg(v_j) \leq \deg(q) - 1$ for all $j \in \{r+1, \ldots, n\}$.

(d) There exist unique polynomials $q, w_{r+1}, \ldots, w_n$ in $\mathbb{A}'[T]$ such that $\mathcal{I}' = (q(u), q'(u)x_{r+1} - w_{r+1}(u), \ldots, q'(u)x_n - w_n(u))$, q is monic, and $\deg(w_j) \leq \deg(q) - 1$ for all $j \in \{r+1, \ldots, n\}$.

Proof. We consider the morphism ψ from $\mathbb{A}'[T]$ to $\mathbb{B}'$ that sends T to u. Since its kernel is generated by the minimal polynomial of u in $\mathbb{B}'$, each of the four assertions are equivalent to saying that $\mathbb{B}'$ is isomorphic to $\mathbb{A}'[T]/\ker(\psi)$. □

Definition 4.3.2. (a) A linear form u satisfying assertions (a)–(d) of Proposition 4.3.1 is a *primitive element* for $\mathcal{I}$.

(b) The polynomials $q, v_{r+1}, \ldots, v_n$ in assertion (c) form a *univariate representation* of $\mathcal{I}$.

(c) The polynomials $q, w_{r+1}, \ldots, w_n$ in assertion (d) form a *Kronecker representation* of $\mathcal{I}$.

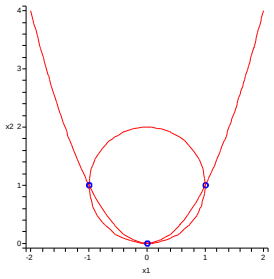
Example 4.3.3. The computation of Example 4.2.2 prove that x_2 is not primitive for the radical unmixed ideal in Noether position $(x_1^2+(x_2-1)^2-1, x_3^2-x_2^2)$. Let $f_1 = (x_1+2x_2+4x_3)^2+(x_2-1)^2+1$ and $f_2 = x_3^2 - x_2^2$ in $\mathbb{K}[x_1, x_2, x_3]$. The one-dimensional ideal (f_1, f_2) is radical unmixed in Noether position with primitive element x_2. Its univariate representation with respect to x_2 is

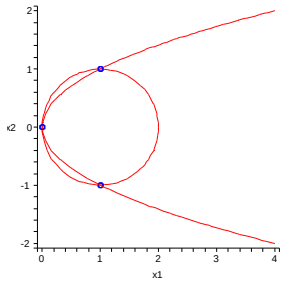
$$\begin{cases} q = & x_2^4 & + & \frac{(84-88x_1)}{185}x_2^3 & + & \frac{(4-6x_1^2)}{185}x_2^2 & + & \frac{(x_1^3+x_1^2)}{185}x_2 & + & \frac{x_1^4}{185} \\ v_3 = & & & \frac{370}{136x_1^2+32x_1}x_2^3 & - & \frac{361x_1-168}{136x_1^2+32x_1}x_2^2 & - & \frac{10x_1^2-10x_1-8}{136x_1^2+32x_1}x_2 & - & \frac{13x_1^3-4x_1^2}{136x_1^2+32x_1}, \end{cases}$$

in which we omit to mention $v_2 = x_2$. One easily deduce that its Kronecker representation with respect to x_2 is

$$\begin{cases} q = & x_2^4 & + & \frac{(84-88x_1)}{185}x_2^3 & + & \frac{(4-6x_1^2)}{185}x_2^2 & + & \frac{(x_1^3+x_1^2)}{185}x_2 & + & \frac{x_1^4}{185} \\ w_3 = & & & -\frac{208x_1-64}{185}x_2^3 & + & \frac{64x_1^2}{185}x_2^2 & + & \frac{16x_1^3}{185}x_2. & & \end{cases}$$

Figure 4.3.5.





$\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ $\mathcal{V}((x_1 - 1)^2 + x_2^2 - 1, x_2^2 - x_1)$

Remark 4.3.4. If $\mathcal{I}$ is any zero-dimensional ideal, then the linear form $u = \lambda_1 x_1 + \cdots + \lambda_n x_n$ is a primitive element for the radical ideal $\sqrt{\mathcal{I}}$ of $\mathcal{I}$ if and only if it takes distinct values when evaluated at the different roots of $\mathcal{I}$ in $\bar{\mathbb{K}}^n$. For instance, x_1 is a primitive element for $\sqrt{(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)}$, with corresponding univariate representation

$$q = x_1(x_1 - 1)(x_1 + 1), v_1 = x_1, v_2 = x_1^2.$$

On the other hand, x_1 is not a primitive element for $\sqrt{((x_1 - 1)^2 + x_2^2 - 1, x_2^2 - x_1)}$, since it takes the same value on both roots $(1, -1)$ and $(1, 1)$ (see Figure 4.3.5).

Let $\mathcal{I}$ be any zero-dimensional ideal, and let $q, v_1, \ldots, v_n$ denote the univariate representation of $\sqrt{\mathcal{I}}$ with respect to a primitive element u. Let χ be the characteristic polynomial of u in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$, so that q is the square-free part of χ. For any root $\alpha \in \bar{\mathbb{K}}$ of χ, the multiplicity of $(v_1(\alpha), \ldots, v_n(\alpha))$ as a root of $\mathcal{I}$ equals the one of α as a root of χ by Proposition 3.2.4. This yields the following definition:

Definition 4.3.6. Let $\mathcal{I}$ be an unmixed ideal in Noether position, and let u be a primitive element for the radical ideal $\sqrt{\mathcal{I}}$. Let $q, v_{r+1}, \ldots, v_n$ denote the univariate representation of $\sqrt{\mathcal{I}}$ for the primitive element u, and let χ be the characteristic polynomial of u modulo $\mathcal{I}$. We call the sequence $\chi, q, v_{r+1}, \ldots, v_n$ *univariate representation of* $\mathcal{I}$ *with multiplicities for the primitive element* u.

Example 4.3.7. The univariate representation with multiplicities of $(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ for the primitive element x_1 is

$$\chi = x_1^2(x_1 - 1)(x_1 + 1), q = x_1(x_1 - 1)(x_1 + 1), v_1 = x_1, v_2 = x_1^2.$$

Remark 4.3.8. Sequences $\chi, v_{r+1}, \ldots, v_n$ also bear the name of *rational univariate representations* in [ABRW96] and [Rou99]. The authors of [GLS01] actually deal with *geometric resolutions* of ideals that are made up of a change of variables that put the ideal in Noether position, a primitive element, and the corresponding univariate representation.

Remark 4.3.9. Univariate representations with multiplicities do not give an exact representation of the ideal. Indeed, the ideals (x_1^4, x_2, x_3) and (x_1^2, x_2^2, x_3) have the same representations for the primitive element $x_1 + x_2$. Nevertheless, it gives a first piece of information, that will be precious for the computation of Part III.

Although Theorem 4.2.1 ensures that the polynomial q of a univariate representation belongs to $\mathbb{A}[T]$, Example 4.3.3 shows that $v_{r+1}, \ldots, v_n$ are rational functions in the free variables

$x_1, \ldots, x_r$. We are to prove that the elements $w_{r+1}, \ldots, w_n$ of a Kronecker representation belong to $\mathbb{A}[T]$, which will be a central fact for the lifting step in Section 6.2. For this purpose, we let $\Lambda_{r+1}, \ldots, \Lambda_n$ be new auxiliary variables, and we introduce the following objects:

$$\mathbb{K}_\Lambda = \mathbb{K}(\Lambda_{r+1}, \ldots, \Lambda_n), \ \mathbb{A}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_r],$$

$$\mathbb{A}'_\Lambda = \mathbb{K}(\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_r), \text{ and } \mathbb{B}'_\Lambda = \mathbb{A}'_\Lambda[x_{r+1}, \ldots, x_n]/\mathcal{I}'_\Lambda,$$

where $\mathcal{I}'_\Lambda$ denotes the extension of $\mathcal{I}$ to $\mathbb{A}'_\Lambda[x_{r+1}, \ldots, x_n]$. We write $\mathcal{I}_\Lambda$ for the extension of $\mathcal{I}$ to $\mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]$ and we let

$$\mathbb{B}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]/\mathcal{I}_\Lambda.$$

We introduce the $\mathbb{K}_\Lambda$-linear form $u_\Lambda = \Lambda_{r+1}x_{r+1} + \cdots + \Lambda_n x_n$. The minimal polynomial of u_Λ in $\mathbb{B}'_\Lambda$ is written q_Λ, and we let

$$w_{\Lambda,j} = -\frac{\partial q_\Lambda}{\partial \Lambda_j}, \text{ for all } j \in \{r+1, \ldots, n\}.$$

Proposition 4.3.10. *Assume that $\mathcal{I}$ is unmixed and in Noether position.*

(a) $\mathcal{I}$ is radical if, and only if, q_Λ is square-free.

(b) If $\mathcal{I}$ is radical then u_Λ is primitive for $\mathcal{I}_\Lambda$, q_Λ belongs to $\mathbb{A}_\Lambda[T]$, $q_\Lambda(u_\Lambda)$ belongs to $\mathcal{I}_\Lambda$, and q_Λ is homogeneous of degree δ when seen as a polynomial in $\mathbb{A}'[\Lambda_{r+1}, \ldots, \Lambda_n, T]$. In addition, if the Noether position is general, then the total degree of q_Λ is δ when seen in $\mathbb{K}_\Lambda[x_1, \ldots, x_r, T]$.

Proof. It is easy to check that $\mathcal{I}_\Lambda$ is in Noether position and unmixed with dimension n. From Theorem 4.2.1, we know that $q_\Lambda \in \mathbb{A}_\Lambda[T]$ and that

$$q_\Lambda(u_\Lambda) \in \mathcal{I}_\Lambda. \tag{4.3.1}$$

By differentiating $q_\Lambda(u_\Lambda)$ with respect to Λ_j, we obtain that

$$q'_\Lambda(u_\Lambda)x_j - w_{\Lambda,j}(u_\Lambda) \in \mathcal{I}_\Lambda. \tag{4.3.2}$$

If $\mathcal{I}$ is radical then $\mathcal{I}_\Lambda$ is radical, hence q_Λ is square-free. Conversely, if q_Λ is square-free then $q'_\Lambda(u_\Lambda)$ is invertible in $\mathbb{B}'_\Lambda$. It thus follows from (4.3.2) that the monomorphism $\mathbb{A}'_\Lambda[T]/(q_\Lambda(T)) \hookrightarrow \mathbb{B}'_\Lambda$ that sends T to u_Λ is surjective, and then that:

$$\mathcal{I}'_\Lambda = (q_\Lambda(u_\Lambda), q'_\Lambda(u_\Lambda)x_{r+1} - w_{\Lambda,r+1}(u_\Lambda), \ldots, q'_\Lambda(u_\Lambda)x_n - w_{\Lambda,n}(u_\Lambda)).$$

Thanks to Corollary 4.1.5, the radicality of $\mathcal{I}'_\Lambda$ implies the one of $\mathcal{I}_\Lambda$, and thus the one of $\mathcal{I}$, which ends the proof of part (a). Since a basis of $\mathbb{B}'$ induces a basis of $\mathbb{B}'_\Lambda$, q_Λ is indeed the characteristic polynomial of a matrix whose entries are homogeneous of degree one in $\Lambda_{r+1}, \ldots, \Lambda_n$, and thus q_Λ is homogeneous of degree δ when seen in $\mathbb{A}'[\Lambda_{r+1}, \ldots, \Lambda_n, T]$. The last assertion directly comes from Theorem 4.2.1(b). □

We are now ready to characterize the univariate representations of $\mathcal{I}$. For any linear form $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$, we write $q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ for the respective specializations of $q_\Lambda, w_{\Lambda,r+1}, \ldots, w_{\Lambda,n}$ at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$.

Corollary 4.3.11. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position.*

(a) u is primitive for $\mathcal{I}$ if, and only if, q_λ is square-free.

(b) If u is primitive for $\mathcal{I}$, then $q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ is the Kronecker representation of $\mathcal{I}$ associated to u. In particular, $q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ all belong to $\mathbb{A}[T]$, and $q_\lambda(u), q'_\lambda(u)x_{r+1} - w_{\lambda,r+1}(u), \ldots, q'_\lambda(u)x_n - w_{\lambda,n}(u)$ all belong to $\mathcal{I}$. In addition, if the Noether position is general, then the total degree of q_λ is δ, and the total degrees of $w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ are at most δ, when seen in $\mathbb{K}[x_1, \ldots, x_r, T]$.

Proof. By substituting $\lambda_{r+1}, \ldots, \lambda_n$ for $\Lambda_{r+1}, \ldots, \Lambda_n$ in (4.3.1) and (4.3.2), we obtain that $\deg(q_\lambda) = \delta$ and that

$$(q_\lambda(u), q'_\lambda(u)x_{r+1} - w_{\lambda,r+1}(u), \ldots, q'_\lambda(u)x_n - w_{\lambda,n}(u)) \subseteq \mathcal{I}.$$

If $q_\lambda(u)$ is square-free then $q'_\lambda(u)$ is invertible in $\mathbb{B}'$, and therefore the map from $\mathbb{A}'[T]/(q_\lambda(T))$ to $\mathbb{B}'$ that sends T to u is surjective. It follows from Proposition 4.3.1(a) that u is a primitive element. Conversely, if u is a primitive element, then the degree of the minimal polynomial q of u equals δ, by Proposition 4.3.1(b), and we thus obtain that q and q_λ have the same degrees, hence are equal. In particular, q_λ is square-free, which concludes part (a). The rest of the proof comes directly from Proposition 4.3.10(b). □

Part (b) of Corollary 4.3.11 permits us to control the degree of the elements of a Kronecker representation for ideals in Noether position. That will be a key of the lifting step in Section 6.2. We end this section with a genericity result:

Corollary 4.3.12. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Then the set of points $(\lambda_{r+2}, \ldots, \lambda_n) \in \mathbb{K}^{n-r-1}$ such that $u = x_{r+1} + \lambda_{r+2}x_{r+2} + \cdots + \lambda_n x_n$ is a primitive element for $\mathcal{I}$ is Zariski dense.*

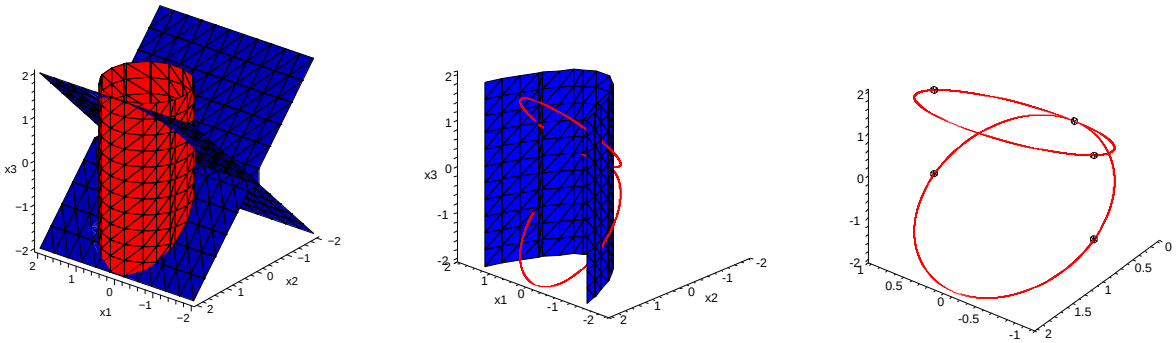
Proof. By Proposition 4.3.10, the discriminant of q_Λ is nonzero and homogeneous in the variables $\Lambda_{r+1}, \ldots, \Lambda_n$. Therefore if the specialization of this discriminant at $\Lambda_{r+1} = 1, \Lambda_{r+2} = \lambda_{r+2}, \ldots, \Lambda_n = \lambda_n$ is nonzero then u is a primitive element for $\mathcal{I}$ by Corollary 4.3.11(a). □

Example 4.3.14. Let

$$\begin{cases} f_1 &= x_1^2 + (x_2 - 1)^2 - 1 \\ f_2 &= x_3^2 - x_2^2 \\ f_3 &= x_2 - x_1^2. \end{cases}$$

As already seen in Example 1.4.16, the variety $\mathcal{V}(f_1, f_2, f_3)$ consists in the five points $(0, 0, 0), (-1, 1, \pm 1), (1,$ (see Figure 4.3.13 below); x_1 is not primitive for $\mathcal{I} = (f_1, f_2, f_3)$. Nevertheless, $x_1 - 2x_2 - 4x_3$ is a primitive element for $\mathcal{I}$.

Figure 4.3.13.



$\mathcal{V}(f_1), \mathcal{V}(f_2)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_3)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_1, f_2, f_3)$

Remark 4.3.15. The previous proofs contain an algorithm to compute $\lambda_{r+2}, \ldots, \lambda_n$ such that u is primitive for $\mathcal{I}$. First we compute q_Λ, that can be done by eliminating $\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_r, u$ in the ideal $\mathcal{I}_\Lambda + (u - \Lambda_{r+1}x_{r+1} - \cdots - \Lambda_n x_n)$ of $\mathbb{A}_\Lambda[u, x_{r+1}, \ldots, x_n]$. Then, we calculate the discriminant of q_Λ with respect to u. Finally, we choose $\lambda_{r+2}, \ldots, \lambda_n$ that do not annihilate this discriminant. As for Noether position, the use of the genericity result of Corollary 4.3.12 will avoid such an expensive calculation.

4.4 Cleaning Step

We finish this chapter with an algorithm to remove components of a zero-dimensional ideal $\mathcal{I}$ given by its univariate representation with respect to the primitive element x_1. This algorithm relies on the following remark: in the univariate case, for any polynomials $f, g \in \mathbb{K}[x_1]$ with f square-free, we have $(f) : g^\infty = (f) : \gcd(f, g)^\infty = (f/\gcd(f, g))$. Univariate representations permit to reduce to the univariate case:

Proposition 4.4.1. *Let $\mathcal{I}$ be a radical zero-dimensional ideal in Noether position with primitive element x_1, let g be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$, and let $q, v_1, \ldots, v_n$ be the univariate representation of $\mathcal{I}$ with respect to x_1. Let $e = \gcd(q, g(v_1, \ldots, v_n))$ in $\mathbb{K}[x_1]$, $Q = q/e$, and V_j be the remainder of v_j divided by Q. Then x_1 is a primitive element for $\mathcal{I} : g^\infty$ and $Q, V_1, \ldots, V_n$ is the univariate representation of $\mathcal{I} : g^\infty$ with respect to x_1.*

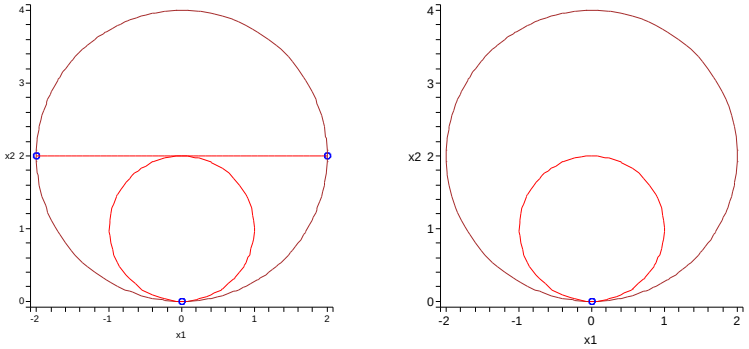
Proof. Since the ideal $\mathcal{I}$ is radical, the polynomial q is square-free. The proof follows from the following straightforward calculations:

$$\begin{aligned}\mathcal{I} : g^\infty &= (q(x_1), x_1 - v_1(x_1), \ldots, x_n - v_n(x_1)) : g^\infty \\ &= (q(x_1), x_1 - v_1(x_1), \ldots, x_n - v_n(x_1)) : e(x_1)^\infty \\ &= (Q(x_1), x_1 - V_1(x_1), \ldots, x_n - V_n(x_1)).\end{aligned}$$

□

Proposition 4.4.1 yields the following algorithm:

Figure 4.4.3.



$\mathcal{V}(\mathcal{I})$ $\mathcal{V}(\mathcal{I} : g^\infty)$

Algorithm 4. *Cleaning Step*

Input: the univariate representation with multiplicities $\chi, q, v_1, \ldots, v_n$ of a zero-dimensional ideal $\mathcal{I}$ with primitive element x_1, and a polynomial $g \in \mathbb{K}[x_1, \ldots, x_n]$.

Output: $\mathcal{I} : g^\infty = (1)$ or the univariate representation with multiplicities $\chi, Q, V_1, \ldots, V_n$ of $\mathcal{I} : g^\infty$ with respect to x_1.

1. Compute $e = \gcd(q, g(v_1, \ldots, v_n))$.
2. Compute $Q = q/e$.
3. If $Q = 1$, then return $\mathcal{I} : g^\infty = (1)$. Stop.
4. For j from 1 to n, compute the remainder V_j of v_j divided by Q.
5. Replace χ with $\chi / \gcd(\chi, e^{\deg(\chi)})$.
6. Return $\chi, Q, V_1, \ldots, V_n$.

Proposition 4.4.2. *Algorithm 4 works correctly as specified.*

Proof. By Proposition 4.4.1, $Q, V_1, \ldots, V_n$ is the univariate representation of $\sqrt{\mathcal{I}}$ with respect to x_1. In the zero-dimensional case, saturating an ideal corresponds to removing points, and the correctness of step 5 comes from Proposition 3.2.4 since χ is the characteristic polynomial of the multiplication by x_1 modulo $\mathcal{I}$. □

Example 4.4.4. Let $\mathcal{I} = ((x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2), x_1^2 + (x_2 - 2)^2 - 4)$, and $g = x_2 - 2$ (see Figure 4.4.3). The univariate representation with multiplicities of $\mathcal{I}$ for the primitive element x_1 is

$$\chi = x_1^2(x_1 - 2)(x_1 + 2),\ q = x_1(x_1 - 2)(x_1 + 2),\ v_2 = x_1^2/2.$$

This yields $e = \gcd(q(x_1), x_1^2/2 - 2) = x_1^2 - 4$, and thus to $Q = x_1$. We obtain the univariate representation with multiplicities

$$\chi = x_1^2,\ Q = x_1,\ V_2 = 0$$

of $\mathcal{I} : g^\infty = ((x_1^2 + (x_2 - 1)^2 - 1), x_1^2 + (x_2 - 2)^2 - 4)$.

Assuming that x_1 is a primitive element for $\mathcal{I}$ is not really restrictive. Indeed, Corollary 4.3.12 ensures it with an high probability after a randomly chosen linear change of the variables. Moreover, we will see in Chapter 6 how to reduce any unmixed ideal to the zero-dimensional case by specializing the free variables.

Chapter 5

Computation of Characteristic Polynomials and Intersection Step

In this chapter, we carry on with the notation of the introduction of Chapter 4. We describe the devices to compute a Noether position when adding a new polynomial f to an ideal $\mathcal{I} \neq (1)$, and we give a proof of the well known principal ideal theorem. Then, we present a formula to compute a characteristic polynomial modulo $\mathcal{I} + (f)$, that is the cornerstone of the Kronecker solver, but that will also be a main ingredient in the definition of the degree of an ideal and in the proof of a Bézout theorem in Section 7.2. Finally, we use this formula to design an algorithm for computing a univariate representation of $\mathcal{I} + (f)$ from one of $\mathcal{I}$ in the case when $\dim(\mathcal{I}) = 1$ and $\dim(\mathcal{I} + (f)) = 0$. This algorithm is indeed the *intersection step* of the Kronecker solver.

5.1 Incremental Noether Position

Univariate representations are defined for ideals in Noether position. If $\mathcal{I}$ is in Noether position then, for a given $f \in \mathbb{K}[x_1, \ldots, x_n]$, there is *a priori* no reason for $\mathcal{I} + (f)$ to be in Noether position, as shows the example $\mathcal{I} = (x_3^2 - x_1^2)$, $f = x_3$ (see Figure 5.1.4 below). We are going to show how to change the variables so that $\mathcal{I}$ and $\mathcal{I} + (f)$ become in Noether position. We let χ and μ denote the characteristic and minimal polynomials of f modulo $\mathcal{I}$ defined at the beginning of Section 4.2. We start with a lemma that relates the first properties of $\mathcal{I} + (f)$ to the constant coefficients χ_0 and μ_0 of χ and μ respectively.

Lemma 5.1.1. *Assume that $\mathcal{I}$ is unmixed and in Noether position.*

(a) μ_0 and χ_0 belong to $\mathcal{I} + (f)$, and $(\mathcal{I} + (f)) \cap \mathbb{A} \subseteq \sqrt{(\mu_0)} = \sqrt{(\chi_0)}$.

(b) f is a zerodivisor in $\mathbb{B}$ if, and only if, $\chi_0 = 0$ (or equivalently, $\mu_0 = 0$), if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$.

(c) $\mathcal{I} + (f) = (1)$ if, and only if, $\chi_0 \in \mathbb{K} \setminus \{0\}$ (or equivalently, $\mu_0 \in \mathbb{K} \setminus \{0\}$).

Proof. From Theorem 4.2.1(c), we have that $\mu(f) \in \mathcal{I}$ and $\chi(f) \in \mathcal{I}$, whence $\mu_0 \in \mathcal{I} + (f)$ and $\chi_0 \in \mathcal{I} + (f)$. Let a be a polynomial in $(\mathcal{I} + (f)) \cap \mathbb{A}$, and let $g \in \mathbb{K}[x_1, \ldots, x_n]$ be such that $a - gf \in \mathcal{I}$. Since g in integral over $\mathbb{A}$ modulo $\mathcal{I}$, there exist $\nu_0, \ldots, \nu_{\alpha-1}$ in $\mathbb{A}$ such that $g^\alpha + \nu_{\alpha-1} g^{\alpha-1} + \cdots + \nu_0 \in \mathcal{I}$. By multiplying the latter expression by f^α, we obtain that $a^\alpha + \nu_{\alpha-1} a^{\alpha-1} f + \cdots + \nu_0 f^\alpha \in \mathcal{I}$. We deduce that μ divides $\rho = a^\alpha + \nu_{\alpha-1} a^{\alpha-1} T + \cdots + \nu_0 T^\alpha$ in $\mathbb{A}'[T]$. Since μ is monic, this division holds in $\mathbb{A}[T]$, and therefore a^α is a multiple of μ_0, which concludes part (a).

If $\mu_0 = 0$ then we have $\nu(f) f = 0$ in $\mathbb{B}$, with $\nu(T) = \mu(T)/T$. Since $\deg(\nu) < \deg(\mu)$ we obtain that $\nu(f) \notin \mathcal{I}$, whence f is a zerodivisor. Conversely, if f is a zerodivisor then there exists $g \notin \mathcal{I}$ such that $fg \in \mathcal{I}$. Therefore there exists a primary component $\mathcal{Q}$ of $\mathcal{I}$ such that $g \notin \mathcal{Q}$ and $fg \in \mathcal{Q}$. It follows that f belongs to $\sqrt{\mathcal{Q}}$, and that $\mu_0 \in \mathcal{I} + (f) \subseteq \sqrt{\mathcal{Q}}$. Since $\mathcal{I}$ is unmixed, $\sqrt{\mathcal{Q}}$ has dimension r, which implies that $\mu_0 = 0$ thanks to Theorem 2.2.5(a). By part (a), $\mu_0 = 0$ if, and only if, $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$, which concludes part (b). Finally part (c) straightforwardly follows from part (a). □

Lemma 5.1.1 already gives us the following property: if f is a zerodivisor in $\mathbb{B}$, then $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}+(f)$, and thus $\mathcal{I}+(f)$ is in Noether position (the general Noether position is also preserved). For instance, the ideal $\mathcal{I} = ((x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2))$ is unmixed in general Noether position with dimension one. The polynomial $f = x_2 - 2$ is a zero-divisor modulo $\mathcal{I}$, and $\mathcal{I} + (f) = (f)$ remains in general Noether position with dimension one. If f is a nonzerodivisor in $\mathbb{B}$, then we can compute a Noether position for $\mathcal{I} + (f)$ as follows:

Proposition 5.1.2. *Assume that $\mathcal{I}$ is unmixed.*

(a) If f is a zerodivisor in $\mathbb{B}$ then $\dim(\mathcal{I} + (f)) = r$. In addition, if $\mathcal{I}$ is in Noether position or in general Noether position then so is $\mathcal{I} + (f)$.

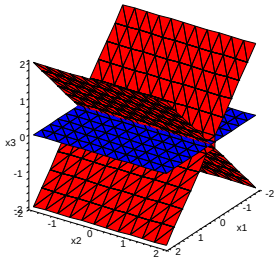
(b) If f is a nonzerodivisor in $\mathbb{B}$ then $\dim(\mathcal{I} + (f))$ equals -1 or $r - 1$. In addition, if $\mathcal{I}$ is in Noether position (respectively, general Noether position), then for any $(\alpha_1, \ldots, \alpha_{r-1}, 1) \in \mathbb{K}^r$ that does not annihilate the homogeneous component h of highest degree of μ_0, the ideals $\mathcal{I} \circ M$ and $(\mathcal{I} + (f)) \circ M$ are in Noether position (respectively, general Noether position), and $deg_{x_r}(\mu_0 \circ M) = \deg(\mu_0 \circ M)$, where M is the matrix defined by

$$M(x_1, \ldots, x_n)^t = (x_1 + \alpha_1 x_r, \ldots, x_{r-1} + \alpha_{r-1} x_r, x_r, \ldots, x_n)^t.$$

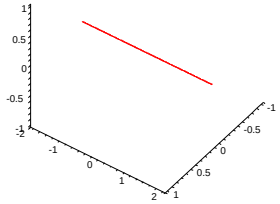
Proof. As previously discussed, part (a) is a consequence of part (b) of Lemma 5.1.1 and part (a) of Theorem 2.2.5.

If $\mu_0 \in \mathbb{K} \setminus \{0\}$ then part (b) trivially holds by Lemma 5.1.1(c). Otherwise, if $\mu_0 \notin \mathbb{K}$ then we use Lemma 2.4.2 with $\mathcal{I} + (f)$, $i = r$ and μ_0: we obtain that $x_r, \ldots, x_n$ are generally integral over $\mathbb{K}[x_1, \ldots, x_{r-1}]$ modulo $(\mathcal{I} + (f)) \circ M$. In order to complete the proof it remains to prove that $x_1, \ldots, x_{r-1}$ are algebraically independent modulo $(\mathcal{I} + (f)) \circ M$. To this aim, let $a \in \mathbb{K}[x_1, \ldots, x_{r-1}] \cap (\mathcal{I} + (f)) \circ M$. By Lemma 5.1.1(a), $\mu_0 \circ M$ divides a power of a. But since Lemma 2.4.2 tells us that $\deg_{x_r}(\mu_0 \circ M) = \deg(\mu_0 \circ M) > 0$, we deduce that $a = 0$, which ends the proof of part (b). □

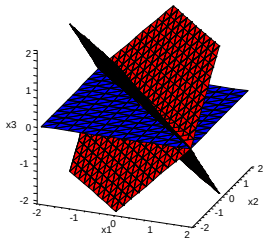
Figure 5.1.4.



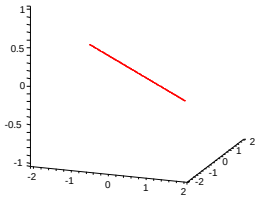
$\mathcal{V}(x_3^2 - x_1^2), \mathcal{V}(x_3)$



$\mathcal{V}(x_3^2 - x_1^2, x_3)$



$\mathcal{V}(x_3^2 - (x_1 + x_2)^2), \mathcal{V}(x_3)$



$\mathcal{V}(x_3^2 - (x_1 + x_2)^2, x_3)$

Example 5.1.3. Let $\mathcal{I}$ be the ideal $(x_3^2 - x_1^2)$ in general Noether position with dimension 2, and $f = x_3$. Then f is a nonzerodivisor in $\mathbb{B}$ since its minimal polynomial is $T^2 - x_1^2$. The ideal $\mathcal{I} + (f)$ is not in Noether position, when $(\mathcal{I} + (f)) \circ (x_1 + \alpha x_2, x_2, x_3)$ is as soon as $\alpha \neq 0$ (see Figure 5.1.4).

Remark 5.1.5. Proposition 5.1.2 gives a way to compute a common Noether position for $\mathcal{I}$ and $\mathcal{I} + (f)$ from μ_0. For the Kronecker solver, we will not deal with $\mathcal{I}$ and $\mathcal{I} + (f)$, but with a specialization, so that we will not really compute μ_0. We will only use the fact that a random linear change of variables yields such a common Noether position with a high probability of succes.

5.2 Incremental Unmixedness of the Radical

Proposition 5.1.2 ensures that if f is a nonzerodivisor in $\mathbb{B}$ and if $\mathcal{I} + (f) \neq (1)$, then the dimension of $\mathcal{I} + (f)$ equals $\dim(\mathcal{I}) - 1$. In the case when $\mathcal{I}$ is unmixed, we expect each component of $\mathcal{V}(\mathcal{I} + (f))$ to have dimension $r - 1$. The proof of the following version of the classical principal ideal theorem is adapted from [Sha94, Chapter I, Section 6.2]. Recall that we assume from the introduction that $\mathcal{I} \neq (1)$.

Theorem 5.2.1. *Assume that $\mathcal{I}$ is unmixed, and let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a nonzerodivisor in $\mathbb{B}$. If $\mathcal{I} + (f) \neq (1)$ then $\sqrt{\mathcal{I} + (f)}$ is unmixed with dimension $r - 1$.*

Proof. Thanks to Theorem 2.4.3, Proposition 5.1.2(b), and Lemma 5.1.1(c), we can assume that $r \geq 1$, $\dim(\mathcal{I} + (f)) = r - 1$, $\mathcal{I}$ and $\mathcal{I} + (f)$ are in general Noether position, and that $\deg_{x_r}(\mu_0) = \deg(\mu_0) \geq 1$. Let us first prove the theorem when $\mathcal{I}$ and f are homogeneous.

Let $E \in \mathbb{K}[x_1, \ldots, x_{r-1}, T]$ be such that $E(x_1, \ldots, x_{r-1}, f) \in \mathcal{I}$. Since the polynomial $\mu(T)$ divides $E(x_1, \ldots, x_{r-1}, T)$, it follows that μ_0 divides $E(x_1, \ldots, x_{r-1}, 0)$. Therefore the inequality $\deg_{x_r}(\mu_0) > 0$ implies that $E(x_1, \ldots, x_{r-1}, 0) = 0$. Since f is a nonzerodivisor in $\mathbb{B}$, we deduce that $E = 0$. In other words $x_1, \ldots, x_{r-1}, f$ are algebraically independent modulo $\mathcal{I}$. Since $\deg_{x_r}(\mu_0) = \deg(\mu_0)$, Theorem 4.2.1(a) implies that x_r is integral over $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$ modulo $\mathcal{I}$. Thanks to Proposition 2.1.5(b) we obtain that $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$ modulo $\mathcal{I}$. This way we have shown that $\mathbb{B}$ is an integral ring extension of $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$.

Thanks to Proposition 4.1.1, in order to prove that $\sqrt{\mathcal{I} + (f)}$ is unmixed, it is sufficient to prove that $\mathbb{K}[x_1, \ldots, x_n]/\sqrt{\mathcal{I} + (f)}$ is torsion-free when seen as a $\mathbb{K}[x_1, \ldots, x_{r-1}]$-module. With this aim in view, let $b \in \mathbb{K}[x_1, \ldots, x_n]$ and $a \in \mathbb{K}[x_1, \ldots, x_{r-1}] \setminus \{0\}$ be such that $ab \in \sqrt{\mathcal{I} + (f)}$. We claim that a power of b belongs to $\mathcal{I} + (f)$.

Let $m \in \mathbb{N}$ and $g \in \mathbb{K}[x_1, \ldots, x_n]$ be such that $a^m b^m - fg \in \mathcal{I}$. In order to prove the latter claim, we consider $\mathbb{B}$ as a $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$-module $\mathbb{B}_f$, and we denote by $\mathbb{B}'_f$ the corresponding finitely dimensional $\mathbb{K}(x_1, \ldots, x_{r-1}, f)$-vector space. By the classical Gauss lemma [Lan02, Chapter IV, Theorem 2.1], the minimal polynomials of g and b^m in $\mathbb{B}'_f$ belong to $\mathbb{K}[x_1, \ldots, x_{r-1}, f][T]$. Let $\rho(T) = T^\alpha + \rho_{\alpha-1}T^{\alpha-1} + \cdots + \rho_0$ denote the minimal polynomial of g in $\mathbb{B}'_f$. Then the minimal polynomial of b^m in $\mathbb{B}'_f$ is

$$f^\alpha \rho(a^m T/f)/a^{m\alpha} = T^\alpha + \rho_{\alpha-1}\left(\frac{f}{a^m}\right)T^{\alpha-1} + \cdots + \left(\frac{f}{a^m}\right)^\alpha \rho_0.$$

We deduce that $(a^m)^j$ divides $f^j\rho_{\alpha-j}$ in $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$, for all $j \in \{0, \ldots, \alpha - 1\}$. Since $x_1, \ldots, x_{r-1}, f$ are algebraically independent, and since $a \in \mathbb{K}[x_1, \ldots, x_{r-1}]$, we obtain that $(a^m)^j$ divides $\rho_{\alpha-j}$, whence $(b^m)^\alpha \in \mathcal{I} + (f)$, which concludes the proof in the homogeneous situation.

In the general situation, for any isolated prime $\mathfrak{p}$ of $\mathcal{I} + (f)$, it can be verified that $\mathfrak{p}^\sharp$ is an isolated prime of $\mathcal{I}^\sharp + (f^\sharp)$. It follows that $\dim(\mathfrak{p}^\sharp) = r$, hence that $\dim(\mathfrak{p}) = r - 1$, by Corollary 2.4.5. □

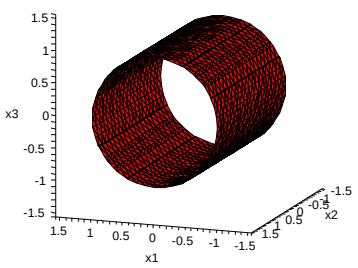
Example 5.2.2. With the polynomials f_1, f_2, f_3 of Example 4.3.14, let $\mathcal{I}$ be the one-dimensional unmixed ideal (f_1, f_2), and remark that f_3 is a nonzerodivisor modulo $\mathcal{I}$ by Lemma 5.1.1 (b). The ideal $\sqrt{(f_1, f_2, f_3)}$ is zero-dimensional, and thus unmixed.

Example 5.2.3. Let $\mathcal{I} = (x_1, x_2) \cap (x_3, x_4)$. The ideal $\mathcal{I}$ is unmixed. If we take the nonzerodivisor $f = x_2 - x_3$, then $\sqrt{\mathcal{I} + (f)} = (x_1, x_2, x_3) \cap (x_2, x_3, x_4)$ is unmixed while $\mathcal{I} + (f) = (x_1, x_2, x_3) \cap (x_2, x_3, x_4) \cap (x_1, x_2 - x_3, x_3^2, x_4)$ is not.

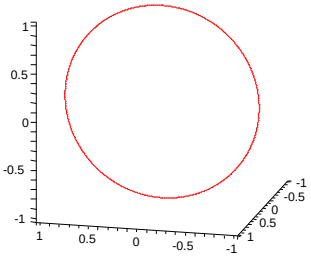
The following corollary of Theorem 5.2.1 is a first step towards the reduction of the dimension of an ideal by specialization of the independent variables, which is one of the main processes that makes the good cost of the Kronecker solver.

Corollary 5.2.4. *Assume that $\mathcal{I}$ is unmixed and in Noether position (respectively, general Noether position), let $s \in \{0, \ldots, r\}$. Then $\sqrt{\mathcal{I} + (x_{s+1}, \ldots, x_r)}$ is in Noether position (respectively, general Noether position) and unmixed with dimension s.*

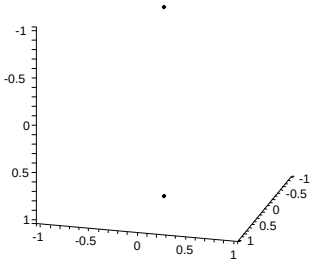
Figure 5.2.6.



$\mathcal{V}(x_3^2 + x_1^2 - 1)$



$\mathcal{V}((x_3^2 + x_1^2 - 1) + (x_2))$



$\mathcal{V}((x_3^2 + x_1^2 - 1) + (x_1, x_2))$

Proof. Since the minimal polynomial of $f = x_r$ modulo $\mathcal{I}$ is $\mu = T - x_r$, Lemma 5.1.1 implies that x_r is a nonzerodivisor in $\mathbb{B}$, and that $\mathcal{I} + (x_r) \neq (1)$. Theorem 5.2.1 thus ensures that $\sqrt{\mathcal{I} + (x_r)}$ is unmixed of dimension $r-1$. Then we obtain that $\sqrt{\mathcal{I} + (x_r)}$ is in Noether position (respectively, general Noether position) from Theorem 2.2.5(a). Finally, since

$$\sqrt{\sqrt{\mathcal{I} + (x_{s+1}, \ldots, x_r)} + (x_s)} = \sqrt{\mathcal{I} + (x_s, \ldots, x_r)}, \tag{5.2.1}$$

a straightforward induction completes the proof. □

Example 5.2.5. From a geometrical point of view, specializing $x_{s+1}, \ldots, x_r$ at zero corresponds to take the intersection of $\mathcal{V}(\mathcal{I})$ with $\mathcal{V}(x_{s+1}, \ldots, x_r)$. For instance, let $\mathcal{I} = (x_3^2 + x_1^2 - 1)$ in $\mathbb{K}[x_1, x_2, x_3]$, so that $\mathcal{V}(\mathcal{I})$ is a cylinder in $\bar{\mathbb{K}}^3$ (see Figure 5.2.6). Then $\mathcal{I} + (x_2)$ defines a circle in the plane $\mathcal{V}(x_2)$, when $\mathcal{V}(\mathcal{I} + (x_1, x_2))$ consists in two points of the x_3-axis $\mathcal{V}(x_1, x_2)$.

In order to deal with specialized ideals, we wish to keep the hypotheses on regularity of intersections. Following Corollary 5.2.7 gives a genericity result for this task:

Corollary 5.2.7. *Assume that $\mathcal{I}$ is unmixed and in Noether position (respectively, general Noether position), and let $f \in \mathbb{K}[x_1, \ldots, x_n]$.*

(a) If χ_0 does not vanish at $x_1 = \cdots = x_r = 0$, then f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/(\mathcal{I} + (x_1, \ldots, x_r))$.

(b) If f is a nonzerodivisor in $\mathbb{B}$ then the set of points $(\beta_1, \ldots, \beta_r) \in \mathbb{K}^r$ such that f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/(\mathcal{I} + (x_1 - \beta_1, \ldots, x_r - \beta_r))$ is Zariski dense.

Proof. Let ψ denote the specialization of χ at $x_1 = \cdots = x_r = 0$, and let $\mathcal{J} = \mathcal{I} + (x_1, \ldots, x_r)$. By Corollary 5.2.4, $\mathcal{J}$ has dimension 0, and thus is unmixed. From Theorem 4.2.1 we have that $\chi(f) \in \mathcal{I}$, whence $\psi(f) \in \mathcal{J}$. Therefore the constant coefficient of the minimal polynomial of f in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$ can not be zero, and thus Lemma 5.1.1(b) implies that f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$. This concludes the proof of part (a). If f is a nonzerodivisor in $\mathbb{B}$ then Lemma 5.1.1(b) implies that $\chi_0 \neq 0$, which immediately yields part (b). □

Example 5.2.8. Let $\mathcal{I}$ be the ideal $(x_2^2 - x_1^2)$ in $\mathbb{K}[x_1, x_2]$, which is unmixed in Noether position. The polynomial $f = x_2$ has characteristic polynomial $T^2 - x_1^2$ in $\mathbb{B} = \mathbb{K}[x_1, x_2]/\mathcal{I}$, and thus is a nonzerodivisor in $\mathbb{B}$ by Lemma 5.1.1. Now, f is a zerodivisor in $\mathbb{K}[x_1, x_2]/(\mathcal{I} + (x_1)) = \mathbb{K}[x_1, x_2]/(x_2^2)$. Nevertheless, it is not in $\mathbb{K}[x_1, x_2]/\mathcal{I} + (x_1 - \beta)$ for any β in $\mathbb{K}\backslash\{0\}$.

Remark 5.2.9. As for Proposition 5.1.2, it is easy to find $(\beta_1, \ldots, \beta_r)$ as in part (b) of Corollary 5.2.7 as soon as we know χ_0. For the Kronecker solver, we will prefer to use the genericity result and a random affine change of the variables since we only compute some specializations of the polynomial χ_0.

5.3 Incremental Computation of the Characteristic Polynomial

We next present the key formula for the computation of the characteristic polynomial of x_r modulo $\mathcal{I} + (f)$.

Proposition 5.3.1. *Assume that $\mathcal{I}$ has dimension $r \geq 1$, is unmixed, and is in Noether position. Let f be a nonzerodivisor in $\mathbb{B}$. Then the polynomial $\chi_0(x_1, \ldots, x_{r-1}, T)$ is proportional over $\mathbb{K}(x_1, \ldots, x_{r-1})$ to the characteristic polynomial of x_r modulo the extension $\mathcal{J}'$ of the ideal $\mathcal{J} = \mathcal{I} + (f)$ to $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$. The proportionality over $\mathbb{K}$ holds if, and only if, $\mathcal{J}$ is in Noether position.*

Proof. Let $\tilde{\mathbb{B}} = \mathbb{K}(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]/\tilde{\mathcal{I}}$, where $\tilde{\mathcal{I}}$ denotes the extension of $\mathcal{I}$ to $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]$. By Proposition 4.1.1, $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module, so is $\tilde{\mathbb{B}}$ seen as a $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$-module. From [Lan02, Chapter III, Theorem 7.3], it follows that $\tilde{\mathbb{B}}$ is free, and, thanks to the Noether position of $\mathcal{I}$, that $\tilde{\mathbb{B}}$ has finite rank. Therefore, by [Lan02, Chapter III, Theorem 7.9], there exist two bases $e_1, \ldots, e_\delta$ and $e'_1, \ldots, e'_\delta$ of $\tilde{\mathbb{B}}$, and some monic polynomials $h_1, \ldots, h_\delta \in \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$ such that h_ℓ divides $h_{\ell+1}$ for all $\ell \in \{1, \ldots, \delta - 1\}$, and such that $f e_\ell = h_\ell e'_\ell$ in $\tilde{\mathbb{B}}$ for all $\ell \in \{1, \ldots, \delta\}$.

On the one hand, since a basis of $\tilde{\mathbb{B}}$ induces a basis of $\mathbb{B}'$, we obtain that $\chi_0 = a h_1 \cdots h_\delta$, for some $a \in \mathbb{K}(x_1, \ldots, x_{r-1})$. On the other hand, we claim that the set $\mathcal{B} = \{x_r^{\alpha_\ell} e'_\ell \mid 1 \leq \ell \leq \delta,\ 0 \leq \alpha_\ell \leq \deg(h_\ell) - 1\}$ is a basis of $\tilde{\mathbb{B}}/(f)$ seen as a $\mathbb{K}(x_1, \ldots, x_{r-1})$-algebra. Let us first verify that $\mathcal{B}$ actually generates $\tilde{\mathbb{B}}/(f)$. Let $g \in \tilde{\mathbb{B}}/(f)$. Any preimage $\tilde{g}$ of g in $\tilde{\mathbb{B}}$ can be written $g = \sum_{\ell=1}^{\delta} g_\ell e'_\ell$, with $g_1, \ldots, g_\delta \in \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$. Since, by construction, the ideal generated by f in $\tilde{\mathbb{B}}$ equals $(h_1 e'_1, \ldots, h_\delta e'_\delta)$, we can write $g = \sum_{\ell=1}^{\delta} r_\ell e'_\ell$ in $\tilde{\mathbb{B}}/(f)$, where each r_ℓ denotes the remainder in the division of g_ℓ by h_ℓ. Secondly, let us verify that $\mathcal{B}$ is free. Let $r_1, \ldots, r_\delta \in \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$ be such that $\deg(r_\ell) < \deg(h_\ell)$ and $\sum_{\ell=1}^{\delta} r_\ell e'_\ell = 0$ in $\tilde{\mathbb{B}}/(f)$. Then there exist some polynomials $q_1, \ldots, q_\delta \in \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$ such that $\sum_{\ell=1}^{\delta} r_\ell e'_\ell + \sum_{\ell=1}^{\delta} q_\ell h_\ell e'_\ell = 0$ in $\tilde{\mathbb{B}}$. Therefore, for all ℓ we obtain $r_\ell + q_\ell h_\ell = 0$, whence $q_\ell = r_\ell = 0$ since $\deg(h_\ell) > \deg(r_\ell)$.

In the basis $\mathcal{B}$, the matrix of multiplication by x_r in $\tilde{\mathbb{B}}/(f)$ is a diagonal block matrix, whose blocks are the companion matrices of the h_ℓ. Therefore the characteristic polynomial q of x_r in $\tilde{\mathbb{B}}/(f)$ equals $h_1 \cdots h_\delta$. We finally obtain that χ_0 is proportional to q over $\mathbb{K}(x_1, \ldots, x_{r-1})$.

Let us now deal with the last assertion of the proposition. If $\mathcal{J} = (1)$ then it trivially holds thanks to Lemma 5.1.1(c). Let us now assume that $\mathcal{J} \neq (1)$. Theorem 5.2.1 gives us that $\dim(\mathcal{J}) = r - 1$. Therefore if $\mathcal{J}$ is in Noether position then there exists a monic polynomial $p \in \mathbb{K}[x_1, \ldots, x_{r-1}][T]$ such that $p(x_r) \in \mathcal{J}$. Since Lemma 5.1.1(a) implies that χ_0 divides a power of $p(x_r)$, we deduce that the leading coefficients of χ_0 seen in $\mathbb{K}[x_1, \ldots, x_{r-1}][x_r]$ belongs to $\mathbb{K}$, and thus that χ_0 is proportional over $\mathbb{K}$ to $q(x_r)$. Conversely, if χ_0 is proportional over $\mathbb{K}$ to $q(x_r)$, then x_r is integral over $\mathbb{K}[x_1, \ldots, x_{r-1}]$ modulo $\mathcal{J}$ by Lemma 5.1.1(a). We thus obtain that $\mathcal{J}$ is in Noether position by Proposition 2.1.5(b) and Theorem 2.2.5(a). □

Example 5.3.2. The basis $\mathcal{B}$ in the proof of Proposition 5.3.1 is built from the isomorphism between the $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$-modules $\tilde{\mathbb{B}}/(f)$ and

$$\bigoplus_{\ell=1}^{\delta} \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]/(h_\ell).$$

In general this direct sum is not a decomposition of $\tilde{\mathbb{B}}/(f)$ into stable $\mathbb{K}(x_1, \ldots, x_{r-1})$-algebras. This can be seen by taking $n = 2$, $\mathcal{I} = (x_2^2 + x_1 x_2)$, $r = 1$, and $f = x_1^2$. Then $\{1, x_2\}$ forms a basis of the $\mathbb{K}[x_1]$-module $\tilde{\mathbb{B}} = \mathbb{K}[x_1, x_2]/\tilde{\mathcal{I}}$, in which the matrix of multiplication by f is the diagonal matrix with $h_1 = x_1^2$ and $h_2 = x_1^2$ on its diagonal. As $\mathbb{K}[x_1]$-modules we thus have $\tilde{\mathbb{B}}/(f) = \mathbb{K}[x_1]/(h_1) \bigoplus \mathbb{K}[x_1]/(h_2)x_2$. These two submodules are stable by multiplication by x_1 but $\mathbb{K}[x_1]/(h_1)$ is not stable by multiplication by x_2.

5.4 Intersection Step

In this section, we let $\mathcal{I}$ be a radical unmixed ideal in Noether position with dimension 1 and primitive element x_2, given by its univariate representation $q, v_2, \ldots, v_n$. We let f be a nonzerodivisor in $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ such that $\sqrt{\mathcal{I} + (f)} \neq (1)$ with primitive element x_1. From Proposition 5.3.1, we deduce an algorithm that computes the univariate representation with multiplicities $\xi, Q, V_1, \ldots, V_n$ of $\mathcal{I} + (f)$ for the primitive element x_1. We write Res_T for the resultant in the main variable T.

Proposition 5.4.1. *The characteristic polynomial of x_1 modulo $\mathcal{I} + (f)$ is proportional over $\mathbb{K}$ to the following resultant in T:*

$$\chi_0 = \mathrm{Res}_T(q(T), f(x_1, v_2(T), \ldots, v_n(T))). \tag{5.4.1}$$

In particular, $Q(x_1)$ is the square-free part of χ_0.

Proof. Let $p^{(1)}, \ldots, p^{(s)}$ denote the roots of the zero-dimensional ideal $\mathcal{I}'$ in an algebraic closure $\overline{\mathbb{K}(x_1)}$ of $\mathbb{K}(x_1)$. Proposition 3.2.4 ensures that $\chi_0 = \prod_{\ell=1}^{s} f(p^{(\ell)})$. The radicality of $\mathcal{I}$ ensures the one of $\mathcal{I}'$ by Corollary 4.1.5. By a well known property of resultants (see for instance [CLO05, Chapter 3, formula (1.4)]), we thus have

$$\mathrm{Res}_T(q(T), f(x_1, v_2(T), \ldots, v_n(T))) = \prod_{q(T)=0} f(x_1, v_2(T), \ldots, v_n(T)) = \prod_{\ell=1}^{s} f(p^{(\ell)}).$$

Therefore the conclusion follows directly from Proposition 5.3.1. □

Proposition 5.4.1 gives a formula to compute the polynomial Q. We obviously have $V_1(x_1) = x_1$. It remains to explain how we calculate the polynomials $V_2, \ldots, V_n$. We proceed by specialization and interpolation. Let $a \in \bar{\mathbb{K}}^n$ be such that x_2 is a primitive element for the zero-dimensional ideal $\sqrt{\mathcal{I} + (x_1 - a)}$. We will see in Corollary 6.1.3 how to compute from $q, v_2, \ldots, v_n$ the univariate representation $q_a, v_{a,2}, \ldots, v_{a,n}$ of $\sqrt{\mathcal{I} + (x_1 - a)}$ with respect to x_2. Then we have

$$\sqrt{\mathcal{I} + (x_1 - a)} = (q_a(x_2), x_1 - a, x_2 - v_{a,2}(x_2), \ldots, x_n - v_{a,n}(x_2)),$$

and so

$$\begin{aligned}\sqrt{\mathcal{I} + (x_1 - a)} + (f) = (f(a, v_{a,2}(x_2), \ldots, v_{a,n}(x_2)), q_a(x_2)) \\ + (x_1 - a, x_2 - v_{a,2}(x_2), \ldots, x_n - v_{a,n}(x_n)).\end{aligned}$$

Now let us assume that $a \in \bar{\mathbb{K}}^n$ is a root of Q. Since x_1 is primitive for $\sqrt{\mathcal{I} + (f)}$, we have

$$\sqrt{\mathcal{I} + (f)} + (x_1 - a) = (x_1 - V_1(a), \ldots, x_n - V_n(a)).$$

Therefore we can compute $V_2(a)$ by means of the following formula:

$$x_2 - V_2(a) = \gcd(f(a, v_{a,2}(x_2), \ldots, v_{a,n}(x_2)), q_a(x_2)),$$

where gcd means the greatest common divisor in x_2. By substituting $V_2(a)$ for x_2 in all the $v_{a,j}$, we obtain $V_j(a) \in \bar{\mathbb{K}}$, for all $j \in \{3, \ldots, n\}$. Finally $V_2, \ldots, V_n$ can be obtained by interpolation.

This yields the following algorithm:

Algorithm 5. *Intersection Step*

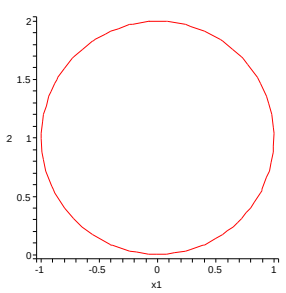
Input: the univariate representation $q, v_2, \ldots, v_n$ with respect to x_2 of a radical unmixed one-dimensional ideal $\mathcal{I}$ in Noether position, and a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ such that:

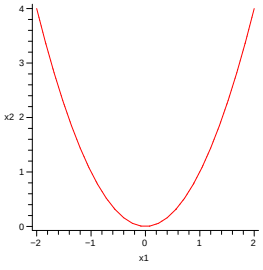
- f is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$,
- if $\mathcal{I} + (f) \neq (1)$, x_1, respectively x_2, is a primitive element for $\mathcal{I} + (f)$, respectively $\sqrt{\mathcal{I} + (x_1 - a)}$ for any first coordinate $a \in \bar{\mathbb{K}}$ of a point in $\mathcal{V}(\mathcal{I} + (f))$.

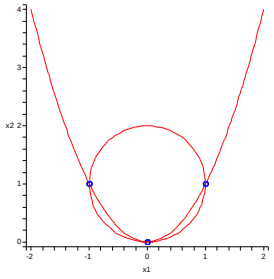
Output: $\mathcal{I} + (f) = (1)$, or the univariate representation with multiplicities $\xi, Q, V_1, \ldots, V_n$ of $\mathcal{I} + (f)$ for the primitive element x_1.

1. Compute $\xi = \mathrm{Res}_T(q(T), f(x_1, v_2(T), \ldots, v_n(T)))$.
2. If $\xi \in \mathbb{K} \backslash \{0\}$, then return $1, 1, 0, \ldots, 0$.
3. If the coefficient c of $x_1^{\deg(\xi)}$ in ξ is not 1, then replace ξ with ξ/c.
4. Compute the square-free part Q of ξ.
5. Let $a_1, \ldots, a_s$ denote the distinct roots of Q in $\bar{\mathbb{K}}$.

Figure 5.4.4.


$\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1)$


$\mathcal{V}(x_2 - x_1^2)$


$\mathcal{V}((x_1^2 + (x_2 - 1)^2 - 1) + (x_2 - x_1^2))$

6. For ℓ from 1 to s, do
   a. compute the univariate representation $q_{a_\ell}, v_{a_\ell,2}, \ldots, v_{a_\ell,n}$ of $\sqrt{\mathcal{I} + (x_1 - a_\ell)}$ with respect to x_2;
   b. compute $V_2(a_\ell) = x_2 - \gcd(f(a_\ell, v_{a_\ell,2}(x_2), \ldots, v_{a_\ell,n}(x_2)), q_{a_\ell}(x_2))$;
   c. for j from 3 to n compute $V_j(a_\ell) = v_{a_\ell,j}(a_\ell, V_2(a_\ell))$.
7. For j from 2 to n, compute the interpolating polynomial V_j from $V_j(a_1), \ldots, V_j(a_s)$.
8. Return $\xi, Q, V_1 = x_1, V_2, \ldots, V_n$.

Proposition 5.4.2. *Algorithm 5 works correctly as specified.*

Proof. The correctness result follows from Proposition 5.4.1, Lemma 5.1.1 (c), and from the computations above the algorithm. □

Example 5.4.3. Let $\mathcal{I} = (x_1^2 + (x_2 - 1)^2 - 1)$, with univariate representation

$$q = (x_2 - 1)^2 + x_1^2 - 1, v_2 = x_2,$$

and let $f = x_2 - x_1^2$. From

$$\mathrm{Res}_T((T-1)^2 + x_1^2 - 1, T - x_1^2) = x_1^2(x_1 - 1)(x_1 + 1),$$

we deduce ξ and $Q = x_1(x_1 - 1)(x_1 + 1)$. Then using the calculations of Example 6.1.4 below, we compute

$$\begin{cases} V_2(0) &= x_2 - \gcd(x_2, x_2^2 - 2x_2) &= 0, \\ V_2(1) &= x_2 - \gcd(x_2 - 1, x_2 - 1) &= 1, \\ V_2(-1) &= x_2 - \gcd(x_2 - 1, x_2 - 1) &= 1. \end{cases}$$

By interpolating, we obtain $V_2 = x_1^2$.

Of course in practice, computations are not really handled in $\bar{\mathbb{K}}$. Instead we appeal classical techniques of computer algebra: for each irreducible factor Q_ℓ of Q, we do the above computations with taking a as the residue class of z in $\mathbb{K}[z]/(Q_\ell(z))$, and finally we recover the result by means of the Chinese remainder theorem. Factorization can even be avoided thanks to dynamic evaluation [Duv94, Duv95].

Here again, the hypotheses needed for Algorithm 5 are not really restrictive thanks in particular to the genericity result of Corollary 4.3.12, as will be detailed in Section 7.1.

Chapter 6

Specialization of Independent Variables and Lifting Step

The Kronecker solver deals with ideals whose dimension is zero or one. To reduce any given ideal in Noether position to a zero-dimensional one, we shall specialize the independent variables $x_1, \ldots, x_r$. In a first section, we study the behavior of univariate representations under specialization. Then we use Newton iterations to recover the whole representation from a specialized one. In this way we achieve the *lifting step* of the Kronecker solver.

6.1 Specialization of the Independent Variables

In this section, we let $\mathcal{I}$ be a radical ideal with dimension r, we let s denote an integer in $\{0, \ldots, r-1\}$, and we let $\mathcal{J} = \mathcal{I} + (x_{s+1}, \ldots, x_r)$. We show how to compute a Kronecker representation of $\sqrt{\mathcal{J}}$ from one of $\mathcal{I}$, with the same primitive element whenever it is possible. For this purpose, we continue with the notation of Section 4.3, and we introduce $\mathcal{J}_\Lambda = \mathcal{I}_\Lambda + (x_{s+1}, \ldots, x_r)$ for the extension of $\mathcal{J}$ to $\mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]$. Let $\mathbb{C}_\Lambda = \mathbb{K}[\Lambda_{r+1}, \ldots, \Lambda_n, x_1, \ldots, x_n]/\mathcal{J}_\Lambda$, and let Q_Λ represent the specialization of q_Λ at $x_{s+1} = \cdots = x_r = 0$. We write $\mathcal{J}'_\Lambda$ for the extension of $\mathcal{J}_\Lambda$ to $\mathbb{K}_\Lambda(x_1, \ldots, x_s)[x_{s+1}, \ldots, x_n]$, and we let $\mathbb{C}'_\Lambda = \mathbb{K}_\Lambda(x_1, \ldots, x_s)[x_{s+1}, \ldots, x_n]/\mathcal{J}'_\Lambda$.

Proposition 6.1.1. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position (respectively, general Noether position). Then $\mathcal{J}$ is in Noether position (respectively, general Noether position), $\sqrt{\mathcal{J}}$ is unmixed with dimension s, and we have that:*

(a) The square-free part of Q_Λ is the minimal polynomial of u_Λ modulo the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1, \ldots, x_s)[x_{s+1}, \ldots, x_n]$.

(b) $\mathcal{J}$ is radical if, and only if, Q_Λ is square-free.

Proof. The Noether position (respectively, general Noether position) of $\mathcal{J}$, the unmixedness of $\sqrt{\mathcal{J}}$, and its dimension come from Corollary 5.2.4 directly. Let us now focus on the case when

$s = r - 1$. We introduce $\tilde{\mathcal{I}}_\Lambda$ for the extension of $\mathcal{I}_\Lambda$ to $\mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]$, and we let

$$\tilde{\mathbb{B}}_\Lambda = \mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]/\tilde{\mathcal{I}}_\Lambda.$$

Since $\mathbb{B}_\Lambda$ is a torsion-free $\mathbb{A}_\Lambda$-module by Proposition 4.1.1, the $\mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r]$-module $\tilde{\mathbb{B}}_\Lambda$ is torsion-free. By [Lan02, Theorem 7.3], and since $\tilde{\mathcal{I}}_\Lambda$ is in Noether position, we deduce that $\tilde{\mathbb{B}}_\Lambda$ is a free $\mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r]$-module of finite rank.

Since q_Λ is the characteristic polynomial of u_Λ in $\mathbb{B}'_\Lambda$, and since a basis of $\tilde{\mathbb{B}}_\Lambda$ induces a basis of $\mathbb{B}'_\Lambda$, we deduce that q_Λ is also the characteristic polynomial of u_Λ in $\tilde{\mathbb{B}}_\Lambda$. Since a basis of $\tilde{\mathbb{B}}_\Lambda$ induces a basis of $\mathbb{C}'_\Lambda$, we deduce that Q_Λ is the characteristic polynomial of u_Λ in $\mathbb{C}'_\Lambda$. It follows that the square-free part of Q_Λ is the minimal polynomial of u_Λ in $\mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]/\sqrt{\mathcal{J}'_\Lambda}$. Since the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$ is $\sqrt{\mathcal{J}'_\Lambda}$, we are done with part (a) when $s = r - 1$. For the other values of s, we can straightforwardly proceed by induction thanks to equality (5.2.1) (as used in the proof of Corollary 5.2.4).

Let us now deal with part (b). If $\mathcal{J}$ is radical then $\mathcal{J}'_\Lambda$ is radical by Corollary 4.1.5, and thus the characteristic polynomial Q_Λ of u_Λ in $\mathbb{C}'_\Lambda$ coincides with its minimal polynomial. We thus obtain that Q_Λ is square-free. Conversely, if Q_Λ is square-free then the minimal polynomial of u_Λ modulo $\mathcal{J}'_\Lambda$ is square-free. Therefore $\mathcal{J}$ is radical by Proposition 4.3.10(a). □

Example 6.1.2. Let $\mathcal{I}$ be the radical unmixed ideal $((x_1 + 1)^2 + (x_2 - 1)^2 - 1)$ in general Noether position in $\mathbb{K}[x_1, x_2]$. We have $u_\Lambda = \Lambda_2 x_2$, and $q_\Lambda = T^2 - 2\Lambda_2 T + \Lambda_2^2(x_1^2 + 1)$. Then $\mathcal{J} = \mathcal{I} + (x_1) = ((x_2 - 1)^2, x_1)$ is not radical, and $Q_\Lambda = (T - \Lambda_2)^2$ is not square-free. Nevertheless, the square-free part $T - \Lambda_2$ of Q_Λ is the minimal polynomial of u_Λ modulo the extension of $\sqrt{\mathcal{J}} = (x_2 - 1)$ to $\mathbb{K}_\Lambda(x_1)[x_2]$.

We are now ready to give formulas to compute a univariate representation of $\sqrt{\mathcal{J}}$, when u remains a primitive element for $\sqrt{\mathcal{J}}$. Let $\tilde{Q}_\Lambda$ represent the square-free part of Q_Λ, and let

$$\tilde{W}_{\Lambda,j} = -\frac{\partial \tilde{Q}_\Lambda}{\partial \Lambda_j}.$$

Let $\tilde{Q}_\lambda, \tilde{W}_{\lambda,r+1}, \ldots, \tilde{W}_{\lambda,n}$ represent $\tilde{Q}_\Lambda, \tilde{W}_{\Lambda,r+1}, \ldots, \tilde{W}_{\Lambda,n}$ specialized at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$. By Proposition 6.1.1(a), $\tilde{Q}_\Lambda$ is the minimal polynomial of u_Λ modulo the extension of $\sqrt{\mathcal{J}}$ to $\mathbb{K}_\Lambda(x_1, \ldots, x_{s-1})[x_s, \ldots, x_n]$, so that by Corollary 4.3.11(b), $\tilde{Q}_\lambda, \tilde{W}_{\lambda,r+1}, \ldots, \tilde{W}_{\lambda,n}$ is the Kronecker representation of $\sqrt{\mathcal{J}}$ with primitive element u.

Let us now assume that we only know the representation $q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ of $\mathcal{I}$. From the only specializations $Q_\lambda, W_{\lambda,r+1}, \ldots, W_{\lambda,n}$ of the latter representation at $x_{s+1} = \cdots = x_r = 0$, one can easily compute the Kronecker representation of $\sqrt{\mathcal{J}}$ by the following formulas, whose proof relies on the Chinese remainder theorem:

Corollary 6.1.3. *Assume that $\mathcal{I}$ is radical, unmixed and in Noether position, and that u is primitive for $\mathcal{I}$ and for $\sqrt{\mathcal{J}}$.*

Let M_λ denote the greatest common divisor of Q_λ and Q'_λ, let $\tilde{q} = Q_\lambda/M_\lambda$ denote the square-free part of Q_λ, let $P_\lambda = Q'_\lambda/M_\lambda$, and let P_λ^{-1} denote the inverse of P_λ in $\mathbb{K}[T]/(\tilde{q}(T))$. Then M_λ divides all the $W_{\lambda,j}$, so that can set $V_{\lambda,j} = W_{\lambda,j}/M_\lambda$, for each $j \in \{r+1, \ldots, n\}$.

We define $\tilde{w}_j$ *as the remainder of* $\tilde{q}'V_{\lambda,j}P_\lambda^{-1}$ *divided by* $\tilde{q}(T)$*, for all* $j \in \{r+1,\ldots,n\}$*, and we let* $\tilde{w}_j = 0$*, for* $j \in \{s+1,\ldots,r\}$*. Then* $\tilde{q}, \tilde{w}_{s+1}, \ldots, \tilde{w}_n$ *is the Kronecker representation of* $\sqrt{\mathcal{J}}$ *with primitive element* u*.*

Proof. We have to prove that $\tilde{q} = \tilde{Q}_\lambda, \tilde{w}_{r+1} = \tilde{W}_{\lambda,r+1}, \ldots, \tilde{w}_n = \tilde{W}_{\lambda,n}$. Since u is a primitive element for $\sqrt{\mathcal{J}}$, Corollary 4.3.11(a) implies that $\tilde{Q}_\lambda$ is square-free, whence $\tilde{q} = \tilde{Q}_\lambda$. It follows that M_λ is the specialization of the greatest common divisor M_Λ of Q_Λ and Q'_Λ at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$.

Let $Q_\Lambda = Q_{\Lambda,1}^{\alpha_1} \cdots Q_{\Lambda,l}^{\alpha_l}$ represent the irreducible factorization of Q_Λ. Of course, we have $\tilde{Q}_\Lambda = Q_{\Lambda,1} \cdots Q_{\Lambda,l}$. We introduce $\hat{Q}_{\Lambda,j} = \tilde{Q}_\Lambda / Q_{\Lambda,j}$ and

$$\tilde{W}_{\Lambda,j,k} = -\frac{\partial Q_{\Lambda,k}}{\partial \Lambda_j}, \text{ for all } j \in \{r+1,\ldots,n\}, \text{and all } k \in \{1,\ldots,l\}.$$

We write $Q_{\lambda,j}$, $\hat{Q}_{\lambda,j}$ and $\tilde{W}_{\lambda,j,k}$ for the respective specializations of $Q_{\Lambda,j}$, $\hat{Q}_{\Lambda,j}$ and $\tilde{W}_{\Lambda,j,k}$ at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$. From

$$\frac{W_{\Lambda,j}}{M_\Lambda} = \sum_{k=1}^{l} \alpha_k \tilde{W}_{\Lambda,j,k} \hat{Q}_{\Lambda,k}, \text{ where } W_{\Lambda,j} = -\frac{\partial Q_\Lambda}{\partial \Lambda_j},$$

we deduce that

$$V_{\lambda,j} = \sum_{k=1}^{l} \alpha_k \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}.$$

Independently, a straightforward computation gives us the following identities:

$$\tilde{W}_{\lambda,j} = \sum_{k=1}^{l} \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}, \text{ and } P_\lambda = \sum_{k=1}^{l} \alpha_k Q'_{\lambda,k} \hat{Q}_{\lambda,k}.$$

Finally the fact that $P_\lambda \tilde{W}_{\lambda,j}$ equals $\tilde{Q}'_\lambda V_{\lambda,j}$ in $\mathbb{K}[T]/(\tilde{Q}_\lambda(T))$ is equivalent to the following identity in $\mathbb{K}[T]/(\tilde{Q}_\lambda(T))$:

$$\left(\sum_{k=1}^{l} \alpha_k Q'_{\lambda,k} \hat{Q}_{\lambda,k}\right)\left(\sum_{k=1}^{l} \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}\right) = \left(\sum_{k=1}^{l} Q'_{\lambda,k} \hat{Q}_{\lambda,k}\right)\left(\sum_{k=1}^{l} \alpha_k \tilde{W}_{\lambda,j,k} \hat{Q}_{\lambda,k}\right),$$

which is clearly satisfied modulo each $Q_{\lambda,k}$ for all $k \in \{1,\ldots,l\}$. □

Example 6.1.4. The Kronecker representation of $\mathcal{I} = (x_1^2 + (x_2-1)^2 - 1)$ with respect to x_2 is $q_\lambda = x_2^2 - 2x_2 + x_1^2$, $w_{\lambda,2} = 2x_2 - 2x_1^2$. By applying the formulas of Corollary 6.1.3, we obtain the Kronecker representation $\tilde{q} = x_2^2 - 2x_2, \tilde{w}_1 = 0, \tilde{w}_2 = 2x_2$ of $\sqrt{\mathcal{I} + (x_1)}$. This yields the univariate representation $q_0 = x_2^2 - 2x_2, v_{0,2} = x_2$ used in Example 5.4.3. To compute the Kronecker representation of $\sqrt{\mathcal{I} + (x_1 - 1)}$, we apply the formulas on the ideal $\mathcal{K} = ((y_2-1)^2 + (y_1+1)^2 - 1)$. We obtain the univariate representation $y_2 - 1, 0, 1$ of $\sqrt{\mathcal{K} + (y_1)}$ with respect to y_2, and thus the one $x_2 - 1, 1, 1$ of $\sqrt{\mathcal{I} + (x_1 - 1)}$ with respect to x_2.

Remark 6.1.5. Let $\mathcal{I}$ be a radical unmixed ideal in Noether position with primitive element u, and let $\delta = \deg_T(q_\Lambda)$ be the degree of the monic polynomial q_Λ. Then Corollary 4.3.11(b) ensures that $\deg_T(Q_\Lambda) = \deg_T(q_\lambda) = \delta$. Now if $\mathcal{J}$ is radical with primitive element u, then Proposition 6.1.1 ensures that Q_Λ is square-free, so that $\deg_T(\tilde{Q}_\lambda) = \delta$. Therefore $\deg(M_\lambda) = 1$, and the Kronecker representation of $\mathcal{J}$ is $q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ evaluated in $x_{s+1} = \ldots = x_n = 0$; we will widely use this particular case in Section 6.2.

Example 6.1.6. Let $\mathcal{I} = (x_3^2 + x_2^2 - 1)$, whose Kronecker representation with respect to x_3 is $q = T^2 + x_2^2 - 1, w_3 = -2x_2^2 + 2$ (see Figure 5.2.6). The Kronecker representation of $\mathcal{I} + (x_1, x_2)$ is $\tilde{q} = T^2 - 1, \tilde{w}_3 = 2$.

Corollary 6.1.3 allows the computation of the Kronecker representation of $\sqrt{\mathcal{J}}$. We now need a sufficient condition on $\mathcal{I}$ for $\mathcal{J}$ to be radical; Corollary 6.1.9 gives a genericity result to ensure this condition on $\mathcal{I}$.

Corollary 6.1.7. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position (respectively, general Noether position), and that $\mathcal{I} + (x_1, \ldots, x_r)$ is radical.*

(a) $\mathcal{J}$ is radical, unmixed with dimension s, and in Noether position (respectively, general Noether position).

(b) If $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ is a primitive element for $\mathcal{I} + (x_1, \ldots, x_r)$ then it is a primitive element for $\mathcal{J}$.

Proof. In order to prove part (a), it remains to prove that $\mathcal{J}$ is radical by Corollary 5.2.4. Since $\mathcal{I} + (x_1, \ldots, x_r)$ is radical, Proposition 6.1.1(b) (applied with $s = 0$) implies that the specialization of q_Λ at $x_1 = \cdots = x_r = 0$ is square-free. We deduce that Q_Λ is square-free, and Proposition 6.1.1(b) thus gives us the radicality of $\mathcal{J}$.

By combining Proposition 6.1.1 applied with $s = 0$ and Corollary 4.3.11(a) we obtain that the specialization of q_Λ at $x_1 = \cdots = x_r = 0$ and $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$ is square-free, so is the specialization of Q_Λ at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$. Therefore part (b) follows from Corollary 4.3.11(a). □

Example 6.1.8. Let $\mathcal{I} = (x_3^2 - x_2)$. Then $\mathcal{I} + (x_2) = (x_3^2, x_2)$ is not radical, and neither is $\mathcal{I} + (x_1, x_2) = (x_3^2, x_2, x_1)$. Geometrically speaking, each point in $\mathcal{V}(\mathcal{I} + (x_2))$ is a double root of $\mathcal{I} + (x_2)$, in particular the origin $\mathcal{V}(\mathcal{I} + (x_1, x_2))$.

Corollary 6.1.9. *Assume that $\mathcal{I}$ is radical, unmixed, and in Noether position. Then the set of points $(\beta_1, \ldots, \beta_r) \in \mathbb{K}^r$ such that $\mathcal{I} + (x_1 - \beta_1, \ldots, x_r - \beta_r)$ is radical is Zariski dense.*

Proof. Proposition 4.3.10(a) tells us that q_Λ is square-free, and thus that its discriminant is nonzero. If the specialization of this discriminant at $x_1 = \beta_1, \ldots, x_r = \beta_r$ is nonzero, then Proposition 6.1.1(b) implies that $\mathcal{I} + (x_1 - \beta_1, \ldots, x_r - \beta_r)$ is radical. □

Example 6.1.10. Let $\mathcal{I} = (x_3^2 - x_2)$ in $\mathbb{K}[x_1, x_2, x_3]$. For any $(\beta_1, \beta_2) \in \mathbb{K}^2$ with $\beta_2 \neq 0$, the ideal $\mathcal{I} + (x_1 - \beta_1, x_2 - \beta_2) = (x_3^2 - \beta_2^2, x_1 - \beta_1, x_2 - \beta_2)$ is radical.

The following corollary gathers our previous genericity results in a form that will be useful in Section 7.1. We let ϕ denote an affine change of the variables of the following form:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \alpha_{1,2} & \dots & \alpha_{1,n} \\ 0 & 1 & \dots & \alpha_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix},$$

where all the $\alpha_{k,l}$ and β_k are taken in $\mathbb{K}$.

Corollary 6.1.11. *Assume that $\mathcal{I}$ is radical and unmixed with dimension $r \geq 1$. Let f and g be in $\mathbb{K}[x_1, \dots, x_n]$ such that f is a nonzerodivisor in $\mathbb{B}$, and such that $(\mathcal{I} + (f)) : g^\infty \neq (1)$. Then $\sqrt{\mathcal{I} + (f)}$ and $\sqrt{\mathcal{I} + (f)} : g^\infty$ are unmixed of dimension $r - 1$, and there exists a Zariski dense subset of maps ϕ such that:*

(a) $\mathcal{I} \circ \phi$, $\sqrt{\mathcal{I} + (f)} \circ \phi$ and $(\sqrt{\mathcal{I} + (f)} : g^\infty) \circ \phi$ are in general Noether position;

(b) $\mathcal{I} \circ \phi + (x_1, \dots, x_r)$ is radical;

(c) $(\sqrt{\mathcal{I} + (f)} : g^\infty) \circ \phi + (x_1, \dots, x_{r-1}) = (\sqrt{\mathcal{I} + (f)} \circ \phi + (x_1, \dots, x_{r-1})) : (g \circ \phi)^\infty$;

(d) x_r is a primitive element for $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \dots, x_{r-1})}$;

(e) x_{r+1} is a primitive element for $\sqrt{\mathcal{I} \circ \phi + (x_1, \dots, x_{r-1}, x_r - a)}$, for each root $a \in \bar{\mathbb{K}}$ of the minimal polynomial of x_r modulo $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \dots, x_{r-1})}$.

Proof. Remark that $(\mathcal{I} + (f)) : g^\infty \neq (1)$ implies that $(\mathcal{I} + (f)) \neq (1)$, so that Theorem 5.2.1 implies that $\sqrt{\mathcal{I} + (f)}$ is unmixed of dimension $r-1$, and so is $\sqrt{\mathcal{I} + (f)} : g^\infty$ by Corollary 4.1.7. By combining Theorem 2.4.3, Corollary 4.1.7 and Proposition 5.1.2 we obtain that there exists a Zariski dense subset of maps ϕ such that property (a) holds. Property (b) comes from Corollary 6.1.9. Since g is a nonzerodivisor modulo $\sqrt{\mathcal{I} + (f)} : g^\infty$, property (c) follows from Corollary 5.2.7.

Now we suppose that properties (a)–(c) hold. From Corollary 5.2.4, we know that the ideal $\sqrt{(\mathcal{I} + (f)) \circ \phi + (x_1, \dots, x_{r-1})}$ has dimension 0. We introduce the linear forms $l_1, \dots, l_n$ defined by

$$(l_1, \dots, l_n) = \phi^{-1}(x_1, \dots, x_n).$$

By construction, $l_1, \dots, l_{r-1}$ are algebraically independent modulo $\mathcal{I} + (f)$ and $l_r, \dots, l_n$ are generally integral over $\mathbb{K}[l_1, \dots, l_{r-1}]$ modulo $\mathcal{I} + (f)$. Since the linear part of ϕ is upper triangular, we deduce from Proposition 2.3.9 that $x_r, \dots, x_n$ are also generally integral over $\mathbb{K}[l_1, \dots, l_{r-1}]$ modulo $\mathcal{I} + (f)$. Therefore we can naturally see $\sqrt{\mathcal{I} + (f) + (l_1, \dots, l_{r-1})}$ as an ideal of $\mathbb{K}[x_r, \dots, x_n]$, so that Corollary 4.3.12 gives us that the set of points $(\lambda_{r+1}, \dots, \lambda_n)$ such that $l_r = x_r + \lambda_{r+1}x_{r+1} + \dots + \lambda_n x_n$ is a primitive element for $\sqrt{\mathcal{I} + (f) + (l_1, \dots, l_{r-1})}$ is Zariski dense, which yields property (d).

Let $a \in \bar{\mathbb{K}}$ be as defined in part (e). By Corollary 5.2.4, $\sqrt{\mathcal{I} + (l_1, \dots, l_{r-1}, l_r - a)}$ has dimension 0. We can use Corollary 4.3.12 again in order to obtain that the set of points $(\lambda_{r+2}, \dots, \lambda_n)$ such that $l_{r+1} = x_{r+1} + \lambda_{r+2}x_{r+2} + \dots + \lambda_n x_n$ is a primitive element for $\sqrt{\mathcal{I} + (l_1, \dots, l_{r-1}, l_r - a)}$ is Zariski dense, which yields property (e). □

6.2 Lifting Step

In this section, we let r be a positive integer, and $f_1, \ldots, f_{n-r}, g$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. We assume that the ideal $\mathcal{I} = (f_1, \ldots, f_{n-r}) : g^\infty$ is unmixed, radical, in general Noether position, with dimension r and primitive element x_{r+1}. Moreover, we assume that the ideal $\mathcal{I} + (x_1, \ldots, x_r)$ is radical with same primitive element x_{r+1}, so that $\mathcal{J} = \mathcal{I} + (x_1, \ldots, x_r)$ and $\mathcal{K} = \mathcal{I} + (x_1, \ldots, x_{r-1})$ are radical unmixed with primitive element x_{r+1} by Corollary 6.1.7. We also assume that g is a nonzerodivisor modulo $\mathcal{J}$.

The input of the lifting step is the univariate representation $Q, V_{r+1}, \ldots, V_n$ of $\mathcal{J}$ seen in $\mathbb{K}[x_{r+1}, \ldots, x_n]$ with primitive element x_{r+1}. We write $Q, W_{r+1}, \ldots, W_n$ for the associated Kronecker representation. The output is the univariate representation $\tilde{Q}, \tilde{V}_{r+1}, \ldots, \tilde{V}_n$ of $\mathcal{K}$ seen in $\mathbb{K}[x_r, \ldots, x_n]$ with the same primitive element x_{r+1}; we write $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ for the associated Kronecker representation.

The ingredients of this lifting step are the Newton iteration that allows us to compute a Taylor expansion of $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ at any order, and Corollary 4.3.11 for the bound on the degrees of the $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$. We introduce $\hat{\mathbb{A}} = \mathbb{K}[[x_1, \ldots, x_r]]$, and $\hat{\mathbb{B}} = \hat{\mathbb{A}}[x_{r+1}, \ldots, x_n]/\hat{\mathcal{I}}$, where $\hat{\mathcal{I}}$ represents the extension of $\mathcal{I}$ to $\hat{\mathbb{A}}[x_{r+1}, \ldots, x_n]$. We let $q, w_{r+1}, \ldots, w_n$ (respectively, $q, v_{r+1}, \ldots, v_n$) denote the Kronecker (respectively, univariate) representation of $\mathcal{I}$ with primitive element x_{r+1}.

From Remark 6.1.5, we know that the specializations of $q, w_{r+1}, \ldots, w_n$ at $x_1 = \cdots = x_r = 0$ coincide with $Q, W_{r+1}, \ldots, W_n$ respectively, and that the specializations of $q, w_{r+1}, \ldots, w_n$ at $x_1 = \cdots = x_{r-1} = 0$ coincide with $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ respectively. Furthermore, thanks to Corollary 4.3.11(b), it is sufficient to compute the approximation of $q, w_{r+1}, \ldots, w_n$ in $\hat{\mathbb{A}}[T]$ to precision $(x_1, \ldots, x_{r-1}, x_r^{\delta+1})$ in order to obtain $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$, where δ denotes $\deg_T(q) = \deg(Q)$.

More generally we are going to present an algorithm that computes the approximation of $q, w_{r+1}, \ldots, w_n$ in $\hat{\mathbb{A}}[T]$ to any precision. This algorithm relies on a modified version of the classical Newton's method. Let $\mathfrak{o}^{[0]}$ be any ideal of $\hat{\mathbb{A}}$ contained in $(x_1, \ldots, x_r)$. It is sufficient to describe how to go from the approximation $q^{[0]}, w_{r+1}^{[0]}, \ldots, w_n^{[0]}$ to precision $\mathfrak{o}^{[0]}$ to the approximation $q^{[1]}, w_{r+1}^{[1]}, \ldots, w_n^{[1]}$ to precision $\mathfrak{o}^{[1]}$, for any ideal $\mathfrak{o}^{[1]}$ containing $(\mathfrak{o}^{[0]})^2$. Inside the approximation algorithm we will need the following statement, in which (b) is part of the classical Jacobian criterion:

Lemma 6.2.1. *The polynomials $v_{r+1} = w_{r+1}(q')^{-1}, \ldots, v_n = w_n(q')^{-1}$ are well defined in $\hat{\mathbb{A}}[T]$, and the following properties hold:*

(a) $\hat{\mathcal{I}} = (q(x_{r+1}), x_{r+1} - v_{r+1}(x_{r+1}), \ldots, x_n - v_n(x_{r+1}))$.

(b) The Jacobian matrix J of $f_1, \ldots, f_{n-r}$ with respect to the variables $x_{r+1}, \ldots, x_n$ is invertible in $\hat{\mathbb{B}}$.

Proof. We have already seen that q' is invertible modulo q in $\hat{\mathbb{A}}[T]$. Therefore $v_{r+1}, \ldots, v_n$ are well defined in $\hat{\mathbb{A}}[T]$, and we obtain the following inclusion from Corollary 4.3.11(b):

$$(q(x_{r+1}), x_{r+1} - v_{r+1}(x_{r+1}), \ldots, x_n - v_n(x_{r+1})) \subseteq \hat{\mathcal{I}}.$$

Conversely, for any $f \in \mathcal{I}$, we have that

$$f(x_1, \ldots, x_r, v_{r+1}(T), \ldots, v_n(T)) = 0 \text{ in } \mathbb{A}'[T]/(q(T)).$$

The fact that the latter equality also holds in $\hat{\mathbb{A}}[T]/(q(T))$ concludes part (a).

Let $u = \lambda_{r+1}x_{r+1} + \cdots + \lambda_n x_n$ be a $\mathbb{K}$-linear form, and let q_λ be its minimal polynomial in $\mathbb{B}'$. By Theorem 4.2.1(c), there exist some polynomials $h_1, \ldots, h_{n-r}$ in $\mathbb{K}[x_1, \ldots, x_n]$ and a nonnegative integer α such that $g^\alpha q_\lambda(u) = h_1 f_1 + \cdots + h_{n-r} f_{n-r}$. By differentiating with respect to $x_{r+1}, \ldots, x_n$, and by multiplying by g both sides of the latter equality, we deduce that all the entries of

$$g^{\alpha+1} q'_\lambda(u)(\lambda_{r+1}, \ldots, \lambda_n) - g(h_1, \ldots, h_{n-r})J \tag{6.2.1}$$

belong to $(f_1, \ldots, f_{n-r})$. Since g is a nonzerodivisor in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$, the constant coefficient of the minimal polynomial of g in $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$ is in $\mathbb{K} \setminus \{0\}$ by Lemma 5.1.1. Therefore by Proposition 6.1.1(a), the constant coefficient of the minimal polynomial of g in $\mathbb{B}$ is invertible in $\hat{\mathbb{B}}$, and so is g. Since (6.2.1) also holds over $\hat{\mathbb{A}}$ and since $q'(u)$ is invertible in $\hat{\mathbb{B}}$, we deduce that J is invertible in $\hat{\mathbb{B}}$, which proves part (b). □

Since $q^{[1]}$ coincides with $q^{[0]}$ to precision $\mathfrak{o}^{[0]}$, there exists a unique polynomial $\Delta \in \mathfrak{o}^{[0]}[T]$ defined to precision $\mathfrak{o}^{[1]}$, with $\deg(\Delta) \leq \delta - 1$, and such that $q^{[0]}(T)$ divides $q^{[1]}(T + \Delta(T))$ to precision $\mathfrak{o}^{[1]}$, namely $\Delta(T)$ is the remainder of $-q^{[1]}(q^{[1]\prime})^{-1}$ divided by $q^{[0]}$ to the precision $\mathfrak{o}^{[1]}$. For each $j \in \{r+1, \ldots, n\}$, we introduce the polynomial $\tilde{v}_j^{[1]}(T)$ as the remainder of $v_j^{[1]}(T + \Delta(T))$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$, where we recall $v_j = w_j(q')^{-1}$.

From Lemma 6.2.1(a), we know that:

$$f_i(x_1, \ldots, x_r, v_{r+1}^{[1]}(T), \ldots, v_n^{[1]}(T)) = 0 \text{ in } (\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[1]}(T)),$$

for all $i \in \{1, \ldots, n-r\}$. By substituting $T + \Delta(T)$ for T in the latter equality we deduce that:

$$f_i(x_1, \ldots, x_r, \tilde{v}_{r+1}^{[1]}(T), \ldots, \tilde{v}_n^{[1]}(T)) = 0 \text{ in } (\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[0]}(T)),$$

for all $i \in \{1, \ldots, n-r\}$. But thanks to Lemma 6.2.1(b), $\tilde{v}_{r+1}^{[1]}, \ldots, \tilde{v}_n^{[1]}$ can be obtained by means of the following Newton iteration computed in $(\hat{\mathbb{A}}/\mathfrak{o}^{[1]})[T]/(q^{[0]}(T))$ to precision $\mathfrak{o}^{[1]}$:

$$\begin{pmatrix} \tilde{v}_{r+1}^{[1]} \\ \vdots \\ \tilde{v}_n^{[1]} \end{pmatrix} = \begin{pmatrix} v_{r+1}^{[0]} \\ \vdots \\ v_n^{[0]} \end{pmatrix} - J^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_{n-r} \end{pmatrix} (x_1, \ldots, x_r, v_{r+1}^{[0]}, \ldots, v_n^{[0]}).$$

Now it remains to show how the $v_j^{[1]}$ can be recovered from the $\tilde{v}_j^{[1]}$. First of all, since $v_{r+1}^{[1]}(T) = T$, we easily recover $\Delta(T) = \tilde{v}_{r+1}^{[1]}(T) - T$. Then, for each $j \in \{r+1, \ldots, n\}$, by means of a second order Taylor expansion, we obtain that:

$$\tilde{v}_j^{[1]}(T) = v_j^{[1]}(T) + \Delta_j(T),$$

where $\Delta_j(T)$ represents the remainder of $\Delta(T)v_j^{[0]\prime}(T)$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$. This way we can deduce $v_j^{[1]}(T)$. In a similar manner we have that

$$q^{[1]}(T) = q^{[0]}(T) + \Delta_q(T),$$

where $\Delta_q(T)$ represents the remainder of $\Delta(T)q^{[0]\prime}(T)$ divided by $q^{[0]}(T)$ to precision $\mathfrak{o}^{[1]}$.

All these operations are summarized in the following algorithm:

Algorithm 6. *Lifting Step*

Input:
- $f_1, \ldots, f_{n-r}, g \in \mathbb{K}[x_1, \ldots, x_n]$ such that the ideal $\mathcal{I} = (f_1, \ldots, f_{n-r}) : g^\infty$ is radical unmixed in general Noether position with dimension r and primitive element x_{r+1}, and such that $\mathcal{J} = \mathcal{I} + (x_1, \ldots, x_r)$ is radical with same primitive element x_{r+1};
- the univariate representation $Q, V_{r+1}, \ldots, V_n$ of $\mathcal{J}$ seen in $\mathbb{K}[x_r, \ldots, x_n]$ with primitive element x_{r+1}; we let $\delta = \deg(Q)$.

Output: the Kronecker representation $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ of the ideal $\mathcal{K} = \mathcal{I} + (x_1, \ldots, x_{r-1})$ seen in $\mathbb{K}[x_r, \ldots, x_n]$ with primitive element x_{r+1}.

1. Initialize $\tilde{Q}$ with Q, $\tilde{V}_j$ with V_j for $j \in \{r+1, \ldots, n\}$, and ℓ with 0.
2. While $2^\ell \leq \delta + 1$, do
   a. compute $\tilde{v}_{r+1}, \ldots, \tilde{v}_n$ to precision $x_r^{2^{\ell+1}}$ with the formula
   $$\begin{pmatrix} \tilde{v}_{r+1} \\ \vdots \\ \tilde{v}_n \end{pmatrix} = \begin{pmatrix} \tilde{V}_{r+1} \\ \vdots \\ \tilde{V}_n \end{pmatrix} - \left(J^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_{n-r} \end{pmatrix} \right) (0, \ldots, 0, x_r, \tilde{V}_{r+1}, \ldots, \tilde{V}_n),$$
   where J^{-1} is the inverse of the Jacobian matrix J of $f_1, \ldots, f_{n-r}$ with respect to $x_{r+1}, \ldots, x_n$;
   b. compute $\Delta = \tilde{v}_{r+1} - x_{r+1}$;
   c. for j in $\{r+1, \ldots, n\}$, do
      i. compute the remainder Δ_j of $\Delta \frac{\partial \tilde{V}_j}{\partial x_{r+1}}$ divided by $\tilde{Q}$ to precision $x_r^{2^{\ell+1}}$;
      ii. replace $\tilde{V}_j$ with $\tilde{v}_j - \Delta_j$ to precision $x_r^{2^{\ell+1}}$.
   d. i. compute the remainder $\Delta_{\tilde{Q}}$ of $\Delta \frac{\partial \tilde{Q}}{\partial x_{r+1}}$ divided by $\tilde{Q}$ to precision $x_r^{2^{\ell+1}}$;
      ii. replace $\tilde{Q}$ with $\tilde{Q} + \Delta_{\tilde{Q}}$;
   e. replace ℓ with $\ell + 1$.
3. For j in $\{r+1, \ldots, n\}$, compute the remainder $\tilde{W}_j$ of $\tilde{V}_j \frac{\partial \tilde{Q}}{\partial x_{r+1}}$ divided by $\tilde{Q}$ to precision $x_r^{\delta+1}$.
4. Return $\tilde{Q}, \tilde{W}_2, \ldots, \tilde{W}_n$.

Proposition 6.2.2. *Algorithm 6 works correctly as specified.*

Proof. We obtain at step 3 a Taylor expansion of $\tilde{Q}, Wt_{r+1}, \ldots, Wt_n$ to precision $x_r^{\delta+1}$, that is exactly the wanted Kronecker representation of $\mathcal{J}$ by part (b) of Corollary 4.3.11. □

In step 4a, the value of the inverse of J can be computed with the classical iteration for the inverse. For more algorithmic details we refer the reader to [GLS01, Section 4].

Example 6.2.3. Let us recover the circle defined by $f_1 = x_1^2 + x_2^2 + x_3^2 - 1, f_2 = x_3 - x_1$ from the two points vanishing $(f_1, f_2) + (x_1)$. The univariate representation of $(f_1, f_2) + (x_1)$ with primitive element x_2 is $Q = x_2^2 - 1/2, V_2 = V_3 = x_2$. The degree of Q is $\delta = 2$, so that we will pass twice through the while loop. For $\ell = 0$, we have

$$\begin{pmatrix} \tilde{v}_2 \\ \tilde{v}_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_2 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} x_2 & -1 \\ x_2 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_2 \end{pmatrix},$$

so that $\Delta = 0$, and $\tilde{Q}, \tilde{V}_2, \tilde{V}_3$ remain unchanged. With $\ell = 1$, we compute

$$\begin{pmatrix} \tilde{v}_2 \\ \tilde{v}_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_2 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} x_2 & -1 \\ x_2 & 1 \end{pmatrix} \begin{pmatrix} x_1^2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_2 - x_1^2 x_2/2 \\ x_2 - x_1^2 x_2/2 \end{pmatrix}.$$

We thus have $\Delta = -x_1^2 x_2/2$, so that $\tilde{V}_2 = \tilde{V}_3 = x_2$. We recover the Kronecker representation $\tilde{Q} = 2x_2^2 + x_1^2 - 1, \tilde{W}_2 = \tilde{W}_3 = -x_1^2 + 1$ of (f_1, f_2) with respect to x_2.

As for Algorithms 4 and 5, part of the hypotheses needed for Algorithm 6 will be verified with an high probability after a random affine change of variables for any input system such that $(f_1, \ldots, f_{n-r}) : g^\infty$ is radical unmixed. Proposition 7.1.6 will permit us to bring back any zero-dimensional system to this situation by a linear mixing of the equations.

Chapter 7

A Kronecker Solver with Multiplicities

We are now ready to complete the presentation of the Kronecker solver as designed in [GLS01]. This algorithm computes a univariate representation of the ideal $\sqrt{(f_1, \ldots, f_n) : g^\infty}$ under some intrinsic geometric hypothesis on the input system $f_1, \ldots, f_n, g$. We extend it so that it further computes a univariate representation with multiplicities of any zero-dimensional ideal $(g_1, \ldots, g_n) : g^\infty$. We conclude this chapter with applying Proposition 5.3.1 to the definition of the degree of an ideal and a proof of a Bézout theorem. Both results are tools for the cost analysis of the Kronecker solver in [GLS01], from which we recall the result in Theorem 7.1.7.

7.1 Computation of the Radical

Let $f_1, \ldots, f_n, g \in \mathbb{K}[x_1, \ldots, x_n]$ be such that $f_1, \ldots, f_n$ is a reduced regular sequence in the open subset $\{g \neq 0\}$, as defined in the introduction of Part II. The algorithm computes some representations of

$$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty$$

in sequence for i from 0 to n, with the convention $\mathcal{I}_0 = (1)$. Since it is easy to make the algorithm stop as soon as it reaches $\mathcal{I}_i = (1)$, in order to simplify the presentation, we will assume in the rest of this section that $\mathcal{I}_i \neq (1)$ for all $i \in \{0, \ldots, n\}$.

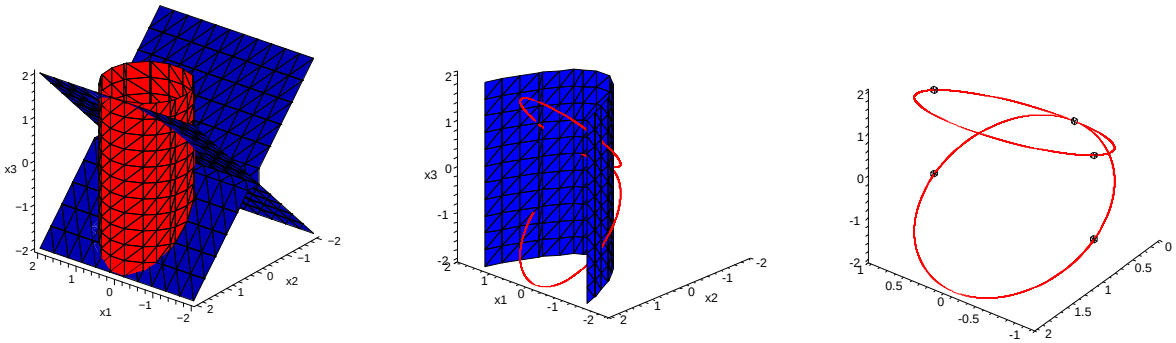
Under our hypotheses we have the following central properties:

Proposition 7.1.1. *Let $f_1, \ldots, f_n, g \in \mathbb{K}[x_1, \ldots, x_n]$ be such that $f_1, \ldots, f_n$ is a reduced regular sequence in the open subset $\{g \neq 0\}$. Then for all $i \in \{0, \ldots, n-1\}$, the ideals $\sqrt{\mathcal{I}_i + (f_{i+1})}$ and $\mathcal{I}_{i+1}$ are unmixed with dimension $n - i - 1$.*

Proof. By definition, $\mathcal{I}_0$ equals (0), hence is unmixed with dimension n. By induction, assume that $\mathcal{I}_i$ is unmixed of dimension $n - i$ for some $i \in \{0, \ldots, n-1\}$. Since f_{i+1} is assumed to be a nonzerodivisor modulo $\mathcal{I}_i$, Theorem 5.2.1 implies that $\sqrt{\mathcal{I}_i + (f_{i+1})}$ is either (1) or unmixed with dimension $n - i - 1$. From

$$\sqrt{\mathcal{I}_{i+1}} = \sqrt{(\mathcal{I}_i + (f_{i+1})) : g^\infty} = \sqrt{\mathcal{I}_i + (f_{i+1})} : g^\infty,$$

Figure 7.1.3.



$\mathcal{V}(f_1), \mathcal{V}(f_2)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_3)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_1, f_2, f_3)$

we deduce that $\mathcal{I}_i + (f_{i+1})$ has dimension $n - i - 1$ since $\mathcal{I}_{i+1}$ is assumed to be proper. When $i \leq n-2$, $\mathcal{I}_{i+1}$ is assumed to be radical, so that its unmixedness and its dimension follow from Corollary 4.1.7. When $i = n-1$, $\mathcal{I}_i + (f_{i+1})$ is necessarily unmixed of dimension 0, so that Corollary 4.1.7 gives us that $\mathcal{I}_{i+1}$ is unmixed of dimension 0. □

Example 7.1.2. Let

$$\begin{cases} f_1 &= x_1^2 + (x_2 - 1)^2 - 1 \\ f_2 &= x_3^2 - x_2^2 \\ f_3 &= x_2 - x_1^2 \\ g &= 1 \end{cases}$$

as in Example 4.3.14. Then $\mathcal{I}_1 = (f_1)$, respectively $\mathcal{I}_2 = (f_1, f_2)$, $\mathcal{I}_3 = (f_1, f_2, f_3)$ are unmixed with dimension 2, respectively 1, 0.

For $i \in \{1, \ldots, n\}$, we set

$$\mathcal{J}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i})}$$

and

$$\mathcal{K}_i = \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})},$$

that define a finite set and a curve obtained from $\mathcal{I}_i$ by specialization. The solver is organized around one main loop. The ith iteration of this loop computes the univariate representation of $\mathcal{J}_{i+1}$ with primitive element x_{n-i} from the one of $\mathcal{J}_i$ with primitive element x_{n-i+1}. This iteration divides into the following three steps:

1. *Lifting step.* Compute the Kronecker representation of $\mathcal{K}_i$ with primitive element x_{n-i+1}.
2. *Intersection step.* Compute the univariate representation of $\sqrt{\mathcal{K}_i + (f_{i+1})}$ with primitive element x_{n-i}.
3. *Cleaning step.* Compute the univariate representation of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty = \mathcal{J}_{i+1}$ with primitive element x_{n-i}.

Of course, these computations do not make sense without some hypotheses on the ideals $\mathcal{I}_i$, as for instance Noether position and suitable primitive elements. We use the genericity results

collected in the previous chapters to ensure these hypotheses. More precisely, before entering the main computations, the solver performs a random affine change of the variables in the input polynomials $f_1, \ldots, f_n$ and g so that the following properties hold:

A_1. $\mathcal{I}_i$ is unmixed of dimension $n-i$ and in general Noether position, for all $i \in \{0, \ldots, n\}$.

A_2. $\sqrt{\mathcal{I}_i + (f_{i+1})}$ is unmixed of dimension $n-i-1$ and in general Noether position, for all $i \in \{0, \ldots, n-1\}$.

A_3. $\sqrt{\mathcal{I}_i + (f_{i+1})} : g^\infty$ is unmixed of dimension $n-i-1$ and in general Noether position, for all $i \in \{0, \ldots, n-1\}$.

A_4. $\mathcal{I}_i + (x_1, \ldots, x_{n-i})$ is radical for all $i \in \{0, \ldots, n-1\}$.

A_5. $\mathcal{J}_{i+1} = \sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$, for all $i \in \{0, \ldots, n-1\}$.

A_6. x_{n-i} is a primitive element for $\sqrt{\mathcal{K}_i + (f_{i+1})}$, for all $i \in \{0, \ldots, n-1\}$.

A_7. x_{n-i+1} is a primitive element for $\sqrt{\mathcal{K}_i + (x_{n-i} - a)}$ for each root $a \in \bar{\mathbb{K}}$ (the algebraic closure of $\mathbb{K}$) of the minimal polynomial of x_{n-i} modulo $\sqrt{\mathcal{K}_i + (f_{i+1})}$, for all $i \in \{1, \ldots, n-1\}$.

A_8. $\mathcal{K}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i-1})$, is unmixed of dimension 1, and is in general Noether position when seen in $\mathbb{K}[x_{n-i}, \ldots, x_n]$, for all $i \in \{0, \ldots, n-1\}$.

A_9. $\mathcal{J}_i$ is zero dimensional, for all $i \in \{0, \ldots, n\}$.

A_{10}. x_{n-i+1} is a primitive element for $\mathcal{J}_i$, for all $i \in \{1, \ldots, n\}$.

A_{11}. x_{n-i+1} as a primitive element for $\mathcal{K}_i$, for all $i \in \{1, \ldots, n-1\}$.

A_{12}. x_{n-i+1} as a primitive element for $\mathcal{I}_i$, for all $i \in \{1, \ldots, n-1\}$.

We are to show that such a change of the variables can be found at random with a very high probability of success. More precisely, we are to prove that almost all affine changes of the variables ϕ with shape

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ 0 & 1 & \ldots & \alpha_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \tag{7.1.1}$$

ensures properties (A_1)–(A_{12}). Let us mention here that our approach closely follows [HMW01, Section 3].

Proposition 7.1.4. *There exists a Zariski dense subset of maps ϕ with shape (7.1.1) for which properties (A_1)–(A_{12}) are satisfied if we replace the input system by $f_1 \circ \phi = \cdots = f_n \circ \phi = 0$, $g \circ \phi \neq 0$.*

Proof. For any $i \in \{0, \ldots, n-1\}$, Corollary 6.1.11 applied with $\mathcal{I}_i$, f_{i+1} and g gives us properties (A_1)–(A_7) directly. Assume now that (A_1)–(A_7) hold. Then (A_8) and (A_9) are necessarily satisfied, by Corollaries 5.2.4 and 6.1.7(a). Property (A_{10}) is obtained via Proposition 4.3.1(a) thanks to (A_6) and the inclusion $\sqrt{\mathcal{K}_i + (f_{i+1})} \subseteq \mathcal{J}_{i+1}$. Finally, properties (A_{11}) and (A_{12}) follow from Corollary 6.1.7(b) thanks to (A_4). □

Example 7.1.5. As already seen in Example 4.3.14, the input system of Example 7.1.2 does not satisfy (A_6). After the change of variables

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

we obtain the system

$$\begin{cases} f_1 &= (x_1 + 2x_2 + 4x_3)^2 + (x_2 - 1)^2 + 1 \\ f_2 &= x_3^2 - x_2^2 \\ f_3 &= x_2 - (x_1 + 2x_2 + 4x_3)^2 \\ g &= 1, \end{cases}$$

which satisfies all properties (A_1)–(A_{12}).

Here it is important to underline that such a change ϕ of the variables does not spoil the evaluation cost of the input system: using evaluation data structures for the input polynomials is a great advantage here. Of course this operation yields a probabilistic aspect in the Kronecker algorithm: if we choose a map ϕ for which one of the properties (A_1)–(A_7) is not verified, the output of the algorithm may not be correct. Nevertheless, the fact that "bad choices" of maps ϕ are enclosed in a Zariski closed subset ensure that the probability that this occurs is very small. Moreover, we could control this probability by evaluating the degrees of the polynomials defining the different Zariski subsets. Estimating such a degree is quite technical here, since the bad choices of the fibers β depend on the choosen Noether position α; by analogy with [HMW01, Section 3], we expect a degree belonging to $D^{\mathcal{O}(1)}$, where D is the product of all the degrees of the input polynomials. The reader interessed in this kind of result may consult [Mat99, KPS01].

In the case when $\mathcal{I}_n = (f_1, \ldots, f_n) : g^\infty$ is not radical, Algorithm 5 permits us to compute a univariate representation with multiplicities at the last intersection step. The following variant of Bertini's lemma further permits to discard the reduced regular sequence hypothesis on the input by ensuring that a suitable random mix of the input equations postpones the multiplicities to the last intersection step. These idea has already be used for algorithmic purpose, for instance in [GH93, KP96]; we refer to [Lec00] for bounds on the probability of failure. We directly give a statement in a form that will be useful for Section 10.2 in Part III, when we use it here with $s = n$:

Proposition 7.1.6. *Let $g_1, \ldots, g_s, g$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ such that $(g_1, \ldots, g_s) : g^\infty$ is a zero-dimensional ideal. Let $\tau = \min(s, n+1)$. Then there exists a Zariski dense open subset $\mathcal{U}$ of $\overline{\mathbb{K}}^{\tau \times s}$ such that for all $\alpha = (\alpha_{k,\ell})_{1 \le \ell \le \tau,\ 1 \le k \le s} \in \mathcal{U}$, the sequence*

$$f_\ell = \alpha_{1,\ell} g_1 + \cdots + \alpha_{s,\ell} g_s, \ell \in \{1, \ldots, \tau\}$$

satisfies the following properties:

(a) *$f_1, \ldots, f_n$ is a reduced regular sequence in the open subset $\{g \neq 0\}$.*

(b) *If $s = n$, then $(f_1, \ldots, f_n) : g^\infty = (g_1, \ldots, g_n) : g^\infty$;*
if $s \geq n+1$, then $(f_1, \ldots, f_n) : g^\infty + (f_{n+1}) = (g_1, \ldots, g_s) : g^\infty$.

Proof. Following [Lec00], we let $\mathcal{V}$, respectively, $\mathcal{V}_i$ for $i \in \{1, \ldots, \tau\}$, denote the variety of zeros of $(g_1, \ldots, g_s)$ in $\bar{\mathbb{K}}^n$, respectively, of $(f_1, \ldots, f_i)$. We let $\tilde{\mathcal{V}}$, respectively, $\tilde{\mathcal{V}}_i$, denote the variety of zeros of $(g_1, \ldots, g_s) : g^\infty$ in $\bar{\mathbb{K}}^n$, respectively, of $(f_1, \ldots, f_i) : g^\infty$; the irreducible components of $\tilde{\mathcal{V}}_i$ are the components of $\mathcal{V}_i$ that are not included in the set of zeros of g. By [Lec00, Lemma 1], for α in a Zariski dense open subset of $\bar{\mathbb{K}}^{\tau s}$, for any irreducible component $\mathcal{W}$ of $\mathcal{V}_i$ of dimension $n - i$, either $\mathcal{W}$ is a component of $\mathcal{V}$, or the variety of zeros of f_{i+1} intersects $\mathcal{W}$ regularly. Then for $i \in \{1, \ldots, n-1\}$, the variety of zeros of f_{i+1} intersects all the components of $\tilde{\mathcal{V}}_i$ regularly since $\tilde{\mathcal{V}}$ is zero-dimensional. The sequence $f_1, \ldots, f_n$ is thus regular in $\{g \neq 0\}$. In the overdetermined case, the previous alternative ensures us that, if m is a point of $\tilde{\mathcal{V}}_n$ that do not belong to $\tilde{\mathcal{V}}$, then m does not vanish f_{n+1}, which gives part (b). Lastly, a similar argument with [Lec00, Lemma 2] yields the radicality of the ideals $(f_1, \ldots, f_i) : g^\infty$, $i \in \{1, \ldots, \tau\}$ for α in a Zariski dense open subset of $\bar{\mathbb{K}}^{\tau s}$. □

We now summarize the main algorithm:

Algorithm 7. *Kronecker Solver with Multiplicities*

Input: $g_1, \ldots, g_n, g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $(g_1, \ldots, g_n) : g^\infty$ is zero-dimensional.

Output: a univariate representation with multiplicities $\chi, Q, V_1, \ldots, V_n$ of $(g_1, \ldots, g_n) : g^\infty$.

1. Let A be a random invertible $n \times n$ matrix with entries in $\mathbb{K}$, and set
$$(f_1, \ldots, f_n) = (A(g_1, \ldots, g_n)^t)^t.$$
2. Let ϕ be a random map as in (7.1.1), and replace $f_1, \ldots, f_n, g$ with $f_1 \circ \phi, \ldots, f_n \circ \phi, g \circ \phi$.
3. Let $Q = f_1(0, \ldots, 0, x_n)/\gcd(f_1(0, \ldots, 0, x_n), g(0, \ldots, 0, x_n))$, $V_n = x_n$ be the univariate representation of $\mathcal{J}_1$ with respect to x_n.
4. For i from 1 to $n - 1$
   a. by Algorithm 6, compute the Kronecker representation of $\mathcal{K}_i$ with primitive element x_{n-i+1};
   b. by Algorithm 5, compute the univariate representation (with multiplicities if $i = n - 1$) of $\mathcal{K}_i + (f_{i+1})$ with primitive element x_{n-i};
   c. by Algorithm 4, compute the univariate representation (with multiplicities if $i = n - 1$) of $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty = \mathcal{J}_{i+1}$ with primitive element x_{n-i}.
5. Return $\chi, Q, \phi^{-1}(V_1, \ldots, V_n)$.

Theorem 7.1.7. *Let $g_1, \ldots, g_n, g$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ given by a straight-line program of size L such that $(g_1, \ldots, g_n) : g^\infty$ is a zero-dimensional ideal. We let d_i denote the degree of g_i, assume that $d_1 \geq \cdots \geq d_n$, and set $D = \prod_{i=1}^n d_i$ and $d = \max(d_1, \ldots, d_n)$. Then Algorithm 7 computes a univariate representation with multiplicities of $(g_1, \ldots, g_n) : g^\infty$ by performing*

$$\tilde{\mathcal{O}}(n(nL + n^4)(dD)^2)$$

arithmetic operations in $\mathbb{K}$. The correctness of the output relies on random choices of $\mathcal{O}(n^2)$ elements of $\mathbb{K}$; choices for which the result is not correct are enclosed in a strict algebraic subset.

Proof. Algorithm 7 works correctly as specified for A and ϕ outside a strict algebraic subset by Propositions 7.1.6, 7.1.4, 4.4.2, 5.4.2 and 6.2.2. Steps 1 and 2 replace the straight-line program of size L given as input with a straight-line program of size $L + 2n^2$. Now, since $d_1 \geq \cdots \geq d_n$, the degree of the variety of zeros of $(f_1, \ldots, f_i) : g^\infty$ is at most $d_1 \cdots d_i$ by Corollary 7.2.8 below. The complexity bound is thus a direct consequence of [GLS01, Theorem 1]. □

Example 7.1.8. Let us continue with the data of Example 7.1.2. Since f_1, f_2, f_3 already form a regular sequence, we do not need to mix the equations. We perform the change of variables announced in Example 7.1.5, and deal with the new equations f_1, f_2, f_3. We enter the third pass through the while loop with a univariate representation of $\mathcal{J}_2 = \sqrt{(f_1, f_2) + (x_1)}$, which lifts into the univariate representation of $\mathcal{K}_2 = (f_1, f_2)$ given in Example 4.3.3. At the end of the intersection step, we obtain the following univariate representation of (f_1, f_2, f_3) with multiplicities:

$$\left\{\begin{array}{lcl} \chi & = & x_1^3(x_1-3)(x_1-1)(x_1+5)(x_1+7), \\ Q & = & x_1(x_1-3)(x_1-1)(x_1+5)(x_1+7), \\ V_1 & = & x_1, \\ V_2 & = & -\frac{11866}{1157625}x_1^6 - \frac{105848}{1157625}x_1^5 + \frac{811}{46305}x_1^4 + \frac{1255064}{1157625}x_1^3, \\ V_3 & = & \frac{389}{44100}x_1^5 + \frac{3427}{44100}x_1^4 - \frac{401}{17640}x_1^3 - \frac{41401}{44100}x_1^2 - \frac{1}{8}x_1. \end{array}\right.$$

Since $g = 1$, the cleaning step has no effect. By applying the inverse change of variables $x_1 \to x_1 - 2x_2 - 4x_3$, we recover a univariate representation in the original coordinates:

$$\left\{\begin{array}{lcl} \chi & = & T^3(T-3)(T-1)(T+5)(T+7), \\ Q & = & T(T-3)(T-1)(T+5)(T+7), \\ V_1 & = & 2\frac{11866}{1157625}T^6 + (2\frac{105848}{1157625} - 4\frac{389}{44100})T^5 + (-2\frac{811}{46305} - 4\frac{3427}{44100})T^4, \\ & & +(-2\frac{1255064}{1157625} + 4\frac{401}{17640})T^3 + (4\frac{41401}{44100})T^2 + (1 + 4\frac{1}{8})T, \\ V_2 & = & -\frac{11866}{1157625}T^6 - \frac{105848}{1157625}T^5 + \frac{811}{46305}T^4 + \frac{1255064}{1157625}T^3, \\ V_3 & = & \frac{389}{44100}T^5 + \frac{3427}{44100}T^4 - \frac{401}{17640}T^3 - \frac{41401}{44100}T^2 - \frac{1}{8}T. \end{array}\right.$$

One can read from this formulas that the multiplicity of the origin as a root of (f_1, f_2, f_3) is 3. We will compute in Part III the structure of this multiple point.

For our main Algorithm 14 in Section 10.3, we will act on the last intersection step, and we will deal with overdetermined systems. We will rather use a variant of the Algorithm 7, that returns some intermediate results:

Corollary 7.1.9. *Let $g_1, \ldots, g_s, g$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ given by a straight-line program of size L, such that $(g_1, \ldots, g_s) : g^\infty$ is a zero-dimensional ideal. We let d_i denote the degree of g_i, we assume that $d_1 \geq \cdots \geq d_s$, and we set $D = \prod_{i=1}^n d_i$ and $d = \max(d_1, \ldots, d_n)$. Then we can compute*

- *an affine change of variables* ϕ *as in* (7.1.1),
- *an unmixed one-dimensional radical ideal* $\mathcal{I}$ *under the form of its Kronecker representation* $q, w_3, \ldots, w_n$ *in* x_2,
- *a polynomial* $f \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $(\mathcal{I} + (f)) : (g \circ \phi)^\infty$ *is zero-dimensional, and equals* $((g_1, \ldots, g_n) : g^\infty) \circ \phi$ *if* $s = n$,
- *the univariate representation with multiplicities* $\chi, Q, V_1, V_2, \ldots, V_n$ *in* x_1 *of* $(\mathcal{I} + (f)) : (g \circ \phi)^\infty$,
- *if* $s > n$, *a polynomial* $h \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $((g_1, \ldots, g_s) : g^\infty) \circ \phi = ((\mathcal{I} + (f)) : (g \circ \phi)^\infty) + (h)$

with

$$\tilde{\mathcal{O}}(n(n(L + ns) + n^4)(dD)^2)$$

arithmetic operations in $\mathbb{K}$. *The correctness of the output relies on random choices of* $\mathcal{O}(ns)$ *elements of* $\mathbb{K}$; *choices for which the result is not correct are enclosed in a strict algebraic subset. The polynomials* f *and* h *are given by a straight-line program of size* $L + ns + n^2$.

Proof. If $s > n$, we replace A by a matrix with $n+1$ rows and s columns in step 1 of Algorithm 7. We thus obtain a new system $f_1, \ldots, f_{n+1}$. We will take $\mathcal{I} = (f_1 \circ \phi, \ldots, f_{n-1} \circ \phi) : (g \circ \phi)^\infty$, $f = f_n \circ \phi$ and $h = f_{n+1} \circ \phi$. For ϕ and A in Zariski dense open subsets, $\mathcal{I}, f$ and h check the asked properties by Propositions 7.1.4 and 7.1.6. Moreover, Algorithm 7 computes the univariate representations of $\mathcal{I}$ and $\mathcal{I} + (f)$.

Steps 1 and 2 replace the straight line program of size L given as input with a straight-line program of size $L+ns+n^2$. The complexity bound is thus a consequence of Theorem 7.1.7. □

Example 7.1.10. With the data of Example 7.1.8, we return the affine change of variable ϕ defined in Example 7.1.5, the Kronecker representation in x_2 of the one-dimensional ideal $((x_1+2x_2+4x_3)^2+(x_2-1)^2+1, x_3^2-x_2^2)$ given in Example 4.3.3, and the univariate representation in x_1 computed in Example 7.1.8.

7.2 Degree and Bézout's Theorem

In this last subsection we prove the necessary results in the degree theory that are needed in the cost analysis of the Kronecker solver; we will not reproduce this analysis in the present thesis, and refer the reader to [GLS01]. In the univariate case, the degree of a polynomial f coincides with the dimension of $\mathbb{K}[x_1]/(f)$. This notion can be extended to any ideal $\mathcal{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$, as explained below. Theorem 7.2.7 gives an information on the degree of $\mathcal{I} + (f)$ from the ones of $\mathcal{I}$ and (f).

Let $\mathcal{I}$ be any ideal in $\mathbb{K}[x_1, \ldots, x_n]$, and let M denote an invertible $n \times n$ matrix over $\mathbb{K}$. In short, we write $\mathcal{I}_M = \mathcal{I} \circ M$, $\mathbb{B}_M = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_M$, $\mathbb{B}'_M = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}'_M$, where $\mathcal{I}'_M$ denotes the extension of $\mathcal{I}_M$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$. We write δ (respectively, δ_M) for the dimension

of $\mathbb{B}'$ (respectively, $\mathbb{B}'_M$) seen as a $\mathbb{A}'$-vector space. Proposition 5.3.1 is a central ingredient to prove the next theorem that asserts that if $\mathcal{I}$ and $\mathcal{I}_M$ are both in general Noether position then $\delta = \delta_M$.

Theorem 7.2.1. *Assume that $\mathcal{I}$ is unmixed and in general Noether position.*

(a) $\delta_M \leq \delta$.

(b) $\delta_M = \delta$ *if, and only if,* $\mathcal{I}_M$ *is in general Noether position.*

Since the proof of Theorem 7.2.1 is quite long, we postpone it to the end of the section. Theorem 7.2.1 ensures that the following definition of the degree of $\mathcal{I}$ actually makes sense.

Definition 7.2.2. The *degree* of an unmixed ideal $\mathcal{I}$, written $\deg(\mathcal{I})$, is the dimension of $\mathbb{B}'_M$ seen as an $\mathbb{A}'$-vector space, for any matrix M such that $\mathcal{I} \circ M$ is in general Noether position.

Example 7.2.3. The degree of any conical is 2, as for instance $\deg(x_1^2 + (x_2 - 1)^2 - 1) = 2 = \deg(x_2 - x_1^2)$. We have computed a univariate representation of the ideal $\mathcal{I} = (x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ at the end of Chapter 5; we have $\deg(\mathcal{I}) = 4$, which is the number of roots of the ideal counted with multiplicities.

Remark 7.2.4. In the case when $\mathcal{I} = (f)$ is a principal ideal, $\deg(\mathcal{I})$ equals the total degree of the polynomial f.

Remark that $\deg((0)) = 1$, and that $\deg(\mathcal{I}) = 0$ if, and only if, $\mathcal{I} = (1)$. The degree decreases when we remove points or multiplicities, as proved in:

Proposition 7.2.5. *Assume that $\mathcal{I}$ is unmixed.*

(a) $\deg(\sqrt{\mathcal{I}}) \leq \deg(\mathcal{I})$*; the inequality is an equality if, and only if, $\mathcal{I}$ is radical.*

(b) $\deg(\mathcal{I} : g^\infty) \leq \deg(\mathcal{I})$*, for any polynomial g; the inequality is an equality if, and only if, g is a nonzerodivisor in $\mathbb{B}$.*

Proof. By Theorem 2.4.3, we can assume that $\mathcal{I}$ is in general Noether position. The inequality of part (a) trivially follows from the inclusion of $\mathcal{I}'$ in the extension of $\sqrt{\mathcal{I}}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$. If the equality holds in part (a) then this extension of $\sqrt{\mathcal{I}}$ coincides with $\mathcal{I}'$. Therefore $\mathcal{I}'$ is radical, and so is $\mathcal{I}$ by Corollary 4.1.5. We are done with part (a).

If $\mathcal{I} : g^\infty = (1)$ then part (b) trivially holds. Otherwise Corollary 4.1.7 tells us that $\mathcal{I} : g^\infty$ is unmixed of dimension r and in general Noether position. On the other hand the extension of $\mathcal{I} : g^\infty$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]$ coincides with $\mathcal{I}' : g^\infty$. Therefore we obtain that $\deg(\mathcal{I} : g^\infty) \leq \deg(\mathcal{I})$. If g is a nonzerodivisor in $\mathbb{B}$, then $\mathcal{I} = \mathcal{I} : g^\infty$, whence $\deg(\mathcal{I} : g^\infty) = \deg(\mathcal{I})$. Conversely, if the latter equality holds then $\mathcal{I}' : g^\infty = \mathcal{I}'$, whence $\mathcal{I} : g^\infty = \mathcal{I}$ by Proposition 4.1.1. □

Example 7.2.6. With the data of Example 4.4.4 at the end of Chapter 4, we have $\deg(\mathcal{I}) = 4$ when $\deg(\mathcal{I} : g^\infty) = 2$. Removing multiplicities, we obtain $\deg(\sqrt{\mathcal{I} : g^\infty}) = 1$.

In Example 7.2.3, we have seen that $\deg((x_1^2+(x_2-1)^2-1)+(x_2-x_1^2)) = \deg(x_1^2+(x_2-1)^2-1)+\deg(x_2-x_1^2)$. Though the equality may not be true in the affine case, Proposition 5.3.1 is the core of the following version of the Bézout theorem:

Theorem 7.2.7. *Assume that $\mathcal{I}$ is unmixed. Let f be a nonzerodivisor in $\mathbb{B}$, and let $\tilde{\mathcal{J}}$ denote the intersection of the primary components $\mathcal{Q}$ of $\mathcal{J} = \mathcal{I}+(f)$ belonging to an isolated associated prime $\mathfrak{p}$. Then we have that $\deg(\tilde{\mathcal{J}}) \leq \deg(\mathcal{I})\deg(f)$. In addition, if $\mathcal{I}$ and f are homogeneous, then the latter inequality is an equality.*

Proof. By Theorem 2.4.3, we can assume that $\mathcal{I}$ and $\mathcal{J}$ are in general Noether position. From Theorem 5.2.1 we know that $\tilde{\mathcal{J}}$ is unmixed of dimension -1 or $r-1$. By means of Theorem 2.2.5(a) we observe that the extensions of $\tilde{\mathcal{J}}$ and $\mathcal{J}$ coincide in $\mathbb{K}(x_1,\ldots,x_{r-1})[x_r,\ldots,x_n]$. Then Proposition 5.3.1 tells us that $\deg(\tilde{\mathcal{J}})$ equals the total degree of the constant coefficient χ_0 of the characteristic polynomial of f in $\mathbb{B}'$. Thanks to Theorem 4.2.1(b), we deduce that $\deg(\tilde{\mathcal{J}}) \leq \deg(\mathcal{I})\deg(f)$. Finally, Theorem 4.2.1(a) implies that the latter inequality is an equality in the homogeneous case. □

Corollary 7.2.8. *Let $g_1,\ldots,g_s$ be polynomials in $\mathbb{K}[x_1,\ldots,x_n]$ with degrees $d_1 \geq \cdots \geq d_s$. Let $f_1,\ldots,f_n$ be linear combinations of $g_1,\ldots,g_s$ as in Proposition 7.1.6, and let $g \in \mathbb{K}[x_1,\ldots,x_n]$. Then for any $i \in \{1,\ldots,n\}$, we have $\deg((f_1,\ldots,f_i) : g^\infty) \leq d_1\cdots d_i$.*

Proof. First let us remark that we can assume that $\deg(f_i) \leq d_i$ without loss of generality. We proceed by induction on i, and set $\mathcal{I}_i = (f_1,\ldots,f_i) : g^\infty$, which is unmixed by Proposition 7.1.1. Proposition 7.2.5(b) direcly yields $\deg(\mathcal{I}_1) \leq d_1$. For $i \in \{1,\ldots,n-2\}$, since considering the radical of an ideal "kills" the embedded primes, Theorem 7.2.7 together with Proposition 7.2.5(a) yields

$$\deg\left(\sqrt{\mathcal{I}_i+(f_{i+1})}\right) \leq \deg(\mathcal{I}_i)\deg(f_{i+1}).$$

Since $\mathcal{I}_{i+1}$ is radical, we have $\mathcal{I}_{i+1} = \sqrt{(\mathcal{I}_i+(f_{i+1})) : g^\infty} = \sqrt{(\mathcal{I}_i+(f_{i+1}))} : g^\infty$, which gives the result for $\mathcal{I}_{i+1}$ by Proposition 7.2.5(b). If $i = n-1$, we can directly apply Theorem 7.2.7 since the zero-dimensional ideal $\mathcal{I}_n$ does not have embedded primes. □

We end this section with the proof of Theorem 7.2.1. The idea of the proof relies on a suitable set of generators of the group of $n \times n$ invertible matrices over $\mathbb{K}$. For this purpose, we introduce the following block notation:

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{pmatrix},$$

with $M_{1,1}$ of size $r \times r$; Id_r represents the $r \times r$ identity matrix.

Lemma 7.2.9. *Assume that $\mathcal{I}$ is unmixed and that M is in one of the following three forms:*

$$\begin{pmatrix} \mathrm{Id}_r & 0 \\ M_{2,1} & \mathrm{Id}_{n-r} \end{pmatrix}, \begin{pmatrix} M_{1,1} & 0 \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}, \text{ or } \begin{pmatrix} \mathrm{Id}_r & 0 \\ 0 & M_{2,2} \end{pmatrix}.$$

(a) $\mathcal{I}$ *is in Noether position (respectively, general Noether position) if, and only if,* $\mathcal{I}_M$ *is in Noether position (respectively, general Noether position).*

(b) $\delta_M = \delta$.

Proof. In the first two cases, part (a) can be straightforwardly verified from the definitions of the Noether positions, whereas the third case follows from Proposition 2.1.5 (respectively, Proposition 2.3.9). Since, in the three cases, M defines an isomorphism of $\mathbb{K}[x_1, \ldots, x_n]$ that leaves $\mathbb{A}$ globally unchanged and that sends $\mathcal{I}$ to $\mathcal{I}_M$, we clearly have that $\delta_M = \delta$. □

Remark that δ is finite and positive. If $x_1, \ldots, x_r$ are algebraically dependent modulo $\mathcal{I}_M$ then $\mathcal{I}'_M = (1)$, whence $\mathbb{B}'_M = 0$ and $\delta_M = 0$. In this situation, the theorem trivially holds, so that we can assume from now on that $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}_M$. In this situation δ_M is finite since $x_{r+1}, \ldots, x_n$ are necessarily algebraic over $\mathbb{A}$ modulo $\mathcal{I}_M$ thanks to Theorem 2.2.5(b).

Claim 7.2.10. *Without loss of generality, we can assume from the outset that*

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}.$$

Proof. Since M is invertible, the rank of the submatrix $\begin{pmatrix} M_{1,1} & M_{1,2} \end{pmatrix}$ is r, so that there exists a $(n-r) \times r$ matrix N such that $M_{1,1} - M_{1,2}N$ is invertible. Then a straightforward calculation gives us that

$$M = \begin{pmatrix} M_{1,1} - M_{1,2}N & M_{1,2} \\ M_{2,1} - M_{2,2}N & M_{2,2} \end{pmatrix} \begin{pmatrix} \mathrm{Id}_r & 0 \\ N & \mathrm{Id}_{n-r} \end{pmatrix}.$$

Thanks to Lemma 7.2.9, we can assume from the outset that $M_{1,1}$ is invertible. And since we have that

$$M = \begin{pmatrix} \mathrm{Id}_r & 0 \\ M_{2,1}M_{1,1}^{-1} & \mathrm{Id}_{n-r} \end{pmatrix} \begin{pmatrix} M_{1,1} & M_{1,2} \\ 0 & M_{2,2} - M_{2,1}M_{1,1}^{-1}M_{2,1} \end{pmatrix},$$

we can now assume that $M_{2,1} = 0$, thanks to Lemma 7.2.9 again. Finally the claim follows by using Lemma 7.2.9 once more time in order to reach $M_{2,2} = \mathrm{Id}_{n-r}$. □

Let $y_1, \ldots, y_r$ be new variables, and let

$$\mathbb{A}_y = \mathbb{K}[y_1, \ldots, y_r], \quad \mathbb{A}'_y = \mathbb{K}(y_1, \ldots, y_r).$$

For each $i \in \{1, \ldots, r\}$, we introduce the linear form

$$l_i = y_i - (\omega_{i,1}x_1 + \cdots + \omega_{i,n}x_n) \in \mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n],$$

where $\omega_{i,j}$ stands for the (i,j)th entry of M^{-1}. For each $i \in \{0, \ldots, r\}$, we write $\mathcal{I}_i$ for the ideal $\mathcal{I} + (l_1, \ldots, l_i)$ of $\mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n]$. We define $\mathcal{I}'_i$ as the extension of $\mathcal{I}_i$ to $\mathbb{A}'_y[x_1, \ldots, x_n]$, and let:

$$\mathbb{B}_i = \mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_n]/\mathcal{I}_i \text{ and } \mathbb{B}'_i = \mathbb{A}'_y[x_1, \ldots, x_n]/\mathcal{I}'_i.$$

We define δ_i as the dimension of the $\mathbb{A}'_y(x_1,\dots,x_{r-i})$-vector space

$$\mathbb{B}''_i = \mathbb{A}'_y(x_1,\dots,x_{r-i})[x_{r-i+1},\dots,x_n]/\mathcal{I}''_i,$$

where $\mathcal{I}''_i$ represents the extension of $\mathcal{I}'_i$ to $\mathbb{A}'_y(x_1,\dots,x_{r-i})[x_{r-i+1},\dots,x_n]$.

It is straightforward to check that $x_1,\dots,x_r,y_{i+1},\dots,y_r$ are algebraically independent modulo $\mathcal{I}_i$, and that $x_{r+1},\dots,x_n,y_1,\dots,y_i$ are generally integral over

$$\mathbb{K}[x_1,\dots,x_r,y_{i+1},\dots,y_r]$$

modulo $\mathcal{I}_i$ by Proposition 2.3.9. From Theorem 2.2.5(a) we deduce that $\dim(\mathcal{I}_i) = 2r - i$. Furthermore, by means of Proposition 4.1.1, it can be verified that the unmixedness of $\mathcal{I}$ implies the one of $\mathcal{I}_i$. This way, we obtain from Proposition 5.1.2(a) that l_{i+1} is a nonzerodivisor $\mathbb{B}_i$.

Claim 7.2.11. *We have $\delta = \delta_0$ and $\delta_M = \delta_r$. The ideal $\mathcal{I}_r$ is in general Noether position if, and only if, $\mathcal{I} \circ M$ is in general Noether position.*

Proof. The former equality is straightforward while the latter equality and the equivalence between the Noether positions both follow from:

$$\begin{aligned}\mathcal{I}_r = (f \circ M(y_1,\dots,y_r,x_{r+1},\dots,x_n) \mid f \in \mathcal{I}) + \\ (x_1 - (m_{1,1}y_1 + \cdots + m_{1,r}y_r + m_{1,r+1}x_{r+1} + \cdots + m_{1,n}x_n),\\ \dots,\\ x_r - (m_{r,1}y_1 + \cdots + m_{r,r}y_r + m_{r,r+1}x_{r+1} + \cdots + m_{r,n}x_n)),\end{aligned}$$

where $m_{i,j}$ stands for the (i,j)th entry of M. □

Claim 7.2.11 implies that the theorem reformulates into: (a) $\delta_r \leq \delta_0$, and (b) the equality holds if, and only if, $\mathcal{I}_r$ is in general Noether position.

It is a classical fact that the primes associated to $\mathcal{I}'_i$ correspond to the ones of $\mathcal{I}_i$ that properly extend to $\mathbb{A}'_y[x_1,\dots,x_n]$ (see [Eis95, Chapter 3, Theorem 3.10(d)], for instance). Let $\mathcal{P}$ be a prime associated to $\mathcal{I}_i$ such that its extension $\mathcal{P}'$ to $\mathbb{A}'_y[x_1,\dots,x_n]$ is proper. Since $y_1,\dots,y_r$ are algebraically independent modulo $\mathcal{P}$, we can find a subset S of $\{x_1,\dots,x_n\}$ of cardinality $r-i$ such that $y_1,\dots,y_r$ and the elements of S are algebraically independent modulo $\mathcal{P}$ by [Lan02, Chapter VIII, Section 1, Theorem 1.1]. The elements of S are algebraically independent over $\mathbb{A}'_y$ modulo $\mathcal{P}'$, and that the variables outside of S are algebraic over $\mathbb{A}'_y(S)$ modulo $\mathcal{P}'$. It follows that $\dim(\mathcal{P}') = r - i$ hence that $\mathcal{I}'_i$ is unmixed of dimension either $r-i$ or -1. But since we have assumed that $\mathcal{I}'_M \neq (1)$, we have that $\mathcal{I}'_r \neq (1)$, whence $\dim(\mathcal{I}'_i) = r - i$ for all $i \in \{1,\dots,r\}$. This way, we obtain from Proposition 5.1.2(a) that l_{i+1} is a nonzerodivisor in $\mathbb{B}'_i$.

Claim 7.2.12. *Without loss of generality, we can assume that $\mathcal{I}'_i$ is in general Noether position, for all $i \in \{0,\dots,r\}$.*

Proof. We are going to exhibit a $\mathbb{K}$-linear change of the variables that preserves δ, and the general Noether position of $\mathcal{I}$. Of course the general Noether position of $\mathcal{I}$ implies the one

of $\mathcal{I}'_0$. Since l_{i+1} is a nonzerodivisor in $\mathbb{B}'_i$, we can use Proposition 5.1.2(b) successively with $f = l_1, \ldots, f = l_r$ in order to construct a matrix

$$M' = \begin{pmatrix} M'_{1,1} & 0 \\ 0 & \mathrm{Id}_{n-r} \end{pmatrix}$$

such that $\mathcal{I}'_i \circ M'$ is in general Noether position for all $i \in \{1, \ldots, r\}$. For each $i \in \{1, \ldots, r\}$, we let

$$l'_i = y_i - (\omega'_{i,1}x_1 + \cdots + \omega'_{i,n}x_n) \in \mathbb{A}[y_1, \ldots, y_r, x_1, \ldots, x_n],$$

where $\omega'_{i,j}$ stands here for the (i,j)th entry of $M^{-1}M'$. By construction we have that $\mathcal{I} \circ M' + (l'_1, \ldots, l'_i) = \mathcal{I}_i \circ M'$ to $\mathbb{A}'_y[x_1, \ldots, x_n]$, so that Claim 7.2.10 allows us to replace $\mathcal{I}$ by $\mathcal{I} \circ M'$ and M by $M'^{-1}M$ from the outset in the theorem. □

In order to prove that $\delta_r \leq \delta_0$, we prove the following stronger statement:

Claim 7.2.13. *For all $i \in \{0, \ldots, r-1\}$, we have that $\delta_{i+1} \leq \delta_i$.*

Proof. Proposition 5.3.1 applied with $\mathcal{I}'_i$ gives us that δ_{i+1} equals to the degree in x_{r-i} of the constant coefficient of the characteristic polynomial of l_{i+1} modulo $\mathcal{I}'_i$. The conclusion thus follows from Theorem 4.2.1(b). □

The proof of part (a) is now completed. If $\mathcal{I}_M$ is in general Noether position, then part (a) applied with $\mathcal{I}_M$ and M^{-1} yields $\delta \leq \delta_M$, whence $\delta = \delta_M$. Conversely, if the latter equality holds then we have to prove that $\mathcal{I}_r$ is in general Noether position in order to complete the proof of part (b), and thus the proof of the theorem. To this aim, we are to show the following stronger statement:

Claim 7.2.14. *If $\delta = \delta_M$ then $\mathcal{I}_i$ is in general Noether position, for all $i \in \{0, \ldots, r-1\}$.*

Proof. The general Noether position of $\mathcal{I}$ implies the one of $\mathcal{I}_0$. By induction, assume that $\mathcal{I}_i$ is in general Noether position for some $i \geq 0$. We can use Proposition 5.3.1 with $\mathcal{I}_i$ and l_{i+1}. Since Claim 7.2.13 implies that $\delta_{i+1} = \delta_i$, we deduce that the constant coefficient χ_0 of the characteristic polynomial of l_{i+1} in $\mathbb{B}''_i$ has degree δ_i in x_{r-i}. Since Theorem 4.2.1(b) implies that $\deg(\chi_0) \leq \delta_i$, we deduce from Lemma 5.1.1(a) that x_{r-i} is generally integral over $\mathbb{K}[y_1, \ldots, y_r, x_1, \ldots, x_{r-i-1}]$ modulo $\mathcal{I}_{i+1}$. By Proposition 2.3.5(b) we finally get that $\mathcal{I}_{i+1}$ is in general Noether position. □

Part III

Computation of the Primary Decomposition: Local Solving

The Kronecker solver presented in Part II computes the roots of any zero-dimensional ideal $(g_1, \ldots, g_n) : g^\infty$ together with their multiplicities. In Part III, we design an algorithm that further computes the local algebra of each root. For this purpose, we act on the last step of the Kronecker solver, and develop a local intersection procedure for a curve and an hypersurface that comes from the basis produced in the proof of Proposition 5.3.1.

Proposition 7.1.6 in Chapter 7 ensures that after replacing the equations $g_1, \ldots, g_n$ with random linear combinations $f_1, \ldots, f_n$ of $g_1, \ldots, g_n$, one can safely assume that $f_1, \ldots, f_n$ is a reduced regular sequence in the complementary $\{g \neq 0\}$ of the set of zeros of g. In particular, this implies that $(f_1, \ldots, f_{n-1}) : g^\infty$ is a radical ideal whose associated primes all have dimension one by Proposition 7.1.1. After performing a random affine change of variables in the input system, the Kronecker solver can compute the univariate representation with multiplicities

$$\chi, Q, V_1, V_2, \ldots, V_n$$

in x_1 of the ideal $(f_1, \ldots, f_n) : g^\infty$ (see Definition 4.3.6). In order to complete the primary decomposition of $(f_1, \ldots, f_n) : g^\infty$, we have to compute all the local algebras of the multiple roots. In Chapters 9 and 10, we assume that the origin is a multiple root of $(f_1, \ldots, f_n) : g^\infty$, whose multiplicity μ_0 can be read off from χ. We focus on the computation of

$$\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, \ldots, x_n]]/(f_1, \ldots, f_n) : g^\infty.$$

In Section 10.3, we come back to the general situation by using *dynamic evaluation* in $\mathbb{K}[T]/(Q)$.

The solver presented in Part II computes the ideals $(f_1, \ldots, f_i) : g^\infty$ in sequence. Here we act on the last intersection step, that is, we deal with the ideal

$$\mathcal{I} = (f_1, \ldots, f_{n-1}) : g^\infty.$$

Thanks to the affine change of variables, we can assume that $\mathcal{I}$ is in Noether position by Proposition 7.1.4; the quotient $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is then a free $\mathbb{K}[x_1]$-module of finite type by Proposition 4.1.1. By localizing and completing $\mathbb{B}$ in x_1, we obtain a free $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$, for which the isomorphism of algebras

$$\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f_n) \simeq \mathbb{D}_0$$

holds; in short we refer to $\mathbb{B}_0$ as *the module of the curve germ* (see Section 9.1 for a precise definition).

The Kronecker solver computes the Kronecker representation $q, w_3, \ldots, w_n$ in x_2 of the ideal $\mathcal{I}$. In Chapter 9, we design an algorithm that computes $\mathbb{B}_0$ from $q, w_3, \ldots, w_n$. In Section 9.1, we prove that $\mathbb{B}_0$ is a submodule of the $\mathbb{K}[[x_1]]$-module

$$\mathbb{L}_0 = \mathbb{K}[[x_1]]\frac{1}{x_1^{m_0}} \oplus \mathbb{K}[[x_1]]\frac{x_2}{x_1^{m_0}} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{\delta_0-1}}{x_1^{m_0}}$$

for suitable integers δ_0 and m_0 that are related to q. This allows us to perform all the computations in the canonical basis of $\mathbb{L}_0$; for instance, the inclusion $(\partial q/\partial x_2)x_j - w_j \in \mathcal{I}$ in Corollary 4.3.11(b) permits us to identify the variable x_j to an element of $\mathbb{L}_0$ for all $j \in \{3, \ldots, n\}$.

On the other hand, Corollary 4.3.11(b) again gives the equality $\mathcal{I} \cap \mathbb{K}[x_1, x_2] = (q)$, which implies that $\mathbb{B}_0$ contains the $\mathbb{K}[[x_1]]$-module

$$\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \mathbb{K}[[x_1]]x_2 \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0 - 1}.$$

In Section 9.3, we compute a basis of the $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$ by using the fact that $\mathbb{B}_0$ is the smallest algebra that contains $\mathbb{M}_0$ and $x_3, \ldots, x_n$.

The isomorphism $\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f_n) \simeq \mathbb{D}_0$ implies that any basis of the cokernel of the morphism of multiplication by f_n in $\mathbb{B}_0$ is a basis of $\mathbb{D}_0$. We explain in Section 10.1 of Chapter 10 how we can deduce such a basis from a Smith form computation. In Section 10.2, we use a similar idea to extend the whole algorithm to overdetermined systems, that is, to the case when the number of equations is greater than the number of variables. Finally, we summarize in Section 10.3 the whole algorithm to compute the primary decomposition of any zero-dimensional ideal.

In Chapters 9 and 10, we deal with formal power series in x_1, so that we have to study the precision needed for the exactness of the computation. In Section 8.2, we use Hermite normal forms to define a basis $\varepsilon_1, \ldots, \varepsilon_{\delta_0}$ of any submodule of $\mathbb{L}_0$ with rank δ_0, such that the coordinates of ε_ℓ in the canonical basis of $\mathbb{L}_0$ are polynomials. We then give an algorithm for adding a vector to a submodule of $\mathbb{L}_0$ given by such a basis; this allows the exact computation of $\mathbb{B}_0$ in Section 9.3. Chapter 8 also contains an algorithm for the computation of the Smith normal form with multipliers that is needed in Section 10.1.

In Part II, we did not reproduce the cost analysis of the Kronecker solver from [GLS01]. In this section, we detail the cost of the algorithms, which yields to the main result in Theorem 10.3.4. At last, we do not need any other hypotheses than the one enclosed in Propositions 7.1.4 and 7.1.6: our computations do not modify the probability of error of the Kronecker solver.

Chapter 8

Normal Forms of Matrices with entries in a Formal Power Series Ring

In Chapters 9 and 10, we will need algorithms to compute normal forms of matrices with entries in a formal power series ring $\mathbb{K}[[t]]$ in one variable over $\mathbb{K}$. Though this question has been studied by many authors for matrices with entries in a polynomial ring, there is no reference for the case of formal power series. We develop in this chapter suitable algorithms for our next chapters, together with their cost analysis in terms of arithmetic operations in $\mathbb{K}$. This chapter can be read apart from the rest of the thesis.

8.1 Hermite Normal Form and Truncation

For any ring R, we let $(\mathrm{R})_{r\times s}$ denote the algebra of matrices with r rows, s columns and entries in R. We let $M_{k,\ell}$, respectively $M_{.,\ell}$, denote the (k,ℓ)-th entry, respectively the ℓ-th column, of the element M of $(\mathrm{R})_{r\times s}$. Afterwards, R will be replaced with the principal rings $\mathbb{K}[[t]]$ or $\mathbb{K}[t]$. *From now on we restrict ourself to matrices with full row rank*, that is of rank r; this implies that s is at least r. We begin with giving the definition of the Hermite normal form of a matrix $M \in (\mathbb{K}[[t]])_{r\times s}$ of full row rank, whose existence and uniqueness can be easily deduced from Lemma 8.1.2 since $\mathbb{K}[[t]]$ is a principal ideal domain (see also [Sto94, Chapter 2, Theorem 1]).

Definition 8.1.1. Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a matrix of full row rank. We say that M is *in Hermite normal form* if for all $(k,\ell) \in \{1,\ldots,r\}\times\{1,\ldots,s\}$,

- if $k < \ell$, then $M_{k,\ell} = 0$;
- there exists an integer ν_k such that $M_{k,k} = t^{\nu_k}$;
- if $k > \ell$, $M_{k,\ell}$ belongs to $\mathbb{K}[t]$ and has degree at most $\nu_k - 1$.

We say that $H \in (\mathbb{K}[[t]])_{r\times s}$ is *the Hermite normal form of* M if H is in Hermite normal form and if there exists a unit P of $(\mathbb{K}[[t]])_{s\times s}$ such that $MP = H$.

In other words, the Hermite normal form H of a matrix M is a lower triangulation obtained by elementary column operations:

$$H = \begin{pmatrix} t^{\nu_1} & 0 & \cdots & 0 & 0 \\ H_{2,1} & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ H_{r,1} & \cdots & H_{r,r-1} & t^{\nu_r} & 0 \end{pmatrix}.$$

The following property of the Hermite normal form H of a matrix M characterizes the diagonal elements of H.

Lemma 8.1.2. *Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a full row rank matrix, and H be its Hermite normal form. Let $e_1, \ldots, e_r$ be the canonical basis of the free $\mathbb{K}[[t]]$-module $\mathcal{L} = \mathbb{K}[[t]]^r$, and let $\mathrm{Im}(M)$ denote the submodule of $\mathcal{L}$ generated by the columns of M. For all $k \in \{1, \ldots, r\}$, t^{ν_k} generates the ideal of $\mathbb{K}[[t]]$ made up of the k-th coordinates of the elements of $\mathrm{Im}(M) \cap (\mathbb{K}[[t]]e_k \oplus \cdots \oplus \mathbb{K}[[t]]e_r)$.*

Proof. Since the matrix P in Definition 8.1.1 is a unit of $(\mathbb{K}[[t]])_{s\times s}$, the columns of the matrices M and H generate the same submodule of $\mathcal{L}$, which proves the lemma. □

Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a matrix of full row rank, and $H = MP$ be its Hermite normal form. Whereas the entries of H are polynomial, those of M and P belong to $\mathbb{K}[[t]]$, so that to compute the Hermite normal form of M, we have to compute in $\mathbb{K}[[t]]/(t^\eta)$ for a suitable integer η. The precision η necessary to ensure the exactness of the computations has to be at least the maximal degree of the entries of H, that is $\nu = \max(\nu_k, k \in \{1, \ldots, r\})$. Our next proposition asserts that the precision $\nu + 1$ is sufficient to compute the Hermite normal form of M. For any integer $\eta \in \mathbb{N}$ and matrices $M, M' \in (\mathbb{K}[[t]])_{r\times s}$, we write $M \equiv M' \mod t^\eta$ if the valuations of all the entries of $M - M'$ are at least η.

Proposition 8.1.3. *Let M be an element of $(\mathbb{K}[[t]])_{r\times s}$ of full row rank, and let $H = MP$ be the Hermite normal form of M. Let ν be the maximal valuation of the diagonal entries of H. Let $H' \in (\mathbb{K}[[t]])_{r\times s}$ be in Hermite normal form, and let P' be a unit of $(\mathbb{K}[[t]])_{s\times s}$ such that $MP' \equiv H' \mod t^{\nu+1}$. Then $H' = H$.*

Proof. With the notation of Lemma 8.1.2, let $\mathrm{Im}(H)$ and $\mathrm{Im}(H')$ denote the submodules of $\mathcal{L} = \mathbb{K}[[t]]^r$ generated by the columns of H and H' respectively. Since $\mathrm{Im}(M)$ equals $\mathrm{Im}(H)$ and since P' is a unit of $(\mathbb{K}[[t]])_{s\times s}$, the following inclusions hold:

$$\begin{array}{ll} (I_1) & \mathrm{Im}(H') \subseteq \mathrm{Im}(H) + t^{\nu+1}\mathcal{L}, \\ (I_2) & \mathrm{Im}(H) \subseteq \mathrm{Im}(H') + t^{\nu+1}\mathcal{L}. \end{array}$$

Using the shape of H', inclusion (I_1) and Lemma 8.1.2, we obtain that $H'_{1,1} = t^{\nu'_1}$ belong to the ideal generated by $H_{1,1} = t^{\nu_1}$ and $t^{\nu+1}$, so that $\nu'_1 \geq \min(\nu_1, \nu + 1)$, that is $\nu'_1 \geq \nu_1$. By symmetry, we obtain $\nu_1 \geq \min(\nu'_1, \nu + 1)$, so that $\nu'_1 = \nu_1$: the first rows of H and H' coincide.

By induction, let us assume that the $(k-1)$ first rows of H and H' coincide for some integer $k \in \{2, \ldots, r\}$. First we prove that $H_{k,k} = H'_{k,k}$, that is $\nu_k = \nu'_k$ with ν'_k being the valuation

of $H'_{k,k}$. Let us recall that $H'_{.,k}$ denotes the k-th column of H'. By (I_1), there exists a vector $V \in \mathcal{L}$ such that $H'_{.,k} - t^{\nu+1}V \in \mathrm{Im}(H)$. The $(k-1)$ first coordinates of $H'_{.,k}$ are zero. Since $\nu + 1 > \nu_i$ for all $i \in \{1, \ldots, k-1\}$, one can assume that the $(k-1)$ first coordinates of V are zero, even if it means adding a linear combination of $H_{.,1}, \ldots, H_{.,k-1}$ to $H'_{.,k} - t^{\nu+1}V$. Then the k-th coordinate $t^{\nu'_k} - t^{\nu+1}V_k$ of $H'_{.,k} - t^{\nu+1}V$ belong to (t^{ν_k}) by Lemma 8.1.2, so that $\nu'_k \geq \nu_k$. By symmetry, $\nu_k = \nu'_k$.

Finally, it remains to prove that $H_{k,\ell} = H'_{k,\ell}$ for all $\ell < k$. Same arguments as before with the difference of the ℓ-th columns $H_{.,\ell} - H'_{.,\ell} \in \mathrm{Im}(H) + t^{\nu+1}\mathcal{L}$ lead to $H_{k,\ell} - H'_{k,\ell} - t^{\nu+1}W_k \in (t^{\nu_k})$ for some $W_k \in \mathbb{K}[[t]]$. Then $H_{k,\ell} - H'_{k,\ell}$ belong to (t^{ν_k}) since $\nu \geq \nu_k$ and therefore $H_{k,\ell} = H'_{k,\ell}$ since both $H_{k,\ell}$ and $H'_{k,\ell}$ are polynomials of degree strictly less than ν_k. □

8.2 Algorithm for a Module-Vector Sum

We now give an application of Hermite normal forms that will be intensively used in Algorithm 11 of Section 9.3. Let $m \in \mathbb{N}$, $\delta \in \mathbb{N}$, and let $\mathbb{L}$ denote the free $\mathbb{K}[[t]]$-module $(\frac{1}{t^m}\mathbb{K}[[t]])^\delta$. Let $\mathbb{M}$ be a submodule of $\mathbb{L}$ of rank δ. We use Hermite normal forms to define a basis of $\mathbb{M}$ whose coordinates in the canonical basis of $\mathbb{L}$ belong to $\mathbb{K}[t]$.

Definition 8.2.1. Let $\mathbb{M}$ be a submodule of $\mathbb{L}$ of rank δ. A basis $\varepsilon_1, \ldots, \varepsilon_\delta$ is said *normal lower triangular basis of* $\mathbb{M}$ if the matrix of $(\mathbb{K}[[t]])_{\delta\times\delta}$ whose ℓ-th column is the coordinate vector of ε_ℓ in the canonical basis of $\mathbb{L}$ is in Hermite normal form.

Example 8.2.2. Let $\delta = 2$ and $m = 3$. The vectors whose coordinates are $(t^3, 0)$ and $(0, t^3)$ in the canonical basis of $\mathbb{L} = (\frac{1}{t^3}\mathbb{K}[[t]])^2$ form a normal lower triangular basis of the module $\mathbb{M} = (\mathbb{K}[[t]])^2$. The module $\mathbb{K}[[t]] \oplus \frac{1}{t}\mathbb{K}[[t]]$ admits $(t^3, 0)$ and $(0, t^2)$ for normal lower triangular basis.

We are to prove that any module $\mathbb{M}$ of rank δ admits a unique normal lower triangular basis; this gives a way to test the equality between two modules. Moreover, under some hypotheses, we can control the degree of the coordinates of the elements of the basis; this will be precious for the cost analysis of our algorithms.

Lemma 8.2.3. *Let $\mathbb{M}$ be a submodule of $\mathbb{L}$ of rank δ. Then there exists a unique normal lower triangular basis $\varepsilon_1, \ldots, \varepsilon_\delta$ of $\mathbb{M}$. For $\ell \in \{1, \ldots, \delta\}$, the coordinates of ε_ℓ in the canonical basis of $\mathbb{L}$ belong to $\mathbb{K}[t]$. In addition, if $\mathbb{M}$ contains the $\mathbb{K}[[t]]$-module $(\mathbb{K}[[t]])^\delta$, then the coordinates of ε_ℓ are of degree at most m.*

Proof. Let $e_1, \ldots, e_\delta$ be any basis of $\mathbb{M}$, and let M be the matrix of $(\mathbb{K}[[t]])_{\delta\times\delta}$ whose ℓ-th column is the vector of the coordinates of e_ℓ in the canonical basis of $\mathbb{L}$. Let H be the Hermite normal form of M. Existence and uniqueness of the normal lower triangular basis $\varepsilon_1, \ldots, \varepsilon_\delta$ of $\mathbb{M}$ straightforward follow from those of H; the coordinates of ε_ℓ in the canonical basis of $\mathbb{L}$ belong to $\mathbb{K}[t]$ by Definition 8.1.1. Now, if $\mathbb{M}$ contains $(\mathbb{K}[[t]])^\delta$, the element of $\mathbb{L}$ whose only non-zero coordinate is the k-th one and equals t^m belong to $\mathbb{M}$ for all $k \in \{1, \ldots, \delta\}$. Then the valuation ν_k of the k-th diagonal entry of H is at most m by Lemma 8.1.2, and all the entries of H have their degree bounded by m. □

Let $\varepsilon_1, \ldots, \varepsilon_\delta$ be the normal lower triangular basis of $\mathbb{M}$, and let v be an element of $\mathbb{L}$. We are interested in computing the normal lower triangular basis of the module $\mathbb{M} + \mathbb{K}[[t]]v$. Let M be the matrix of $(\mathbb{K}[[t]])_{\delta\times(\delta+1)}$ whose ℓ-th column is the vector of coordinates of ε_ℓ in the canonical basis of $\mathbb{L}$ for $\ell \in \{1, \ldots, \delta\}$, and whose $(\delta+1)$-th column is the coordinate vector of v; the shape of M is

$$M = \begin{pmatrix} t^{\nu_1} & 0 & \cdots & 0 & v_1 \\ M_{2,1} & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ M_{\delta,1} & \cdots & M_{\delta,\delta-1} & t^{\nu_\delta} & v_\delta \end{pmatrix}. \tag{8.2.1}$$

The normal lower triangular basis of $\mathbb{M} + \mathbb{K}[[t]]v$ is given by the Hermite normal form H of M. To compute H, we have to truncate the coordinates of v. If $\mathbb{M}$ contains the free module $(\mathbb{K}[[t]])^\delta$, Proposition 8.1.3 and Lemma 8.2.3 allow us to compute with precision $m+1$ as in the following algorithm. For $a, b \in \mathbb{K}[[t]]$, we let $\mathrm{quo}(a, b)$ denote the quotient of a divided by b.

Algorithm 8. *Module-Vector Sum*

Input: The normal lower triangular basis $\varepsilon_1, \ldots, \varepsilon_\delta$ of a submodule $\mathbb{M}$ of $\mathbb{L} = (\frac{1}{t^m}\mathbb{K}[[t]])^\delta$ that contains $(\mathbb{K}[[t]])^\delta$, and the coordinates of an element v of $\mathbb{L}$ to precision $m+1$.

Output: The normal lower triangular basis of $\mathbb{M} + \mathbb{K}[[t]]v$.

1. Initialize $\overline{M}$ with the matrix M defined in (8.2.1) to precision $m+1$.
2. Initialize aux with 0.
3. For k from 1 to δ, do
   a. if the valuation of $\overline{M}_{k,\delta+1}$ is greater than the one of $\overline{M}_{k,k}$, then replace $\overline{M}_{.,\delta+1}$ with $\overline{M}_{.,\delta+1} - \mathrm{quo}(\overline{M}_{k,\delta+1}, \overline{M}_{k,k})\overline{M}_{.,k}$; else
      i. replace aux with 1;
      ii. exchange $\overline{M}_{.,k}$ and $\overline{M}_{.,\delta+1}$;
      iii. multiply $\overline{M}_{.,k}$ by $(t^{-\mathrm{val}(\overline{M}_{k,k})}\overline{M}_{k,k})^{-1}$;
      iv. replace $\overline{M}_{.,\delta+1}$ with $\overline{M}_{.,\delta+1} - \mathrm{quo}(\overline{M}_{k,\delta+1}, \overline{M}_{k,k})\overline{M}_{.,k}$.
4. If $aux = 1$, then for ℓ from 1 to $\delta - 1$ and for k from $\ell + 1$ to δ, replace $\overline{M}_{.,\ell}$ with $\overline{M}_{.,\ell} - \mathrm{quo}(\overline{M}_{k,\ell}, \overline{M}_{k,k})\overline{M}_{.,k}$.
5. Return the δ first columns of $\overline{M}$.

Proposition 8.2.4. *Algorithm 8 works correctly as specified with $\tilde{\mathcal{O}}(\delta^2)$ arithmetic operations in $\mathbb{K}[[t]]/(t^{m+1})$ if $v \in \mathbb{M}$, and $\tilde{\mathcal{O}}(\delta^3)$ operations otherwise. It thus costs $\tilde{\mathcal{O}}(m\delta^2)$ operations in $\mathbb{K}$ if $v \in \mathbb{M}$, and $\tilde{\mathcal{O}}(m\delta^3)$ otherwise.*

Proof. Algorithm 8 computes the Hermite normal form of the matrix M defined in (8.2.1) by vanishing recursively the entries of its last column. To be more precise, at the beginning of the k-th crossing through the loop of step 3, the shape of the matrix $\overline{M}$ is

$$\overline{M} = \begin{pmatrix} t^{\nu_1} & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ \overline{M}_{2,1} & \ddots & \ddots & & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots & 0 \\ \vdots & & \ddots & t^{\nu_k} & \ddots & \vdots & \overline{M}_{k,\delta+1} \\ \vdots & & & \ddots & \ddots & 0 & \vdots \\ \overline{M}_{\delta,1} & \cdots & \cdots & \cdots & \overline{M}_{\delta,\delta-1} & t^{\nu_\delta} & \overline{M}_{\delta,\delta+1} \end{pmatrix}.$$

Step 3.a vanishes $\overline{M}_{k,\delta+1}$ by elementary operations on $\overline{M}_{.,k}$ and $\overline{M}_{.,\delta+1}$. If the valuation of $\overline{M}_{k,\delta+1}$ is greater than ν_k, the k-th column of $\overline{M}$ remains the k-th column of M. Thus if $aux = 0$ at step 4 the δ first columns of $\overline{M}$ are the ones of the input matrix M, and $\overline{M}$ is in normal form. In this case, $\mathbb{M} + \mathbb{K}[[t]]v = \mathbb{M}$ since they have the same normal lower triangular basis. Otherwise we have to reduce the lower entries of $\overline{M}$, that is done in step 4.

Lemma 8.2.3 and Proposition 8.1.3 ensure that the computation can be done to precision $m+1$. Step 3.a costs $\mathcal{O}(\delta)$ operations in $\mathbb{K}[[t]]/(t^{m+1})$. Then step 3 costs $\mathcal{O}(\delta^2)$ operations in $\mathbb{K}[[t]]/(t^{m+1})$. If $v \notin \mathbb{M}$, the reducing step 4 cost $\mathcal{O}(\delta^3)$ operations, which ends the proof of the proposition. □

Example 8.2.5. Let $\delta = 2$ and $m = 3$, let $\mathbb{M} = \mathbb{K}[[t]]^2$, and let $(0, -t^2/4 + 3t^3/4)$ be the truncated coordinates of a vector v to precision 7. Then the vectors of the normal triangular basis of $\mathbb{M} + \mathbb{K}[[t]]v$ have coordinates $(t^3, 0)$ and $(0, t^2)$ in $\mathbb{L}$. We thus have $\mathbb{M} + \mathbb{K}[[t]]v = \mathbb{K}[[t]] \oplus \frac{1}{t}\mathbb{K}[[t]]$.

Remark 8.2.6. Algorithm 8 computes the Hermite normal form of matrices with a particular shape. Algorithms for the calculation of Hermite normal forms were first studied for matrices with entries in the integer ring (see [Coh93, Section 2.4]). In the polynomial case, the main difficulty is the growth of the degrees of the intermediate expressions. The first algorithm with polynomial bound on this intermediate degrees was given in [Kan85]. We refer to [Vil95] for an overview of the classical algorithms in the polynomial case; more recently, the algorithm of [MS03] is based on reduction of lattices. In the case of formal power series ring, we work with truncated series, hence the question of the growth of intermediate expression disappears. The second difficulty in the polynomial case is the computation of gcds, which is just a comparison between valuations when in $\mathbb{K}[[t]]$.

8.3 Smith Form

Hermite forms are triangularizations obtained by elementary operations on the columns; Smith forms are diagonalizations obtained by elementary operations on both the rows and the columns. For our Algorithm 12 in Section 10.1, we need to compute the Smith normal form S of a matrix M with entries in $\mathbb{K}[[t]]$ together with multipliers, that are two invertible matrices U, V such that $UMV = S$. The algorithms of [KKS90, Vil94, Vil95] solve this problem for the case of matrices in a polynomial ring. In this section, we give an algorithm inspired by [Vil95], that

computes the Smith normal form of a matrix with entries in $\mathbb{K}[[t]]$, together with some pre- and post-multipliers to a fixed precision. We recall below the definition of the Smith normal form of a matrix with entries in $\mathbb{K}[[t]]$. For the existence of the Smith normal form of a given matrix of $(\mathbb{K}[[t]])_{r\times s}$, we refer the reader to [Lan02, Theorem 7.9]; uniqueness follows from Lemma 8.3.2.

Definition 8.3.1. Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a matrix of rank ρ. We say that M is *in Smith normal form* if, for all $(k,\ell) \in \{1,\dots,r\} \times \{1,\dots,s\}$,

- if $k \neq \ell$, $M_{k,\ell} = 0$;
- there exists some integers $\nu_1 \leq \cdots \leq \nu_\rho$ such that $M_{k,k} = t^{\nu_k}$ for $k \in \{1,\dots,\rho\}$;
- if $\rho < \min(r,s)$, then $M_{k,k} = 0$ for all $k > \rho$.

We say that $S \in (\mathbb{K}[[t]])_{r\times s}$ is *the Smith normal form of* M if S is in Smith normal form and if there exist two units U of $(\mathbb{K}[[t]])_{r\times r}$ and V of $(\mathbb{K}[[t]])_{s\times s}$ such that $UMV = S$; the matrices U and V, that are not unique, are called *pre-* and *post-multipliers* respectively.

Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a matrix of rank ρ. For $k \in \{1,\dots,\rho\}$, we define the *determinant ideal* $I_k(M)$ *of* M as the ideal of $\mathbb{K}[[t]]$ generated by all the $k \times k$ minors of M. We then write $\nu_k(M)$ *for the common valuation of all the generators of the ideal* $I_k(M)$.

Lemma 8.3.2. *Let $M \in (\mathbb{K}[[t]])_{r\times s}$ be a matrix of rank ρ, and let $\nu_1,\dots,\nu_\rho$ denote the valuations of the diagonal entries of the Smith normal form S of M. Then for all $k \in \{1,\dots,\rho\}$, we have $\nu_k(M) = \nu_1 + \cdots + \nu_k$.*

Proof. The lemma straightforward follows from the equality $I_k(M) = I_k(S)$ (see [Lan02, Chapter 19, Section 2, Inclusion (1)]). □

Lemma 8.3.2 intrinsically characterizes the diagonal entries of the Smith normal form, which can be deduced from gcd computations. The difficulty is indeed the computation of pre- or post-multipliers. In [Vil95], Algorithm $F[x]$-TNSF calculates some multipliers for matrices in $(\mathbb{K}[t])_{r\times s}$ by computing a lower triangulation $T = NP$, where P is a unit of $(K[[t]])_{s\times s}$, of some preconditioned matrix $N = CM$ verifying that the diagonal of T is the diagonal of the Smith normal form S of M. The matrix P is then a post-multiplier, and one easily deduce from T and C the Smith normal form of M and a pre-multiplier by "cleaning" the lower elements of T by rows operations. Such a matrix T is called a *triangular Smith form*.

We adapt this strategy for a matrix $M \in (\mathbb{K}[[t]])_{r\times s}$. The following algorithm computes a triangular Smith form of the matrix M by computing recursively some units C_k of $(\{0,1\})_{r\times r}$ and P_k of $(\mathbb{K}[[t]])_{s\times s}$ such that the shape of C_kMP_k is

$$T_k = \begin{pmatrix} t^{\nu_1} & 0 & \cdots & \cdots & \cdots & 0 \\ * & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & t^{\nu_k} & 0 & \cdots & 0 \\ \vdots & & * & & & \\ \vdots & & \vdots & & \bar{M}_{k+1} & \\ * & \cdots & * & & & \end{pmatrix}, \tag{8.3.1}$$

where $t^{\nu_1}, \ldots, t^{\nu_k}$ are the k-th first diagonal entries of the Smith normal form of M. Here again, we let $\mathrm{quo}(a, b)$ denote the quotient of a divided by b in $\mathbb{K}[[t]]$.

Algorithm 9. *Triangular Smith Form*

Input: A matrix M of $(\mathbb{K}[[t]])_{r\times s}$ of rank ρ to precision $\eta \geq \nu_\rho(M) + 1$.

Output: Some matrices $T \in (\mathbb{K}[t])_{r\times s}$, $C \in (\{0,1\})_{r\times r}$ and $P \in (\mathbb{K}[t])_{s\times s}$ such that

- T is a lower triangular matrix whose diagonal entries are those of the Smith normal form of M,
- P and C are unit of $(\mathbb{K}[[t]])_{s\times s}$ and $(\mathbb{K}[[t]])_{r\times r}$ respectively,
- $CMP \equiv T \mod t^\eta$.

1. a. Initialize T with $M \mod t^\eta$.
   b. Initialize C with the $r \times r$ identity matrix.
   c. Initialize P with the $s \times s$ identity matrix.
2. For k from 1 to ρ, do
   a. find an index $(\tilde{\iota}, \tilde{\kappa}) \in \{k, \ldots, r\} \times \{k, \ldots, s\}$ such that
   $$\mathrm{val}(T_{\tilde{\iota},\tilde{\kappa}}) = \min(\mathrm{val}(T_{i,j}), k \leq i \leq r, k \leq j \leq s),$$
   with $\tilde{\iota}$ minimal for this property.
   b. i. if $\tilde{\iota} \neq k$,
      - replace $T_{k,\cdot}$ with $T_{k,\cdot} + T_{\tilde{\iota},\cdot}$,
      - replace $C_{k,\tilde{\iota}}$ with 1;

      ii. if $\tilde{\kappa} \neq k$,
      - exchange $T_{\cdot,k}$ and $T_{\cdot,\tilde{\kappa}}$;
      - exchange $P_{\cdot,k}$ and $P_{\cdot,\tilde{\kappa}}$;

      iii.
      - multiply $T_{\cdot,k}$ by $(t^{-\mathrm{val}(T_{k,k})}T_{k,k})^{-1}$;
      - multiply $P_{\cdot,k}$ by $(t^{-\mathrm{val}(T_{k,k})}T_{k,k})^{-1}$;

   c. for j from $k+1$ to s,
      - replace $T_{\cdot,j}$ with $T_{\cdot,j} - \mathrm{quo}(T_{k,j}, T_{k,k})T_{\cdot,k}$;
      - replace $P_{\cdot,j}$ with $P_{\cdot,j} - \mathrm{quo}(T_{k,j}, T_{k,k})P_{\cdot,k}$.
3. Return T, C, P.

Proposition 8.3.3. *Algorithm 9 works correctly as specified with $\tilde{\mathcal{O}}(\rho rs)$ arithmetic operations in $\mathbb{K}[[t]]/(t^\eta)$, hence with $\tilde{\mathcal{O}}(\rho rs\eta)$ arithmetic operations in $\mathbb{K}$.*

Proof. We prove by induction that the matrix T satisfies the properties of the matrix (8.3.1) at the issue of the k-th crossing through the for loop of step 2. Let $k \in \{1, \dots, \rho\}$, and assume that the property is true for $k-1$, that is, that we enter in the k-th loop with a matrix T of shape T_{k-1}. After steps 2.b.i and 2.b.ii, $T_{k,k}$ is the gcd of the elements of $((T_{i,j}))_{k \le i \le r, k \le j \le s}$; after step 2.b.iii, this gcd is monic, that is, it is a power of t. Step 2.c vanishes the $(s-k)$ last entries of the $T_{k,.}$; thus T has shape (8.3.1). By Lemma 8.3.2, $T_{k,k}$ is the k-th diagonal entry of S since $I_k(T') = I_k(M)$. Lastly, the output T, C, P of Algorithm 9 is such that $T \equiv CMP \mod t^\eta$ by construction, which ends the proof of correctness. The proposition follows from the fact that step 2 performs $\mathcal{O}(\rho r s)$ operations in $\mathbb{K}[[t]]/(t^\eta)$. □

Algorithm 10 achieves the computation of the Smith normal form by cleaning the lower elements of T.

Algorithm 10. *Smith Normal Form*

Input: A matrix M of $(\mathbb{K}[[t]])_{r \times s}$ of rank ρ to precision $\eta \ge \nu_\rho(M) + 1$.

Output: Some matrices $S \in (\mathbb{K}[t])_{r \times s}$, $Q \in (\mathbb{K}[t])_{r \times r}$ and $P \in (\mathbb{K}[t])_{s \times s}$ such that

- S is the Smith normal form of M,
- P and Q are units of $(\mathbb{K}[[t]])_{s \times s}$ and $(\mathbb{K}[[t]])_{r \times r}$ respectively,
- $QMP \equiv S \mod t^\eta$.

1. a. Let T, C, P be the output of Algorithm 9 applied to M to precision η.
   b. Initialize Q with C and S with T.
2. For ℓ from 2 to r, for k from 1 to $\min(\ell - 1, \rho)$,
   a. replace $S_{\ell,.}$ with $S_{\ell,.} - \mathrm{quo}(S_{\ell,k}, S_{k,k}) S_{k,.}$,
   b. replace $Q_{\ell,.}$ by $Q_{\ell,.} - \mathrm{quo}(S_{\ell,k}, S_{k,k}) Q_{k,.}$;
3. Return S, Q, P.

Proposition 8.3.4. *Algorithm 10 works correctly as specified with $\tilde{\mathcal{O}}(\rho r s)$ arithmetic operations in $\mathbb{K}[[t]]/(t^\eta)$, and hence $\tilde{\mathcal{O}}(\rho r s \eta)$ arithmetic operations in $\mathbb{K}$.*

Proof. Since the rank of M is ρ, all the entries of $((T_{i,j}))_{\rho+1 \le i \le r, \rho+1 \le j \le s}$ are zero. By construction of T, for $k \in \{1, \dots, \rho\}$, the valuation of any entry of $T_{.,k}$ is at least ν_k. The correctness of Algorithm 10 is thus a consequence of Proposition 8.3.3. Step 1 costs $\tilde{\mathcal{O}}(\rho r s \eta)$ arithmetic operations in $\mathbb{K}$, and step 2 performs at most $\mathcal{O}(\rho r s)$ operations in $\mathbb{K}[[t]]/(t^\eta)$, which ends the proof. □

Chapter 9

Module of a Curve Germ

In this chapter, we come back to the computation of local algebras. As announced in the introduction of Part III, we act on the last intersection step of the Kronecker solver. We thus deal with a one-dimensional unmixed radical ideal $\mathcal{I}$ in general Noether position, given by its Kronecker representation $q, w_3, \ldots, w_n$ with respect to x_2. This ideal defines a curve which is assumed to pass through the origin. In a first section, we define a module of the curve germ at the origin. We then give some properties of this module and design an algorithm to compute it from the Kronecker representation of $\mathcal{I}$.

9.1 Curve Germ

Under the previous hypotheses on $\mathcal{I}$, Proposition 4.1.1 ensures that the $\mathbb{K}[x_1]$-module $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is torsion-free. Since $\mathbb{K}[x_1]$ is a principal ideal domain, $\mathbb{B}$ is thus a finitely generated free module by [Lan02, Chapter III, Theorem 7.3]. In order to focus on the information at the origin, we work with the extension $\mathcal{I}_0$ of $\mathcal{I}$ to $\mathbb{K}[[x_1]][x_2, \ldots, x_n]$. Moreover, if $q = \prod q_i$ is the factorization of q in $\mathbb{K}[[x_1]][x_2]$, we let q_0 be the product of all the q_i such that $q_i(0,0) = 0$; since q is monic in x_2, we can assume that q_0 is monic. We set

$$\mathcal{J}_0 = \mathcal{I}_0 + (q_0)$$

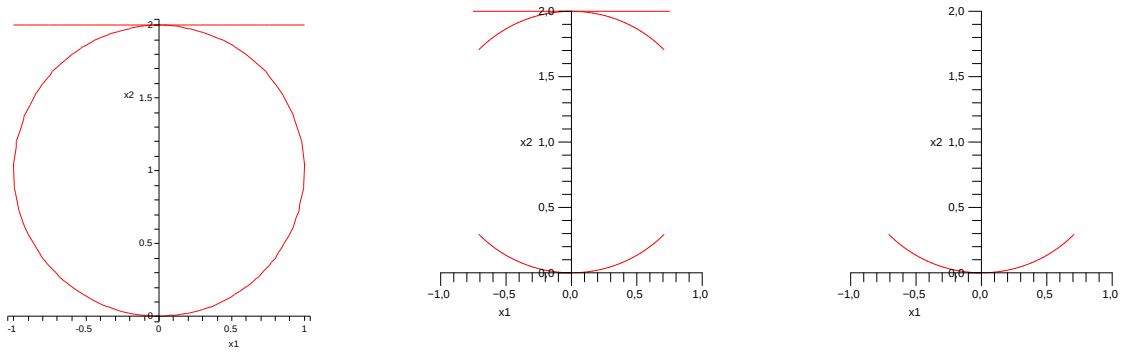
and

$$\mathbb{B}_0 = \mathbb{K}[[x_1]][x_2, \ldots, x_n]/\mathcal{J}_0.$$

Remark 9.1.1. By Proposition 7.1.4, we can assume that x_2 is a primitive element for $\sqrt{\mathcal{I} + (x_1)}$. The origin is thus the only point in $\mathcal{V}(\mathcal{I})$ with first coordinates $(x_1, x_2) = (0, 0)$. Then the ideals $\mathcal{I}$ and $\mathcal{J}_0$ extended to $\mathbb{K}[[x_1, \ldots, x_n]]$ coincide, and $\mathcal{J}_0$ describes the curve germ at the origin.

Example 9.1.2. Let $\mathbb{K}$ be the rational number field $\mathbb{Q}$, let $\mathcal{I}$ be the ideal of $\mathbb{Q}[x_1, x_2]$ generated by $q = (x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2)$. The curve defined by $\mathcal{I}$ is the union of a circle and a line (see Figure 9.1.3 below). The factorization of q in $\mathbb{Q}[[x_1]][x_2]$ is $q = (x_2 - 2)(x_2 - \sigma_1(x_1))(x_2 - \sigma_2(x_1))$, where $\sigma_1, \sigma_2 \in \mathbb{K}[[x_1]]$ are the roots of $x_2^2 + 2x_2 + x_1^2 = 0$ in $\mathbb{K}[[x_1]]$, with $\sigma_1(0) = 0$ and $\sigma_2(0) = -2$. By replacing q with $q_0 = x_2 - \sigma_1(x_1)$, we discard the line $x_2 = 2$ and we only keep the germ of the circle at the origin. Let us remark that the quotient $\bar{\mathbb{Q}}[[x_1]][x_2]/\mathcal{I}_0$ is a free $\mathbb{K}[[x_1]]$-module

Figure 9.1.3.



$\mathcal{V}(\mathcal{I})$ $\mathcal{V}(\mathcal{I}_0)$ $\mathcal{V}(\mathcal{J}_0)$

of dimension 3 whereas the dimension of $\mathbb{B}_0$ is one, which is the number of branches of the curve passing through the origin.

Our final purpose is the computation of the local algebra $\mathbb{D}_0$ of the origin as a root of $\mathcal{I}+(f)$ for some polynomial f that is a nonzerodivisor modulo $\mathcal{I}$. Following Proposition 9.1.4 justifies our interest in $\mathbb{B}_0$, and will give rise to the local intersection algorithm in Section 10.1:

Proposition 9.1.4. *Let f be nonzerodivisor modulo $\mathcal{I}$ such that x_1 is a primitive element for $\mathcal{I}+(f)$, and let $\mathbb{D}_0$ denote the local algebra of the origin as a root of $\mathcal{I}+(f)$. Then the $\bar{\mathbb{K}}$-algebra $\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f)$ is isomorphic to $\mathbb{D}_0$.*

Proof. Let $0, p^{(2)}, \ldots, p^{(r)}$ denote all the zeros of $\mathcal{I}+(f)$ in $\bar{\mathbb{K}}^n$, with respective local algebras $\mathbb{D}_0, \mathbb{D}_{p^{(2)}} \ldots, \mathbb{D}_{p^{(r)}}$. Since x_1 is primitive element for $\mathcal{I}+(f)$, the origin is the only root of $\mathcal{I}+(f)$ with first coordinate 0; the extensions of the ideals $\mathcal{I}+(f)$ and $\mathcal{J}_0+(f)$ to $\bar{\mathbb{K}}[[x_1, \ldots, x_n]]$ are thus equal. The proposition is then a consequence of the isomorphism of $\bar{\mathbb{K}}$-algebra

$$\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f) \simeq \mathbb{D}_0 \times \mathbb{D}_{p^{(2)}} \times \cdots \times \mathbb{D}_{p^{(r)}}$$

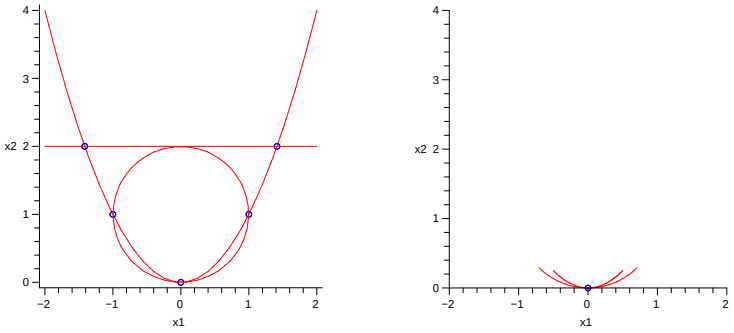
given by Theorem 3.2.1. □

Example 9.1.5. With the ideal $\mathcal{I}$ of Example 9.1.2, let $f = x_2 - x_1^2$. The curve defined by $\mathcal{I}$ intersects the parabola of zeros of f at the points $(0,0), (1,1), (-1,1), (-\sqrt{2}, 2), (\sqrt{2}, 2)$ in $\bar{\mathbb{Q}}^2$. Then $\mathcal{I}+(f) = (x_1^2(x_1-1)(x_1+1)(x_1^2-2), x_2 - x_1^2)$, though $\mathcal{I}_0+(f) = (x_1^2, x_2)$ since (x_1-1), (x_1+1) and (x_1^2-2) are units of $\mathbb{K}[[x_1]]$. We thus recover the local algebra $\bar{\mathbb{K}}[[x_1, x_2]]/(x_1^2, x_2)$ of the origin as a root of $\mathcal{I}+(f)$ (see Figure 9.1.8).

Remark 9.1.6. In Proposition 9.1.4, the requirement "x_1 is primitive for $\mathcal{I}+(f)$" can be replaced with "x_2 is primitive for $\sqrt{\mathcal{I}+(x_1)}$". Nevertheless, both hypotheses will be assumed to be true in our main algorithm 14.

Remark 9.1.7. As already mentioned in Remark 3.1.7 in Chapter 1, if g is a polynomial that does not vanishes when evaluated at the origin, it is a unit of $\mathbb{K}[[x_1, \ldots, x_n]]$, so that the local algebra $\mathbb{D}_0$ defined in Proposition 9.1.4 coincides with the one at the origin as a root of $(\mathcal{I}+(f)) : g^\infty$.

Figure 9.1.8.



$\mathcal{V}(\mathcal{I}+(f))$ $\mathcal{V}(\mathcal{J}_0+(f))$

The purpose of this chapter is the computation of $\mathbb{B}_0$. With this aim in view, we now express $\mathbb{B}_0$ as a submodule of an easily computable free module, in which all the calculation will be done. Let δ_0 be the degree of q_0. We let $\mathrm{Disc}(q)$ and $\mathrm{Disc}(q_0)$ denote the discriminants in x_2 of q and q_0 respectively. Since $\mathcal{I}$ is radical, the polynomials q and q_0 are square-free, so that $\mathrm{Disc}(q_0) \neq 0$; we let v_0 denote the *valuation* of $\mathrm{Disc}(q_0)$ in x_1, that is the largest integer such that $x_1^{v_0}$ divides $\mathrm{Disc}(q_0)$. We set $m_0 = \lfloor v_0/2 \rfloor$ and

$$\mathbb{L}_0 = \mathbb{K}[[x_1]]\frac{1}{x_1^{m_0}} \oplus \mathbb{K}[[x_1]]\frac{x_2}{x_1^{m_0}} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{\delta_0-1}}{x_1^{m_0}}.$$

We are to show that $\mathbb{B}_0$ is a submodule of $\mathbb{L}_0$. For this, we will use the following good properties of the Kronecker representation of $\mathcal{I}$, that come from Corollary 4.3.11:

$$\mathcal{I} \cap \mathbb{K}[x_1, x_2] = (q), \tag{9.1.1}$$

$$\forall j \in \{3, \ldots, n\}, (\partial q/\partial x_2)x_j - w_j \in \mathcal{I}. \tag{9.1.2}$$

Proposition 9.1.9. *$\mathbb{B}_0$ is a free $\mathbb{K}[[x_1]]$-submodule of $\mathbb{L}_0$ with rank δ_0.*

Proof. Since the ideal $\mathcal{I}$ is in Noether position, $x_3, \ldots, x_n$ are integral over $\mathbb{K}[[x_1]]$ modulo $\mathcal{J}_0$. Thus $\mathbb{B}_0$ is isomorphic to a submodule of the integral closure $\overline{\mathbb{K}[[x_1]]}$ of $\mathbb{K}[[x_1]]$ in $\mathbb{K}((x_1))[x_2]/(q_0)$, where $\mathbb{K}((x_1))$ denotes the field of formal Laurent series in x_1 over $\mathbb{K}$. The proposition is a refinement of the classical fact that $\overline{\mathbb{K}[[x_1]]}$ is a free submodule of the module $\mathbb{K}[[x_1]]1/\mathrm{Disc}(q_0) \oplus \mathbb{K}[[x_1]]x_2/\mathrm{Disc}(q_0) \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0-1}/\mathrm{Disc}(q_0)$ (see [Eis95, Proposition 13.14] for instance), as proved in the next paragraph.

Let b be an element of $\overline{\mathbb{K}[[x_1]]}$, and $b_1, \ldots, b_{\delta_0}$ be its coordinates in the basis $1, x_2, \ldots, x_2^{\delta_0-1}$ of the $\mathbb{K}((x_1))$-vector space $\mathbb{K}((x_1))[x_2]/(q_0)$. For j in $\{1, \ldots, \delta_0\}$, $x_1^{m_0}b_j$ belongs to $\mathbb{K}((x_1))$. Since $\overline{\mathbb{K}[[x_1]]} \cap \mathbb{K}((x_1)) = \mathbb{K}[[x_1]]$, it is sufficient to prove that $x_1^{m_0}b_j$ belongs to $\overline{\mathbb{K}[[x_1]]}$. With this aim in view, we introduce an auxiliary matrix. Since q_0 is monic, it splits in $\overline{\mathbb{K}[[x_1]]}$. Let $\alpha_1, \ldots, \alpha_{\delta_0}$ denote its roots, and for i in $\{1, \ldots, \delta_0\}$, let σ_i denote the $\mathbb{K}((x_1))$-automorphism that maps x_2 to α_i. Let M denote the matrix whose (i,j)th entry is $\sigma_i(x_2^{j-1}) = \alpha_i^{j-1}$, and let v be the vector whose ith entry is b_i. Then the ith entry of Mv is $\sigma_i(b)$, which is an element of $\overline{\mathbb{K}[[x_1]]}$ since b is in $\overline{\mathbb{K}[[x_1]]}$. Now, let d be the determinant of M. Since M has its coefficients

in $\overline{\mathbb{K}[[x_1]]}$, so has its matrix C of cofactors, and the i-th entry db_i of CMv belongs to $\overline{\mathbb{K}[[x_1]]}$. At last, $d = \prod_{r<s}(\alpha_s - \alpha_r)$ as a Vandermonde determinant, so that $d^2 = \mathrm{Disc}(q_0)$, and d has valuation m_0. We thus have $x_1^{m_0} b_i \in \overline{\mathbb{K}[[x_1]]}$.

Lastly, thanks to Property (9.1.1), we have $\mathcal{J}_0 \cap \mathbb{K}[[x_1]][x_2] = (q_0)$. Therefore $1, x_2, \ldots, x_2^{\delta_0 - 1}$ belong to $\mathbb{B}_0$, and thus the rank of $\mathbb{B}_0$ is δ_0. □

Remark 9.1.10. For computational purpose, it will be useful to have a bound on the quantities δ_0 and m_0. If δ denotes the partial degree of q in x_2, one easily deduce from the definition of q_0 that $\delta_0 \leq \delta$. Thanks to the general Noether position of $\mathcal{I}$, the total degree of q equals δ by Corollary 4.3.11(b), so that the valuation of $\mathrm{Disc}(q)$ is at most $\delta(\delta-1)$. Since $\mathrm{Disc}(q)$ equals $\mathrm{Disc}(q_0)(\mathrm{Res}(q_0, q/q_0))^2 \mathrm{Disc}(q/q_0)$ up to a sign, we thus have $m_0 \leq \delta(\delta-1)/2$. Finally, Corollary 7.2.8 will permit to control δ from the degree of the input system in the proof of Theorem 10.3.4.

Since q_0 is the monic generator of $\mathcal{J}_0 \cap \mathbb{K}[[x_1]][x_2]$ by Property (9.1.1), the $\mathbb{K}[[x_1]]$-module

$$\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \mathbb{K}[[x_1]]x_2 \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0 - 1}$$

is a $\mathbb{K}[[x_1]]$-submodule of $\mathbb{B}_0$. In Section 9.3, we will compute $\mathbb{B}_0$ by constructing a sequence $\mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_\gamma \subseteq \mathbb{L}_0$ of submodules with strict inclusions. Following [Eis95, Section 2.4], we call such a sequence a *chain of submodules of* $\mathbb{L}_0$; the integer γ is called the *length of the chain*. We end this subsection with a technical lemma that will be useful to establish the termination of our algorithm.

Lemma 9.1.11. *The length of a chain* $\mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_\gamma \subseteq \mathbb{L}_0$ *of submodules of* $\mathbb{L}_0$ *beginning with* $\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \mathbb{K}[[x_1]]x_2 \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0-1}$ *is at most* $m_0\delta_0$.

Proof. For $\alpha \in \{1, \ldots, m_0\delta_0\}$, we let q_α, respectively, r_α, denote the quotient, respectively, the remainder, of the Euclidean division of α by m_0. We set

$$\mathbb{N}_\alpha = \mathbb{K}[[x_1]]\frac{1}{x_1^{m_0}} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{q_\alpha - 1}}{x_1^{m_0}} \oplus \mathbb{K}[[x_1]]\frac{x_2^{q_\alpha}}{x_1^{r_\alpha}} \oplus \mathbb{K}[[x_1]]x_2^{q_\alpha+1} \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta_0-1},$$

and $\mathbb{N}_0 = \mathbb{M}_0$. The lemma directly follows from [Eis95, Theorem 2.13] since $\mathbb{N}_0 \subset \mathbb{N}_1 \subset \cdots \subset \mathbb{N}_{m_0\delta_0} = \mathbb{L}_0$ is a composition series. □

Example 9.1.12. With $\delta_0 = m_0 = 2$, we have $\mathbb{N}_0 = \mathbb{M}_0$,

$$\mathbb{N}_1 = \mathbb{K}[[x_1]]\frac{1}{x_1} \oplus \mathbb{K}[[x_1]]x_2,\ \mathbb{N}_2 = \mathbb{K}[[x_1]]\frac{1}{x_1^2} \oplus \mathbb{K}[[x_1]]x_2,\ \mathbb{N}_3 = \mathbb{K}[[x_1]]\frac{1}{x_1^2} \oplus \mathbb{K}[[x_1]]\frac{x_2}{x_1},$$

and $\mathbb{N}_4 = \mathbb{L}_0$.

9.2 Truncated Coordinates

We will give in Section 9.3 an algorithm to compute $\mathbb{B}_0$, that is based on the fact that $\mathbb{B}_0$ is the smallest algebra that contains $\mathbb{M}_0$ and the images of the variables $x_3, \ldots, x_n$ in $\mathbb{L}_0$. As

announced at the end of Section 9.1, we will construct a chain of submodules of $\mathbb{L}_0$ by adding vectors to $\mathbb{M}_0$, beginning with the images of $x_3, \ldots, x_n$ in $\mathbb{L}_0$; this operation is made possible by Algorithm 8 in Section 8.2 as soon as we can compute the coordinates of $x_3, \ldots, x_n$ to precision m_0+1. We study in this section the cost of computing q_0, which gives m_0, and the coordinates of the variables in $\mathbb{L}_0$ to any precision. For any $a \in \mathbb{K}[[x_1]][x_2]$, we write $a \mod q_0$ for the remainder of a divided by q_0.

Lemma 9.2.1. *Let $\eta \in \mathbb{N}\backslash\{0\}$.*

(a) The polynomial q_0 to precision η can be computed from q with $\tilde{\mathcal{O}}(\eta\delta)$ arithmetic operations in $\mathbb{K}$; this cost includes the computation of the inverse of q/q_0 modulo q_0 to precision η.

(b) The integer m_0 and a polynomial $\pi \in \mathbb{K}[[x_1]][x_2]$ such that $\pi\partial q_0/\partial x_2 \equiv x_1^{m_0} \mod q_0$ can be computed to precision η from q and q_0 to precision $\eta+m_0$ with $\tilde{\mathcal{O}}((\eta+m_0)\delta_0^2)$ arithmetic operations in $\mathbb{K}$.

Proof. The computations of part (a) can be achieved by a Hensel lifting of the Bézout relation $uq_0 + v(q/q_0) = 1$ modulo x_1, whose cost is given in [GG03, Theorem 15.11]. Let now $\tilde{q}_0 \in \mathbb{K}[x_1, x_2]$ denote the remainder of q_0 divided by $x_1^{\eta+m_0}$. Since q_0 is monic in x_2, $\mathrm{Disc}(q_0)$ and $\mathrm{Disc}(\tilde{q}_0)$ coincide to precision $\eta + m_0$. Now $\mathrm{Disc}(\tilde{q}_0)$ and some polynomials $a, b \in \mathbb{K}[x_1, x_2]$ such that $a\tilde{q}_0 + b\partial\tilde{q}_0/\partial x_2 = \mathrm{Disc}(\tilde{q}_0)$ can be computed from $\tilde{q}_0$ with $\tilde{\mathcal{O}}((m_0+\eta)\delta_0^2)$ arithmetic operations in $\mathbb{K}$ by [GG03, Corollary 11.18]. We can then take for π the truncation of $(x_1^{-m_0}\,\mathrm{Disc}(\tilde{q}_0))^{-1}b$ to precision η. □

Example 9.2.2. We gave in Example 4.3.3 the Kronecker representation of $\mathcal{I} = ((x_2-1)^2+(x_1+2x_2+4x_3)^2-1, x_3^2-x_2^2)$, which we recall comes from the change of variables in Example 7.1.5. We deduce from these data that $m_0 = 3$, and that the polynomial q_0 to precision $2m_0+\mu_0+1 = 10$ is

$$x_2^2 - (x_1^2 + 2x_1^3 + \tfrac{101}{4}x_1^4 + \tfrac{367}{2x_1^5} + \tfrac{14057}{8}x_1^6 + \tfrac{65453}{4}x_1^7 + \tfrac{10348865}{64}x_1^8 + \tfrac{51973671}{32}x_1^9)x_2$$
$$+(\tfrac{1}{4}x_1^4 + x_1^5 + \tfrac{77}{8}x_1^6 + 77x_1^7 + \tfrac{46301}{64}x_1^8 + \tfrac{109591}{16}x_1^9)$$

Let us remark that $\delta_0 = 2$, which is the number of branches of $\mathcal{V}(\mathcal{I})$ that pass through the origin.

Let $\tilde{m}$ be a monomial in $x_1, \ldots, x_n$. By Proposition 9.1.9, $\tilde{m}$ can be identified to an element of $\mathbb{L}_0$; we call *coordinates of $\tilde{m}$ in $\mathbb{L}_0$ to precision η* the coordinates of this element in the canonical basis $1/x_1^{m_0}, \ldots, x_2^{\delta_0-1}/x_1^{m_0}$ of $\mathbb{L}_0$, truncated in degree η. The following lemma allows the computation of the coordinates of any monomial to any precision.

Lemma 9.2.3. *Let $\eta \in \mathbb{N}$.*

(a) For $j \in \{3, \ldots, n\}$, the coordinates of x_j to precision η can be computed from w_j and the data of Lemma 9.2.1 to precision η with $\tilde{\mathcal{O}}(\eta\delta)$ arithmetic operations in $\mathbb{K}$.

(b) Let a and b be two elements of $\mathbb{B}_0$. The coordinates of ab to precision η can be computed from the coordinates of a and b to precision $\eta + m_0$ and q_0 to precision $\eta + m_0$ with $\tilde{\mathcal{O}}((\eta + m_0)\delta_0)$ operations in $\mathbb{K}$.

Proof. By Property (9.1.2), $(\partial q_0/\partial x_2)(q/q_0)x_j - w_j$ belongs to $\mathcal{J}_0$. Then with the notation of Lemma 9.2.1, $x_1^{m_0}x_j - (q/q_0)^{-1}\pi w_j$ belongs to $\mathcal{J}_0$. The coordinates of x_j in the basis $1/x_1^{m_0}, \ldots, x_2^{\delta_0-1}/x_1^{m_0}$ of $\mathbb{L}_0$ are thus the coefficients of $(q/q_0)^{-1}\pi w_j \mod q_0$, which ends the proof of part (a). Part (b) is a direct consequence of the fact that the coordinates of ab in $\mathbb{L}_0$ are the coefficients of $x_1^{m_0}ab \mod q_0$ in $\mathbb{K}[[x_1]]$. □

Example 9.2.4. (continued from Example 9.2.2) The coordinates of x_3 in the basis $1/x_1^3, x_2/x_1^3$ of $\mathbb{L}_0$ to precision $\delta_0 m_0 + \mu_0 + 1 = 10$ are

$$\begin{array}{l}(\frac{1}{8}x_1^4 - \frac{1}{8}x_1^5 - \frac{25}{32}x_1^6 - \frac{19}{4}x_1^7 - \frac{2479}{64}x_1^8 - \frac{42351}{128}x_1^9,\\ -\frac{1}{4}x_1^2 + \frac{3}{4}x_1^3 + \frac{19}{8}x_1^4 + \frac{187}{16}x_1^5 + \frac{3097}{32}x_1^6 + \frac{25671}{32}x_1^7 + \frac{235735}{32}x_1^8 + \frac{17894435}{256}x_1^9).\end{array}$$

9.3 Computation of the Module

We now give an algorithm to compute $\mathbb{B}_0$, together with the matrices of multiplication by the variables in $\mathbb{B}_0$ at a fixed precision. In this algorithm, any submodule of $\mathbb{L}_0$ is represented by its normal lower triangular basis (see Definition 8.2.1).

Algorithm 11. *Basis of* $\mathbb{B}_0$.

Input: The Kronecker representation $q, w_3, \ldots, w_n$ of an unmixed one-dimensional radical ideal $\mathcal{I}$ in general Noether position with primitive element x_2, and a positive integer η.

Output: The normal lower triangular basis of the $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$, and the matrices of multiplication by $x_2, \ldots, x_n$ with respect to the latter basis of $\mathbb{B}_0$ to precision η.

1. Compute δ_0, m_0, and q_0 to precision $2m_0 + 1$.
2. Compute the coordinates of $x_3, \ldots, x_n$ in $\mathbb{L}_0$ to precision $m_0 + 1$.
3. Initialize $\mathbb{M}$ with $\mathbb{M}_0$.
4. Initialize $\mathbb{M}'$ with $\mathbb{M}_0 + \mathbb{K}[[x_1]]x_3 + \cdots + \mathbb{K}[[x_1]]x_n$.
5. While $\mathbb{M} \neq \mathbb{M}'$,
   a. replace $\mathbb{M}$ with $\mathbb{M}'$,
   b. and let $e_1, \ldots, e_{\delta_0}$ denote the normal lower triangular basis of $\mathbb{M}$.
   c. for all $(k, \ell) \in \{1, \cdots, \delta_0\}^2$,
      i. compute the coordinates of $e_k e_\ell$ to precision $m_0 + 1$;
      ii. replace $\mathbb{M}'$ with $\mathbb{M} + \mathbb{K}[[x_1]]e_k e_\ell$.
6. a. Compute q_0 and the coordinates of $x_3, \ldots, x_n$ to precision $m_0\delta_0 + m_0 + \eta$.
   b. Compute the matrices $N_{x_2}, \ldots, N_{x_n}$ of multiplication by $x_2, \ldots, x_n$ respectively with respect to the basis $e_1, \ldots, e_{\delta_0}$ to precision η.

7. Return $\mathbb{M}', N_{x_2}, \ldots, N_{x_n}$.

Proposition 9.3.1. *Algorithm 11 works correctly as specified with*

$$\tilde{\mathcal{O}}(n(m_0\delta_0+\eta)(\delta+\delta_0^4)+m_0^2\delta_0^5)$$

arithmetic operations in $\mathbb{K}$.

Proof. Lemma 9.1.11 ensures the termination of Algorithm 11. Thanks to Proposition 8.2.4, step 4 can be performed from the coordinates of $x_3, \ldots, x_n$ to precision m_0+1, and step 5.c.ii can be deduced from the coordinates of $e_k e_\ell$ to precision m_0+1, that can be computed from the exact coordinates of e_k and e_ℓ and from q_0 to precision $2m_0+1$ by Lemma 9.2.3 (b). Then the returned module is the smallest algebra that contains $\mathbb{M}_0$ and $x_3, \ldots, x_n$, that is $\mathbb{B}_0$.

By Lemma 9.2.1, step 1 costs $\tilde{\mathcal{O}}(m_0(\delta+\delta_0^2))$ operations in $\mathbb{K}$; by Lemma 9.2.3 (a), step 2 costs $(n-2)\tilde{\mathcal{O}}(m_0\delta)$ operations. Lemma 9.1.11 bounds the number of crossing through the while loop of step 5 by $m_0\delta_0$. Step 5.c.i costs $\tilde{\mathcal{O}}(m_0\delta_0)$ operations by Lemma 9.2.3 (b), and is performed δ_0^2 times at each cross through the while loop; this amounts to $\tilde{\mathcal{O}}(m_0^2\delta_0^4)$ operations in $\mathbb{K}$ all in all. Finally, Algorithm 11 computes at most $(n-2)+m_0\delta_0^3$ module-vector sums in $\mathbb{L}_0$; the cost of computing all these sums belongs to $m_0\delta_0\tilde{\mathcal{O}}(m_0\delta_0^3)+(n-2+m_0\delta_0^3-m_0\delta_0)\tilde{\mathcal{O}}(m_0\delta_0^2)$ operations in $\mathbb{K}$ by Lemma 9.1.11 and Proposition 8.2.4, and thus to $\tilde{\mathcal{O}}(m_0\delta_0^2(n+m_0\delta_0^3))$ operations.

Lastly, let $e_1, \ldots, e_{\delta_0}$ be the normal lower triangular basis of $\mathbb{B}_0$, let E be the δ_0 square matrix whose ℓ-th column is the vector of coordinates of e_ℓ in $\mathbb{L}_0$, and let M_j be the δ_0 square matrix M_j whose ℓ-th column is the vector of coordinates of $x_j e_\ell$ in $\mathbb{L}_0$; the matrix of multiplication by x_j in the basis $e_1, \ldots, e_{\delta_0}$ of $\mathbb{B}_0$ is thus $N_{x_j} = E^{-1}M_j$. Since the degree of the entries of E are bounded by m_0 by Lemma 8.2.3, the determinant of E has valuation at most $m_0\delta_0$; the knowledge of M_j to precision $m_0\delta_0+\eta$ thus allows the computation of N_{x_j} to precision η. At last, the matrix M_j to precision $m_0\delta_0+\eta$ can be deduced from q_0 and the coordinates of x_j to precision $m_0\delta_0+m_0+\eta$ by part (b) of Lemma 9.2.3. By Lemma 9.2.1 and Lemma 9.2.3, step 6 takes $\tilde{\mathcal{O}}(n(m_0\delta_0+\eta)(\delta+\delta_0^4))$ operations in $\mathbb{K}$. □

Example 9.3.2. (continued from Example 9.2.4) We begin at step 3 of Algorithm 11 with $\mathbb{M}_0 = \mathbb{K}[[x_1]] + \mathbb{K}[[x_1]]x_2$, with normal lower triangular basis $x_1^3(1/x_1^3), x_1^3(x_2/x_1^3)$. At step 4, we initialize $\mathbb{M}'$ with the basis $e_1 = x_1^3(1/x_1^3), e_2 = x_1^2(x_2/x_1^3)$ of $\mathbb{M}_0 + \mathbb{K}[[x_1]]x_3$. Then since $\mathbb{M}' + \mathbb{K}[[x_1]]e_1^2 = \mathbb{M}' = \mathbb{M}' + \mathbb{K}[[x_1]]e_1e_2 = \mathbb{M}' + \mathbb{K}[[x_1]]e_2^2$, we obtain that $\mathbb{B}_0 = \mathbb{M}_0 + \mathbb{K}[[x_1]]x_3$. The matrices of multiplication by the variables in the basis e_1, e_2 of $\mathbb{B}_0$ to precision $\mu_0+1=4$ are

$$N_{x_1} = \begin{pmatrix} x_1 & 0 \\ 0 & x_1 \end{pmatrix}, \; N_{x_2} = \begin{pmatrix} 0 & -\frac{1}{4}x_1^3 \\ x_1 & x_1^2+2x_1^3 \end{pmatrix} \text{ and}$$

$$N_{x_3} = \begin{pmatrix} -\frac{1}{8}x_1 - \frac{1}{8}x_1^2 - \frac{25}{32}x_1^3 & \frac{1}{16}x_1^2 + \frac{1}{16}x_1^3 \\ -\frac{1}{4} + \frac{3}{4}x_1 + \frac{19}{8}x_1^2 + \frac{187}{16}x_1^3 & -\frac{1}{8}x_1 + \frac{1}{8}x_1^2 - \frac{103}{32}x_1^3 \end{pmatrix}.$$

Chapter 10

Intersection and Overdetermined Case

In this chapter, we achieve the computation of the primary decomposition of a zero-dimensional ideal. First we give an algorithm to compute the local intersection at the origin from the module of the curve germ. Then we explain how a similar idea permits to deal with overdetermined systems. Finally, we summarize the top level algorithm for zero-dimensional primary decomposition, together with its cost analysis.

10.1 Smith Form and Intersection

We enter this section with

- the normal lower triangular basis of a $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$ related to an unmixed one-dimensional radical ideal $\mathcal{I}$,
- the matrices $N_{x_2}, \ldots, N_{x_n}$ of the morphisms of multiplication by $x_2, \ldots, x_n$ in $\mathbb{B}_0$ with respect to the latter basis,
- and a polynomial f,

such that the $\bar{\mathbb{K}}$-algebra $\bar{\mathbb{K}} \otimes \mathbb{B}_0/(f)$ is isomorphic to the local algebra

$$\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, \ldots, x_n]]/(\mathcal{I} + (f)), \tag{10.1.1}$$

whose dimension μ_0 is supposed to be known.

Our purpose is the design of an algorithm to calculate the matrices $M_{x_1}, \ldots, M_{x_n}$ of the morphisms of multiplication by $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}_0$. In the following lemma, we recall the basis found in the proof of Proposition 5.3.1, which can be easily deduced from a Smith normal form with multipliers (see Definition 8.3.1):

Lemma 10.1.1. *Let $e_1, \ldots, e_{\delta_0}$ and $e'_1, \ldots, e'_{\delta_0}$ be two bases of the $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$ and $\nu_1 \leq \cdots \leq \nu_{\delta_0}$ be integers such that for all $k \in \{1, \ldots, \delta_0\}$, $fe_k = x_1^{\nu_k} e'_k$. Then*

$$\mathcal{B} = \{x_1^{n_k} e'_k, 1 \leq k \leq \delta_0, 0 \leq n_k < \nu_k\}$$

is a basis of $\mathbb{D}_0$. *In particular,* μ_0 *equals* $\sum_{k=1}^{\delta_0} \nu_k$.

Proof. The lemma directly follows from isomorphism (10.1.1) since $\mathcal{B}$ is a basis of the cokernel of the morphism of multiplication by f in $\mathbb{B}_0$. □

Lemma 10.1.1 and Proposition 8.3.4 directly yield the following algorithm:

Algorithm 12. *Local Intersection.*

Input: The normal lower triangular basis of $\mathbb{B}_0$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$, the dimension μ_0 of $\mathbb{D}_0$, the matrices $N_{x_2}, \ldots, N_{x_n}$ of multiplication by the variables in the normal lower triangular basis of $\mathbb{B}_0$ to precision $\mu_0 + 1$.

Output: The matrices $M_{x_1}, \ldots, M_{x_n}$ of multiplication by $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}_0 \simeq \mathbb{B}_0/(f)$.

1. Compute the matrix N_f of multiplication by f with respect to the normal lower triangular basis of $\mathbb{B}_0$ to precision $\mu_0 + 1$.
2. Compute the diagonal $x_1^{\nu_1}, \ldots, x_1^{\nu_{\delta_0}}$ of the Smith normal form S of N_f, together with the pre-multiplier U to precision $\mu_0 + 1$.
3. For i from 1 to n,
   a. compute $\bar{N}_{x_i} = U N_{x_i} U^{-1}$ to precision $\mu_0 + 1$;
   b. for (k, ℓ) in $\{1, \ldots, \mu_0\} \times \{1, \ldots, \mu_0\}$,
      i. initialize M_{x_i} with the zero $\mu_0 \times \mu_0$ matrix;
      ii. let $i_k = 1 + \max\{i, \sum_{r=1}^{i} \nu_r \leq k\}$ and $j_\ell = 1 + \max\{j, \sum_{r=1}^{j} \nu_r \leq \ell\}$;
      iii. let $(M_{x_i})_{k,\ell}$ be the coefficient of $x_1^{k-i_k}$ in $x_1^{\ell - j_\ell} (\bar{N}_{x_i})_{i_k, j_\ell}$.
4. Return $M_{x_1}, \ldots, M_{x_n}$.

Proposition 10.1.2. *If* f *is given by a straight-line program of size* L, *then Algorithm 12 works correctly as specified with*

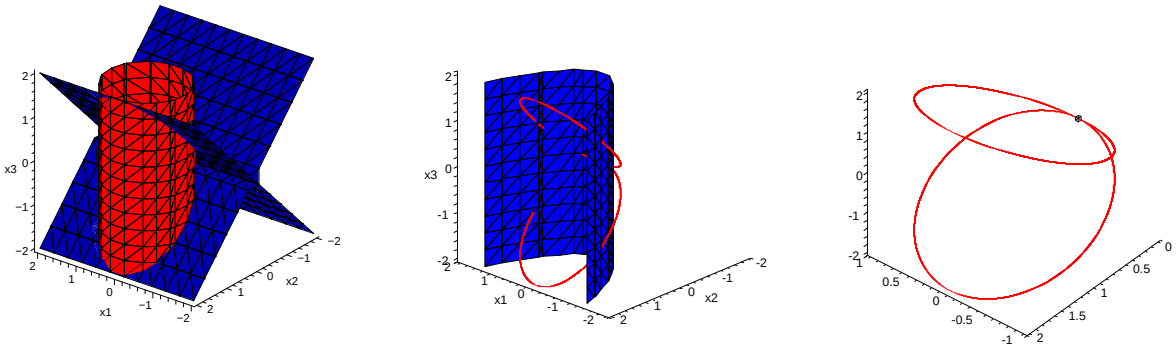
$$\tilde{\mathcal{O}}(\mu_0 \delta_0^3 (L + n + \delta_0))$$

arithmetic operations in $\mathbb{K}$.

Proof. The columns of the matrix U computed at step 2 are the vectors of coordinates of a basis e' of $\mathbb{B}_0$ as in Lemma 10.1.1; we let $\mathcal{B}$ denote the associated basis of $\mathbb{D}_0$. In step 3.b, we compute the matrices of multiplication by the variables with respect to the basis $e'_1, \ldots, e'_{\delta_0}$ of $\mathbb{B}_0$: for $\ell \in \{1, \ldots, \delta_0\}$ and $i \in \{2, \ldots, n\}$, we have $x_i e'_\ell = \sum_{k=1}^{\delta} (N_{x_i})_{k,\ell} e'_k$. Step 3.c extracts the coefficients in $\mathbb{K}$ of $\sum_{i_k=1}^{\delta_0} (x_1^s (N_{x_i})_{i_k, j_\ell}) e'_{i_k}$, that are the coordinates of $x_i (x_1^s e'_{j_\ell})$ in the basis $\mathcal{B}$ of $\mathbb{D}_0$.

The evaluation of f at $(N_{x_1}, \ldots, N_{x_n})$ to precision $\mu_0 + 1$ gives the matrix N_f to precision $\mu_0 + 1$. Step 2 can be executed from N_f to precision $\mu_0 + 1$ by Proposition 8.3.3. Step 3.b can

Figure 10.1.4.



$\mathcal{V}(f_1), \mathcal{V}(f_2)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_3)$ $\mathcal{V}(f_1, f_2), \mathcal{V}(f_1, f_2, f_3)$

be performed from the matrices U and N_{x_i} to precision $\mu_0 + 1$ that are computed at steps 1 and 2 (since the determinant of the matrix U has valuation 0, we can invert U without loss of precision). Finally, the knowledge of N_{x_i} to precision $\mu_0 + 1$ allows the computation of step 3.c since all the ν_k are bounded by μ_0.

Step 1 costs $\tilde{\mathcal{O}}(L\mu_0\delta_0^3)$ operations in $\mathbb{K}$. By Proposition 8.3.3, the cost of step 2 belongs to $\tilde{\mathcal{O}}(\mu_0\delta_0^3)$ operations. Finally, the computation of U^{-1} costs $\tilde{\mathcal{O}}(\mu_0\delta_0^4)$ operations, so that the cost of step 3 belongs to $\tilde{\mathcal{O}}(\mu_0\delta_0^3(\delta_0 + n))$ operations. □

Example 10.1.3. (continued from Example 9.3.2) Let us recall from Example 7.1.5 that $f_3 = x_2 - (x_1 + 2x_2 + 4x_3)^2$; the Smith normal form of N_{f_3} is $\begin{pmatrix} x_1 & 0 \\ 0 & x_1^2 \end{pmatrix}$. With the notation of Lemma 10.1.1, the matrices of multiplication by the variables in the basis e_1', e_2', x_1e_2' of $\mathbb{D}_0$ are

$$M_{x_1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \; M_{x_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } M_{x_3} = \begin{pmatrix} 0 & \frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{1}{16} & 0 \end{pmatrix}.$$

Coming back to the original system

$$\begin{cases} f_1 &= x_1^2 + (x_2 - 1)^2 + 1 \\ f_2 &= x_3^2 - x_2^2 \\ f_3 &= x_2 - x_1^2 \end{cases}$$

by applying ϕ^{-1}, we obtain the matrices

$$M_{x_1} = \begin{pmatrix} 0 & -4\frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & 1 + 4\frac{1}{16} & 0 \end{pmatrix}, \; M_{x_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } M_{x_3} = \begin{pmatrix} 0 & \frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{1}{16} & 0 \end{pmatrix}.$$

Let us remark that $M_{x_1}^2 = M_{x_1}M_{x_3} = M_{x_3}^2 = 0$; the monomials $1, x_1, x_3$ thus constitute a basis of the $\bar{\mathbb{K}}$-algebra $\mathbb{D}_0$. The computation of Example 3.3.3 give the corresponding primary ideal $(x_1^2, x_1x_3, x_3^2, x_2)$.

10.2 Overdetermined Case

In this section, we explain how to deal with overdetermined systems, that is, with zero-dimensional ideals $(g_1, \ldots, g_s) : g^\infty$ such that $s > n$.

Proposition 7.1.6 permits to assume that $s = n + 1$. We thus have to end the computation of

$$\mathbb{D}'_0 \simeq \mathbb{D}_0 + (h) \tag{10.2.1}$$

for some polynomial h. Isomorphism (10.2.1) directly yields an algorithm that computes the matrices $M'_{x_1}, \ldots, M'_{x_n}$ of multiplication by $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}'_0$ from the matrices $M_{x_1}, \ldots, M_{x_n}$ above:

Algorithm 13. *Overdetermined Case*

Input: The matrices $M_{x_1}, \ldots, M_{x_n}$ of multiplication by $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}_0$.

Output: The matrices $M'_{x_1}, \ldots, M'_{x_n}$ of multiplication by $x_1, \ldots, x_n$ with respect to a basis of $\mathbb{D}'_0 \simeq \mathbb{D}_0/(h)$.

1. Let M_h be the matrix obtained by evaluating h in $(M_{x_1}, \ldots, M_{x_n})$.
2. Compute a basis $e_1, \ldots, e_{\mu_0}$ of $\mathbb{D}_0$ such that $e_1, \ldots, e_{\mu'_0}$ is a basis of the cokernel of M_h.
3. For $i \in \{1, \ldots, n\}$,
   a. compute the matrix M''_{x_i} of multiplication by x_i in the basis $e_1, \ldots, e_{\mu_0}$;
   b. $M'_{x_i} = (((M''_{x_i})_{j,k}))_{1 \le j \le \mu'_0, 1 \le k \le \mu'_0}$.
4. Return $M'_{x_1}, \ldots, M'_{x_n}$.

Proposition 10.2.1. *Let us assume that h is given by a straight-line program of size L. Then Algorithm 13 works correctly as specified with $\mathcal{O}((L+n)\mu_0^3)$ arithmetic operations in $\mathbb{K}$.*

Proof. The correctness of Algorithm 13 is a direct consequence of isomorphism (10.2.1). Since the computations of Algorithm 13 are linear algebra in $\mathbb{D}_0$ whose dimension is μ_0, its cost belongs to $(L+n)\mathcal{O}(\mu_0^3)$ arithmetic operations in $\mathbb{K}$. □

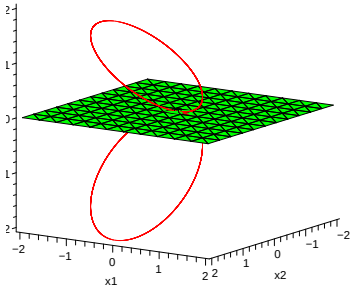
Example 10.2.2. Let $n = 2$, $\mathcal{I} = (x_2^2)$, $f = x_1^2$ and $h = x_1x_2$. Then $1, x_1, x_2, x_1x_2$ form a basis of $\mathbb{D}_0$, and the cokernel of the morphism of multiplication by h in $\mathbb{D}_0$ is obviously generated by $1, x_1, x_2$. The matrices of multiplication by x_1, x_2 in this basis of $\mathbb{D}'_0$ can easily be deduced from their matrices in the latter basis of $\mathbb{D}_0$.

Example 10.2.4. With the notation of Example 10.1.3, the image of the morphism of multiplication by $h = x_3$ is generated by $w = (1159449/65536)e'_1 - (1/16)x_1e'_2$. In the basis $e'_2, x_1e'_2$ have

$$M_{x_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \; M_{x_2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } M_{x_3} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

These matrices yield the primary ideal (x_1^2, x_2, x_3) to describe the origin (see Figure 10.2.3).

Figure 10.2.3.



$\mathcal{V}(f_1, f_2), \mathcal{V}(x_3)$

10.3 Top Level Algorithm

In this section, we summarize our main algorithm, in which all the local algebras are computed together. The output of our algorithm will be an extension of the univariate representation with multiplicities $\tilde{\chi}, \tilde{Q}, \tilde{V}_1, \ldots, \tilde{V}_n$ of the zero-dimensional ideal $(g_1, \ldots, g_s) : g^\infty$ given as input. More precisely, our algorithm further computes:

- an integer ρ;
- a sequence of integers $\mu_1, \ldots, \mu_\rho$ and a sequence of pairwise relatively prime univariate polynomials $Q_1, \ldots, Q_\rho \in \mathbb{K}[T]$ such that $\tilde{\chi} = Q_1^{\mu_1} \cdots Q_\rho^{\mu_\rho}$;
- for each $\ell \in \{1, \ldots, \rho\}$, a sequence of square $\mu_\ell \times \mu_\ell$ matrices $M_{x_1}^{(\ell)}, \ \ldots, M_{x_n}^{(\ell)}$ with entries in $\mathbb{K}[T]$ such that for any root α of Q_ℓ in $\bar{\mathbb{K}}$, the evaluation of $M_{x_1}^{(\ell)}, \ldots, M_{x_n}^{(\ell)}$ in $T = \alpha$ are the matrices of multiplication by $x_1, \ldots, x_n$ with respect to a common basis of the local algebra $\mathbb{D}_{V(\alpha)}$ of $V(\alpha)$ as a root of $(g_1, \ldots, g_s) : g^\infty$.

In the sequel, we refer to the sequence $(\mu_\ell, Q_\ell, M_{x_1}^{(\ell)}, \ \ldots, M_{x_n}^{(\ell)})_{1 \le \ell \le \rho}$ as a *local univariate representation* of the zero-dimensional ideal $(g_1, \ldots, g_s) : g^\infty$.

Example 10.3.1. Let $n = s = 2$, $f_1 = x_1^2 + (x_2 - 1)^2 - 1$, $f_2 = x_2 - x_1^2$ and $g = 1$. The univariate representation in x_1 with multiplicities of $(f_1, f_2) : g^\infty = (f_1, f_2)$ is

$$\chi = T^2(T-1)(T+1), \ V_1 = T, \ V_2 = T^2.$$

A local univariate representation of (f_1, f_2) is $\rho = 2$,

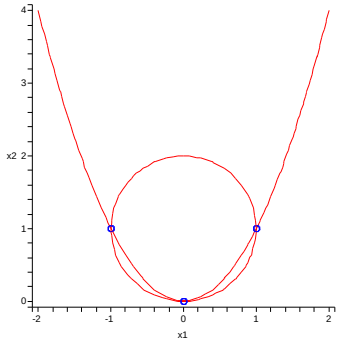
$$\mu_1 = 1, \ Q_1 = T^2 - 1, \ M_{x_1}^{(1)} = (T), \ M_{x_2}^{(1)} = (1)$$

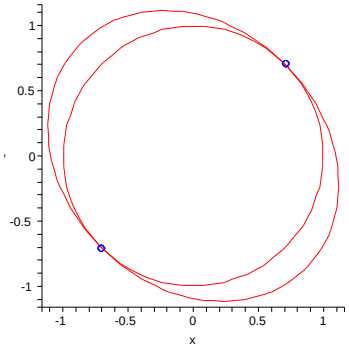
for the two simple roots $(-1, 1)$ and $(1, 1)$, and

$$\mu_2 = 2, \ Q_2 = T, M_{x_1}^{(2)} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } M_{x_2}^{(2)} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

for the double root $(0, 0)$.

Figure 10.3.3.





$\mathcal{V}(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)$ $\mathcal{V}(x_1^2 + x_2^2 - 1, 5x_1^2 + 2x_1x_2 + 5x_2^2 - 6)$

Example 10.3.2. The equations $f_1 = x_1^2 + x_2^2 - 1$ and $f_2 = 5x_1^2 + 2x_1x_2 + 5x_2^2 - 6$ have two common double roots $(\sqrt{2}/2, \sqrt{2}/2)$ and $(-\sqrt{2}/2, -\sqrt{2}/2)$. Our top level algorithm in Section 10.3 returns the univariate representation

$$\chi = (T^2 - 1/2)^2, V_1 = T, V_2 = -2T^3 + 2T$$

of (f_1, f_2), the only factor $Q_1 = (T^2 - 1/2)$ with multiplicity $\mu_1 = 2$, and the matrices

$$M_{x_1}^{(1)} = \begin{pmatrix} 0 & -1/2 \\ 1 & 2T \end{pmatrix} \text{ and } M_{x_2}^{(2)} = \begin{pmatrix} 2T & 1/2 \\ -1 & 0 \end{pmatrix}.$$

The evaluation of $M_{x_1}^{(1)}$ and $M_{x_2}^{(2)}$ in $T = \sqrt{2}/2$ are the matrices of multiplication by the variables with respect to a basis of $\mathbb{D}_{(\sqrt{2}/2, \sqrt{2}/2)}$ (indeed the basis is $1, x_1$).

The polynomials $Q_1, \ldots, Q_\rho$ of our representation come from the use of dynamic evaluation (see [Duv94, Duv95]). Dynamic evaluation is a rather intuitive process that avoids irreducible factorization. More precisely, let Q be a square-free polynomial and $\mathbb{F}$ be the quotient $\mathbb{K}[T]/(Q)$. Computations are done in $\mathbb{F}$, where T is treated as a parameter. When we encounter a test on T whose answer depends on the irreducible factors of Q, the computation tree splits in two branches. For instance, let $Q = T(T^2 - 1)$ and assume that the test is "T is a simple root of $\chi = T^2(T - 1)(T + 1)$". Then we continue the computation in $\mathbb{K}[T]/(T)$ with the answer no, and in $\mathbb{K}[T]/(T^2 - 1)$ with the answer yes.

Our main algorithm works as follows: first, we use the Kronecker solver to reduce the problem to the intersection of an unmixed one-dimensional radical ideal $\mathcal{I}$ and a polynomial f. Algorithm 7 returns the rational univariate representation with multiplicities $\chi, Q, V_1 = x_1, V_2 \ldots, V_n$ of $(\mathcal{I} + (f)) : g^\infty$ with respect to x_1. By performing the translation $x_1 - T, x_2 - V_2(T), \ldots, x_n - V_n(T)$ in the dynamic field $\mathbb{F} = \mathbb{K}[T]/(Q)$, we come back to the computation of the local algebra $\mathbb{D}_0$ of the origin as a root of $\mathcal{I} + (f)$. We then apply Algorithms 11 and 12 to end the computation. If the input system is overdetermined, the variant of Algorithm 7 presented in Corollary 7.1.9 returns a polynomial h to which we apply Algorithm 13. We finish with going back to the original play of variables.

For sake of simplicity, we do not detail the dynamic evaluation process in step 2 of our main algorithm:

Algorithm 14. *Local Univariate Representation*

Input: $g_1, \ldots, g_s, g \in \mathbb{K}[x_1, \ldots, x_n]$, given by a straight line program of size L such that the ideal $(g_1, \ldots, g_s) : g^\infty$ is zero-dimensional.

Output: A local univariate representation of $(g_1, \ldots, g_s) : g^\infty$.

1. a. By Algorithm 7, compute
   - an affine change of variables ϕ with shape (7.1.1),
   - the Kronecker representation $q, w_3, \ldots, w_n$ in x_2 of an unmixed one-dimensional radical ideal $\mathcal{I}$,
   - a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ such that $(\mathcal{I} + (f)) : (g \circ \phi)^\infty$ is zero-dimensional with primitive element x_1, and equals $((g_1, \ldots, g_n) : g^\infty) \circ \phi$ if $s = n$,
   - the univariate representation with multiplicities $\chi, Q, V_1, V_2, \ldots, V_n$ in x_1 of $(\mathcal{I} + (f)) : (g \circ \phi)^\infty$,
   - if $s > n$, a polynomial $h \in \mathbb{K}[x_1, \ldots, x_n]$ such that $((g_1, \ldots, g_s) : g^\infty) \circ \phi = ((\mathcal{I} + f) : (g \circ \phi)^\infty) + h$.

   b. Replace $\mathbb{K}$ with the dynamic field $\mathbb{F} = \mathbb{K}[T]/(Q)$, and $q, w_3, \ldots, w_n, f$ and g with their evaluation at $x_1 - T, x_2 - V_2(T), \ldots, x_n - V_n(T)$.

   c. Initialize μ_0 with the valuation of χ in T.

2. a. By Algorithm 11, compute
   - the normal lower triangular basis of
   $$\mathbb{B}_0 = \mathbb{F}[[x_1]][x_2, \ldots, x_n]/(\mathcal{I}_0 + (q_0)),$$
   - the matrices of multiplication by $x_2, \ldots, x_n$ with respect to this basis to precision $\mu_0 + 1$.

   b. By Algorithm 12, compute the matrices $M_{x_1}, \ldots, M_{x_n}$ of multiplication by $x_1, \ldots, x_n$ with respect to a basis of
   $$\mathbb{D}_0 = \bar{\mathbb{K}}[[x_1, \ldots, x_n]]/(\mathcal{I} + (f)) : (g \circ \phi)^\infty.$$

   c. If $s > n$,

      i. by Algorithm 13, replace $M_{x_1}, \ldots, M_{x_n}$ with the matrices of multiplication by $x_1, \ldots, x_n$ with respect to a basis of
      $$\mathbb{D}'_0 = \bar{\mathbb{K}}[[x_1, \ldots, x_n]]/(\mathcal{I} + (f)) : (g \circ \phi)^\infty + (h);$$

      ii. replace χ with $\gcd(\chi, h(x_1, V_2(x_1), \ldots, V_n(x_1))$ and μ_0 with the valuation of χ.

3. Return the univariate representation with multiplicities $\chi(T), \phi^{-1}(T, V_2(T), \ldots, V_n(T))$ of $(g_1, \ldots, g_s) : g^\infty$, and the matrices $\phi^{-1}(M_{x_1}, \ldots, M_{x_n})$.

Theorem 10.3.4. *Algorithm 14 works correctly as specified with*

$$\tilde{\mathcal{O}}(n(n(L+ns)+n^4)(d_1D)^2 + D^2(\delta^9 + n\delta^7) + nD^2\delta^4 + (L+ns)D^5)$$

operations in $\mathbb{K}$, where δ is the degree of the polynomial q in step 1.a, which is bounded by $d_1 \cdots d_{n-1}$, and where D is the product $d_1 \cdots d_n$. The correctness of the output relies on random choices of $\mathcal{O}(ns)$ elements of $\mathbb{K}$; choices for which the result is not correct are enclosed in a strict algebraic subset.

Proof. The correctness of Algorithm 14 is a consequence of Propositions 9.3.1, 10.1.2 and 10.2.1. By Corollary 7.1.9, step 1 can be performed with $\tilde{\mathcal{O}}(n(n(L+ns)+n^4)(d_1D)^2)$ arithmetic operations in $\mathbb{K}$. From Propositions 9.3.1, 10.1.2, 10.2.1 and Remark 9.1.10, we obtain that steps 1.b, 1.c, 2 and 3 cost

$$\tilde{\mathcal{O}}(\delta^9 + n\delta^7 + \mu_0(n\delta^4 + (L+ns)(\delta^3 + \mu_0^2))) \tag{10.3.1}$$

operations in the dynamic field $\mathbb{F}$.

The latter expression is the cost of the computations of one path through the dynamic evaluation tree $\mathcal{T}$. Since the degree of χ is at most D, μ_0 can be bounded by D in (10.3.1). Since the degree of Q is at most D, any operation in a node of $\mathcal{T}$ costs at most $\tilde{\mathcal{O}}(D)$ operations in $\mathbb{K}$; the cost of one path through the tree thus belongs to $\tilde{\mathcal{O}}(D(\delta^9 + n\delta^7) + \mu_0 D(n\delta^4 + (L+ns)D^3))$ operations in $\mathbb{K}$ since δ is at most D. Finally, the bound on the degree of Q ensures that $\mathcal{T}$ has at most D external nodes, which leads to the result since the sum of the multiplicities of all the external nodes is at most D. □

Example 10.3.5. Combining Examples 7.1.10, 9.3.2 and 10.1.3, we obtain the univariate representation with multiplicities

$$\begin{cases} \chi &= T^3(T-3)(T-1)(T+5)(T+7), \\ Q &= T(T-3)(T-1)(T+5)(T+7), \\ V_1 &= -2\frac{11866}{1157625}T^6 - (2\frac{105848}{1157625} - 4\frac{389}{44100})T^5 - (-2\frac{811}{46305} - 4\frac{3427}{44100})T^4 \\ &\quad +(-2\frac{1255064}{1157625} + \frac{401}{17640})T^3 + (4\frac{41401}{44100})T^2 + (1+4\frac{1}{8})T, \\ V_2 &= -\frac{11866}{1157625}T^6 - \frac{105848}{1157625}T^5 + \frac{811}{46305}T^4 + \frac{1255064}{1157625}T^3, \\ V_3 &= \frac{389}{44100}T^5 + \frac{3427}{44100}T^4 - \frac{401}{17640}T^3 - \frac{41401}{44100}T^2 - \frac{1}{8}T, \end{cases}$$

and the local univariate representation

- $\rho = 2$,
- $\mu_1 = 1$, $Q_1 = (T-3)(T-1)(T+5)(T+7)$ and

  $$M_{x_1} = \left(\frac{1}{30}T^3 + \frac{1}{5}T^2 - \frac{7}{30}T - 1\right),\ M_{x_2} = (1),\ M_{x_3} = \left(\frac{1}{120}T^3 + \frac{1}{20}T^2 - \frac{37}{120}T - \frac{3}{4}\right)$$

  for the four simple roots,

- $\mu_2 = 3,\ Q_2 = T$ and

$$M_{x_1} = \begin{pmatrix} 0 & -4\frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & 1+4\frac{1}{16} & 0 \end{pmatrix},\ M_{x_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } M_{x_3} = \begin{pmatrix} 0 & \frac{1159449}{65536} & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{1}{16} & 0 \end{pmatrix}$$

  for the triple root at the origin.

Proof of "Théorème 1". Théorème 1 in the introduction is a corollary of Theorem 10.3.4 since δ is bounded by D and n is at most D whenever d_n is strictly greater than 1. □

The exponent of Théorème 1 is not optimal. First it could be lowered by considering the precise cost of linear algebra, that is, by replacing the exponent 3 with ω; to make this relevant, we should have to give better algorithms in Chapter 8. Then, the bottleneck of the algorithm is the computation of $\mathbb{B}_0$ from the Kronecker representation of $\mathcal{I}$. Algorithm 11 in Section 9.3 could be replaced by an algorithm inspired from [FGLM93] that avoids useless module-vector sums; another way to reduce the cost of the computation of $\mathbb{B}_0$ may be to use structured linear algebra. Finally, the cost of dynamical evaluation could be examined more precisely.

Bibliographie

[ABRW96] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann, *Zeros, multiplicities, and idempotents for zero-dimensional systems*, Algorithms in algebraic geometry and applications (Basel), Progr. Math., vol. 143, Birkhäuser, 1996, pp. 1–15.

[BCS97] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 315, Springer-Verlag, 1997.

[BGHM97] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, *Polar varieties, real equation solving, and data structures: the hypersurface case*, J. Complexity **13** (1997), no. 1, 5–27.

[BGHM01] ———, *Polar varieties and efficient real elimination*, Math. Z. **238** (2001), no. 1, 115–144.

[BGHP04] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties and an efficient real elimination procedure*, Kybernetika (Prague) **40** (2004), no. 5, 519–550.

[BHMW02] N. Bruno, J. Heintz, G. Matera, and R. Wachenchauzer, *Functional programming concepts and straight-line programs in computer algebra*, Math. Comput. Simulation **60** (2002), no. 6, 423–473.

[BLS+04] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ACM, 2004, pp. 42–49.

[BMWW04] A. Bompadre, G. Matera, R. Wachenchauzer, and A. Waissbein, *Polynomial equation solving by lifting procedures for ramified fibers*, Theoret. Comput. Sci. **315** (2004), no. 2-3, 334–369.

[Buc70] B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungsystems*, Aequationes Math. **4** (1970), 374–383.

[BW93] T. Becker and V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, 1993.

[CCT97] M. Caboara, P. Conti, and C. Traverso, *Yet another ideal decomposition algorithm*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., Springer, Berlin, 1997, pp. 39–54.

[CGH+03] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.

[CHLM00] B. Castaño, J. Heintz, J. Llovet, and R. Martínez, *On the data structure straight-line program and its implementaion in symbolic computation*, Math. Comput. Simulation **51** (2000), no. 5, 497–528.

[CL07] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. Complexity **23** (2007), no. 3, 380–420.

[CLO97] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, 1997.

[CLO05] ———, *Using algebraic geometry*, second ed., Graduate Texts in Mathematics, Springer-Verlag, 2005.

[CM06a] A. Cafure and G. Matera, *Fast computation of a rational point of a variety over a finite field*, Math. Comp. **75** (2006), no. 256, 2049–2085.

[CM06b] ———, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), no. 2, 155–185.

[CMPSM02] D. Castro, J. L. Montaña, L. M. Pardo, and J. San Martín, *The distribution of condition numbers of rational data of bounded bit length*, Found. Comput. Math. **2** (2002), no. 1, 1–52.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[CPHM01] D. Castro, L. M. Pardo, K. Hägele, and J. E. Morais, *Kronecker's and Newton's approaches to solving: a first comparison*, J. Complexity **17** (2001), no. 1, 212–303.

[CPSM03] D. Castro, L. M. Pardo, and J. San Martín, *Systems of rational polynomial equations have polynomial size approximate zeros on the average*, J. Complexity **19** (2003), no. 2, 161–209.

[Dem85] M. Demazure, *Réécriture et bases standard*, Notes informelles de calcul formel. Centre de Mathématiques, École polytechnique, Palaiseau, France, 1985, `http://www.stix.polytechnique.fr/publications/1984-1994.html`.

[DGP99] W. Decker, G.-M. Greuel, and G. Pfister, *Primary decomposition: algorithms and comparisons*, Algorithmic algebra and number theory, Springer, Berlin, 1999, pp. 187–220.

[DL07] C. Durvye and G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. (2007), doi:10.1016/j.exmath.2007.07.001.

[DLDM05] M. De Leo, E. Dratman, and G. Matera, *Numeric vs. symbolic homotopy algorithms in polynomial system solving: a case study*, J. Complexity **21** (2005), no. 4, 502–531.

[DPS02] W. Decker, G. Pfister, and H. Schönemann, `primedec.lib`, A SINGULAR 2.0.3 library for computing the primary decomposition and radicals of ideals, Centre for Computer Algebra, University of Kaiserslautern, 2002.

[Dur07] C. Durvye, *Evaluation techniques for zero-dimensional primary decomposition*, preprint, 2007.

[Duv94] D. Duval, *Algebraic numbers: an example of dynamic evaluation*, J. Symbolic Comput. **18** (1994), no. 5, 429–445.

[Duv95] ———, *Évaluation dynamique et clôture algébrique en Axiom*, J. Pure Appl. Algebra **99** (1995), no. 5, 267–295.

[DZ05] B. Dayton and Z. Zeng, *Computing the multiplicity structure in solving polynomial systems*, Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 116–123 (electronic).

[EHV92] D. Eisenbud, C. Huneke, and W. Vasconcelos, *Direct methods for primary decomposition*, Inv. Math. **110** (1992), no. 2, 207–235.

[Eis95] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer-Verlag, 1995.

[FGLM93] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner basis by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344.

[FGS95] N. Fitchas, M. Giusti, and F. Smietanski, *Sur la complexité du théorème des zéros*, Approximation and optimization in the Caribbean, II (Havana, 1993), Approx. Optim., vol. 8, Lang, Frankfurt am Main, 1995, pp. 274–329.

[GG03] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003.

[GH93] M. Giusti and J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Computational algebraic geometry and commutative algebra (Cortona, 1991), Sympos. Math., XXXIV, Cambridge Univ. Press, 1993, pp. 216–256.

[GH01] ———, *Kronecker's smart, little black boxes*, Foundations of computational mathematics (Oxford, 1999), London Math. Soc. Lecture Note Ser., vol. 284, Cambridge Univ. Press, 2001, pp. 69–104.

[GHH+97] M. Giusti, K. Hägele, J. Heintz, J. L. Montaña, J. E. Morais, and L. M. Pardo, *Lower bounds for Diophantine approximations*, J. Pure Appl. Algebra **117/118** (1997), 277–317.

[GHL+00] M. Giusti, K. Hägele, G. Lecerf, J. Marchand, and B. Salvy, *The projective Noether Maple package: computing the dimension of a projective variety*, J. Symbolic Comput. **30** (2000), no. 3, 291–307.

[GHM+98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo, *Straight-line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 101–146.

[GHMP95] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo, *When polynomial equation systems can be "solved" fast?*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Lecture Notes in Comput. Sci., vol. 948, Springer-Verlag, 1995, pp. 205–231.

[GHMP97] ———, *Le rôle des structures de données dans les problèmes d'élimination*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 11, 1223–1228.

[GHS93] M. Giusti, J. Heintz, and J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), no. 1, 56–95.

[GLS01] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.

[GLSY05] M. Giusti, G. Lecerf, B. Salvy, and J.-C. Yakoubsohn, *On location and approximation of clusters of zeros of analytic functions*, Found. Comput. Math. **5** (2005), no. 3, 257–311.

[GLSY07] ———, *On location and approximation of clusters of zeros: case of embedding dimension one*, Found. Comput. Math. **7** (2007), no. 1, 1–49.

[GP96] G.-M. Greuel and G. Pfister, *Advances and improvements in the theory of standard bases and syzygies*, Arch. Math. (Basel) **66** (1996), no. 2, 163–176.

[GP02] ———, *A Singular introduction to commutative algebra*, Springer-Verlag, Berlin, 2002.

[GPS05] G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR *3.0*, A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005, `http://www.singular.uni-kl.de`.

[GS99] M. Giusti and É. Schost, *Solving some overdetermined polynomial systems*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation, ACM, 1999, pp. 1–8.

[GS05] P. Gaudry and É. Schost, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), no. 249, 429–454.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), no. 2-3, 149–167.

[GWW07] S. Gao, D. Wan, and M. Wang, *Primary decomposition of zero-dimensional ideals over finite fields*, To appear in Mathematics of Computation, 2007.

[Häg98] K. Hägele, *Intrinsic height estimates for the Nullstellensatz*, Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1998.

[HKP+00] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), no. 1, 70–109.

[HMPS00] K. Hägele, J. E. Morais, L. M. Pardo, and M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz*, J. Pure Appl. Algebra **146** (2000), no. 2, 103–183.

[HMPW98] J. Heintz, G. Matera, L. M. Pardo, and R. Wachenchauzer, *The intrinsic complexity of parametric elimination methods*, Electronic J. of SADIO **1** (1998), no. 1, 37–51.

[HMW01] J. Heintz, G. Matera, and A. Waissbein, *On the time-space complexity of geometric elimination procedures*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 4, 239–296.

[JKSS04] G. Jeronimo, T. Krick, J. Sabia, and M. Sombra, *The computational complexity of the Chow form*, Found. Comput. Math. **4** (2004), no. 1, 41–117.

[JMSW06] G. Jeronimo, G. Matera, P. Solerno, and A. Waissbein, *Deformation techniques for sparse systems*, `arXiv:math/0608714v1`, 2006.

[JPS01] G. Jeronimo, S. Puddu, and J. Sabia, *Computing Chow forms and some applications*, J. Algorithms **41** (2001), no. 1, 52–68.

[JS00] G. Jeronimo and J. Sabia, *Probabilistic equidimensional decomposition*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), no. 6, 485–490.

[JS02] ———, *Effective equidimensional decomposition of affine varieties*, J. Pure Appl. Algebra **169** (2002), no. 2-3, 229–248.

[Kan85] R. Kannan, *Solving systems of linear equations over polynomials*, Theoret. Comput. Sci. **39** (1985), no. 1, 69–88.

[KKS90] E. Kaltofen, M.-S. Krishnamoorthy, and B. Saunders, *Parallel algorithms for matrix normal forms*, Linear Algebra Appl. **136** (1990), 189–208.

[KL91] T. Krick and A. Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 539, Springer, 1991, pp. 195–205.

[KP96] T. Krick and L. M. Pardo, *A computational method for Diophantine approximation*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., vol. 143, Birkhäuser, 1996, pp. 193–253.

[KPS01] T. Krick, L.-M. Pardo, and M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), no. 3, 521–598.

[Kro82] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. reine angew. Math. **92** (1882), 1–122.

[Lan02] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, 2002.

[Lec] G. Lecerf, *`Kronecker`, a `Magma` package for polynomial system solving*, `http://www.math.uvsq.fr/~lecerf`.

[Lec00] G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, ACM, 2000, pp. 209–216.

[Lec01] G. Lecerf, *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques*, Ph.D. thesis, École polytechnique, Palaiseau, France, 2001.

[Lec02] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity*, Found. Comput. Math. **2** (2002), no. 3, 247–293.

[Lec03] ———, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596.

[Lec06] G. Lecerf, *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. Comp. **75** (2006), 921–933.

[Lec07] ———, *Improved dense multivariate polynomial factorization algorithms*, J. Symbolic Comput. **42** (2007), no. 4, 477–494.

[Leh04] L. Lehmann, *Polar varieties, real elimination and wavelet design*, 2004, Talk given at Dagstuhl Seminar 04061 on Real Computation and Complexity.

[Ley08] A. Leykin, *Numerical primary decomposition*, `arXiv:math/0801.3105v1`, 2008.

[LVZ06] A. Leykin, J. Verschelde, and A. Zhao, *Newton's method with deflation for isolated singularities of polynomial systems*, Theoret. Comput. Sci. **359** (2006), no. 1-3, 11–122.

[Mal03] S. Mallat, *Foveal detection and approximation for singularities*, Appl. Comput. Harmon. Anal. **14** (2003), no. 2, 133–180.

[Mat99] G. Matera, *Probabilistic algorithms for geometric elimination*, Appl. Algebra Engrg. Comm. Comput. **9** (1999), no. 6, 463–520.

[MMM96] M.-G. Marinari, H.-M. Möller, and T. Mora, *On multiplicities in polynomial system solving*, Trans. Amer. Math. Soc. **348** (1996), no. 8, 3283–3321.

[Mon02] C. Monico, *Computing the primary decomposition of zero-dimensional ideals*, J. Symbolic Comput. **34** (2002), no. 5, 451–459.

[Mor91] T. Mora, *La queste del Saint* $\mathrm{Gr}_a(AL)$*: a computational approach to local algebra*, Discrete Appl. Math. **33** (1991), no. 1-3, 161–190.

[Mor97] J. E. Morais, *Resolución eficaz de sistemas de ecuaciones polinomiales*, Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1997.

[Mor03] T. Mora, *Solving polynomial equation systems. I The Kronecker-Duval philosophy*, Encyclopedia of Mathematics and its Applications, vol. 88, Cambridge University Press, 2003.

[Mou97] B. Mourrain, *Isolated points, duality and residues*, J. Pure Appl. Algebra **117/118** (1997), 469–493.

[MS03] T. Mulders and A. Storjohann, *On lattice reduction for polynomial matrices*, J. Symbolic Comput. **35** (2003), no. 4, 377–401.

[Par95] L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Lecture Notes in Comput. Sci., vol. 948, Springer-Verlag, 1995, pp. 33–69.

[PSM04] L. M. Pardo and J. San Martín, *Deformation techniques to solve generalised Pham systems*, Theoret. Comput. Sci. **315** (2004), no. 2-3, 593–625.

[Rou99] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Appl. Algebra Engrg. Comm. Comput. **9** (1999), no. 5, 433–461.

[Saf05] M. Safey El Din, *Finding sampling points on real hypersurfaces is easier in singular situations*, Proceedings of Effective Methods in Algebraic Geometry, 2005.

[Sch03] É. Schost, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 349–393.

[Sei74] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.

[Sei78] _____, *Constructions in a polynomial ring over the ring of integers*, Amer. J. Math. **100** (1978), no. 4, 685–703.

[Sei84] _____, *On the Lasker-Noether decomposition theorem*, Amer. J. Math. **106** (1984), no. 3, 611–638.

[Sha94] I. R. Shafarevich, *Basic algebraic geometry. 1 Varieties in projective space*, second ed., Springer-Verlag, 1994.

[SS04] M. Safey El Din and É. Schost, *Properness defects of projections and computation of at least one point in each connected component of a real algebraic set*, Discrete Comput. Geom. **32** (2004), no. 3, 417–430.

[Ste05] A. Steel, *Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic*, J. Symbolic Comput. **40** (2005), no. 3, 1053–1075.

[Sto94] A. Storjohann, *Computation of Hermite and Smith normal forms of matrices*, Master's thesis, Waterloo, Ontario, Canada, 1994, http://www.cs.uwaterloo.ca/ astorjoh/publications.html.

[SVW05] A. J. Sommese, J. Verschelde, and C. W. Wampler, *Solving polynomial systems equation by equation*, To appear in the IMA Volume on Algorithms in Algebraic Geometry, 2005.

[SY96] T. Shimoyama and K. Yokoyama, *Localization and primary decomposition of polynomial ideals*, J. Symbolic Comput. **22** (1996), no. 3, 247–277.

[Vil93] G. Villard, *Computation of the Smith normal form of polynomial matrices*, Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ACM, 1993, pp. 209–217.

[Vil94] ———, *Fast parallel computation of the Smith normal form of polynomial matrices*, Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation, ACM, 1994, pp. 312–317.

[Vil95] ———, *Generalized subresultants for computing the Smith normal form of polynomial matrices*, J. Symbolic Comput. **20** (1995), no. 3, 269–286.

[Wan04] D. Wang, *Elimination practice. Software tools and applications*, Imperial College Press, London, 2004.

Résumé

Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation

Les algorithmes de résolution polynomiale sont impliqués dans des outils sophistiqués de calcul en géométrie algébrique aussi bien qu'en ingénierie. Les plus populaires d'entre eux reposent sur des bases de Gröbner, des matrices de Macaulay ou des décompositions triangulaires. Dans tous ces algorithmes, les polynômes sont développés dans une base des monômes et les calculs utilisent essentiellement des routines d'algèbre linéaire. L'inconvénient majeur de ces méthodes est l'explosion exponentielle du nombre de monômes apparaissant dans des polynômes éliminants. De manière alternative, l'algorithme *Kronecker* manie des polynômes codés comme la fonction qui calcule ses valeurs en tout point.

Dans cette thèse, nous donnons une présentation concise de ce dernier algorithme, ainsi qu'une preuve autonome de son bon fonctionnement. Toutes nos démonstrations sont intimement liées aux algorithmes, et ont pour conséquence des résultats classiques en géométrie algébrique, comme un théorème de Bézout. Au delà de leur intérêt pédagogique, ces preuves permettent de lever certaines hypothèses de régularité, et donc d'étendre l'algorithme au calcul des multiplicités sans coût supplémentaire.

Enfin, nous présentons un algorithme de décomposition primaire pour les idéaux de polynômes de dimension nulle. Nous en donnons également une étude de complexité précise, complexité qui est polynomiale en le nombre de variables, en le coût d'évaluation du système, et en un nombre de Bézout.

Mots clefs : algorithme, résolution polynomiale, décomposition primaire, complexité, géométrie algébrique effective.

Abstract

Algorithms for primary decomposition of zero-dimensional polynomials ideals given by an evaluation structure

Nowadays, polynomial system solvers are involved in sophisticated computations in algebraic geometry as well as in practical engineering. The most popular algorithms are based on Gröbner bases, resultants, Macaulay matrices, or triangular decompositions. In all these algorithms, multivariate polynomials are expanded in a monomial basis, and the computations mainly reduce to linear algebra. The major drawback of these techniques is the exponential explosion of the size of eliminant polynomials. Alternatively, the *Kronecker* solver uses data structures to represent the input polynomials as the functions that compute their values at any given point.

In this PhD thesis we give a concise presentation of the Kronecker solver, with a self-contained proof of correctness. Our proofs closely follow the algorithms, and as consequences, we obtain some classical results in algebraic geometry such as a Bézout Theorem. Beyond their pedagogical interest, these new proofs allow us to discard some regularity hypotheses, and so to enhance the solver in order to compute the multiplicities of the zeros without any extra cost.

At last, we design a new algorithm for primary decomposition of a zero-dimensional polynomial ideal. We also give a cost analysis of this algorithm, which is polynomial in the number of variables, in the evaluation cost of the input system, and in a Bézout number.

Keyword: algorithm, polynomial solving, primary decomposition, complexity, effective algebraic geometry.