MATHÉMATIQUES
&
APPLICATIONS

Directeurs de la collection :
G. Allaire et M. Benaïm

59

MATHÉMATIQUES & APPLICATIONS

Comité de Lecture / Editorial Board

Directeurs de la collection :
G. ALLAIRE et M. BENAÏM

Instructions aux auteurs :

Les textes ou projets peuvent être soumis directement à l'un des membres du comité de lecture avec copie à G. ALLAIRE OU M. BENAÏM. Les manuscrits devront être remis à l'Éditeur sous format LaTeX2e.

Mohamed Elkadi
Bernard Mourrain

Introduction à la résolution des systèmes polynomiaux

Springer

Mohamed Elkadi

Laboratoire J.A. Dieudonné
Université de Nice Sophia Antipolis
Parc Valrose
06108 Nice cedex
France
e-mail: Mohamed.Elkadi@unice.fr

Bernard Mourrain

Project GALAAD, INRIA
2004 routes deś lucioles
B.P. 93
06902 Sophia Antipolis cedex
France
e-mail: Bernard.Mourrain@sophia.inria.fr

Library Congress Control Number: 2007925261

Mathematics Subject Classification (2000): 13P10, 68Q40, 14Q20, 65F15, 08-0, 14-01, 68-01

ISSN 1154-483X
ISBN-10 3-540-71646-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-71646-4 Springer Berlin Heidelberg New York

springer.com
WMXDesign GmbH

Imprimé sur papier non acide 3100/SPi - 5 4 3 2 1 0 -

Table des matières

Introduction

Les équations polynomiales sont présentes dans de nombreux domaines. Elles interviennent pour modéliser des contraintes géométriques, des relations entre des grandeurs physiques, des propriétés satisfaites par certaines inconnues ... Voici quelques exemples de tels domaines.

Biologie moléculaire. — Si les distances entre deux atomes consécutifs et les angles entre deux liaisons consécutives d'une molécule à 6 atomes sont connus, quelles sont les configurations possibles de celle-ci ?

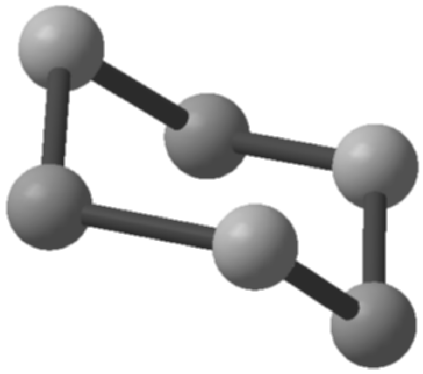

FIGURE 1. Molécule de cyclohexane.

Robotique. — Considérons un robot parallèle, c'est-à-dire une plate-forme rigide reliée à un socle par 6 bras extensibles, et fixés par des rotules au socle et à la plate-forme. Supposons que l'on détache ces 6 bras de la plate-forme (par exemple pour changer une pièce). Une fois cette opération effectuée, il faut rattacher les bras, aux mêmes endroits sur la plate-forme, mais rien ne nous garantit que la plate-forme sera dans la même position. Combien de positions possibles de la plate-forme, existe-t-il satisfaisant les contraintes de distances, imposées par ces bras ?

FIGURE 2. Un robot parallèle.

Vision. — Une caméra (calibrée) en mouvement prend une photographie d'une même scène (par exemple une maison) à deux instants différents. Dans ces deux photographies, on peut reconnaître un certain nombre de paires de points qui se correspondent, d'une image à l'autre. Par exemple, un coin de fenêtre peut être visible dans les deux images. Ceci nous fournit une paire de points (un dans chaque image), que l'on dit en correspondance.

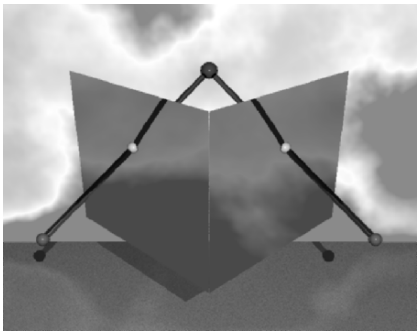

FIGURE 3. Points en correspondance dans deux images.

Quel est le nombre minimal nécessaire de paires de points en correspondance pour qu'il y ait un nombre fini de déplacements possibles entre les deux photos ? Dans ce cas, quel est le nombre maximal de déplacements de la caméra ?

Géométrie algorithmique. — Pour la construction d'un diagramme (dit de Voronoï), il est nécessaire de pouvoir déterminer si un point est à l'intérieur ou à l'extérieur d'un cercle tangent à trois segments.

Comment peut-on s'y prendre sans calcul explicite de ce cercle ? Quelle précision doit-on utiliser pour garantir le résultat, si les calculs se font de manière approchée ?

Ces problèmes se traduisent par des systèmes polynomiaux. Dans ce cours, nous nous intéresserons à des méthodes et outils permettant de les résoudre. Nous présenterons certains aspects de la géométrie algébrique effective, en considérant avec une attention particulière les variétés algébriques de dimension 0 (i.e. les systèmes d'équations polynomiales qui définissent un nombre fini de points). Pour cette étude, préliminaire à l'analyse des variétés en dimension supérieure, nous commençerons par rappeler le dictionnaire entre l'algèbre et la géométrie. Le « leitmotiv » est le suivant : *les propriétés algébriques permettent de comprendre la géométrie des solutions.* Nous nous intéresserons à certains invariants tels que la dimension et le degré d'une variété algébrique.

Pour résoudre les problèmes cités ci-dessus, nous commençerons par *nommer les inconnues, puis définir les contraintes et travailler modulo les relations qu'elles engendrent.* Ceci conduit à l'étude des algèbres quotients. Nous considérerons en particulier les quotients de dimension 0, qui correspondent aux systèmes d'équations ayant un nombre fini de solutions. Nous introduirons les techniques de bases de Gröbner, et nous montrerons comment *la résolution algébrique se transforme en un calcul de valeurs et de vecteurs propres.*

En suite, nous analyserons certaines classes spécifiques de problèmes, en commençant par le cas des systèmes ayant plus d'équations que d'inconnues. Ceci nous amènera à l'étude de la théorie des résultants. Nous verrons comment détecter si un système polynomial admet des solutions, puis analyser, localiser et déterminer ces dernières. L'autre classe de problèmes concerne les systèmes ayant autant d'équations que d'inconnues. Nous développerons les propriétés des quotients associés à ce type de systèmes et à leurs duaux. Pour cela, nous définirons la notion des résidus et étudierons leurs applications dans les problèmes de représentation et de résolution algébrique.

Des exemples de problèmes et de calculs effectifs accompagneront ces développements. Nous avons utilisé pour cela, le package maple `multires`[(1)]. Nous encourageons le lecteur à l'utiliser pour mettre en pratique, les notions que nous abordons.

Cette publication est le fruit de cours donnés pendant plusieurs années au DEA de Mathématiques de l'Université de Nice Sophia Antipolis. Nous remercions toutes les personnes qui nous ont aidé de près ou de loin dans sa

(1) voir `http ://www-sop.inria.fr/galaad/logiciel/multires`

réalisation, spécialement André Galligo et Laurent Busé qui ont bien voulu lire une première version de ce manuscrit et Marie-Françoise Coste-Roy pour l'intérêt constant qu'elle a apporté à ce travail.

CHAPITRE 1

ÉQUATIONS, IDÉAUX, VARIÉTÉS

Sommaire

Dans ce chapitre, nous introduisons les objets que nous allons étudier tout au long de ce cours : les idéaux de polynômes et les variétés algébriques. Nous rappelons la correspondance entre l'algèbre et la géométrie, la décomposition primaire d'un idéal et définissons quelques invariants utiles pour la suite.

1.1. Polynômes

Dans beaucoup de domaines (robotique, vision par ordinateur, géométrie algorithmique, théorie des nombres, mathématiques financières, théorie des jeux, biologie moléculaire, statistique ...), la modélisation conduit souvent à la résolution de systèmes polynomiaux. Les grandeurs sont représentées par des variables vérifiant des contraintes polynomiales qui, si possible, caractérisent les solutions du problème. Ces variables sont notées $x_1, \ldots, x_n$ et ces contraintes $f_1 = 0, \ldots, f_m = 0$.

Problème :

Nous considérons une caméra calibrée[1] *qui observe une scène tridimensionnelle, dans laquelle trois points A, B, C sont reconnus. Nous voulons déterminer la position de la caméra à partir de ces observations.*

Pour cela, nous allons déterminer les contraintes vérifiées par les distances x_1, x_2, x_3 entre le centre de la caméra X et respectivement A, B, C. Puis à partir de ces distances, nous allons déduire la position de X par rapport à ces points. Comme la caméra est calibrée, nous pouvons à partir de mesures des distances entre les images des points A, B, C, déduire les angles entre les rayons optiques XA, XB, XC (voir figure 1.1).

Notons α l'angle entre XB et XC, β l'angle entre XA et XC, γ l'angle entre XA et XB. Supposons que ces angles et les distances a entre B et C, b entre A et C, c entre A et B sont connus. De simples relations trigonométriques dans un triangle conduisent aux équations suivantes :

$$\begin{cases} x_1^2 + x_2^2 - 2\cos(\gamma)x_1x_2 - c^2 = 0 \\ x_1^2 + x_3^2 - 2\cos(\beta)x_1x_3 - b^2 = 0 \\ x_2^2 + x_3^2 - 2\cos(\alpha)x_2x_3 - a^2 = 0. \end{cases} \tag{1.1}$$

Dans ce chapitre, nous allons étudier ce système et l'utiliser pour illustrer les différentes notions que nous allons introduire.

Les contraintes $f_1 = 0, \ldots, f_m = 0$ sont à coefficients entiers, entiers modulo un nombre premier, rationnels, réels, complexes, ou encore des fractions

[1] sa distance focale et les coordonnées de la projection du centre optique dans l'image sont connues.

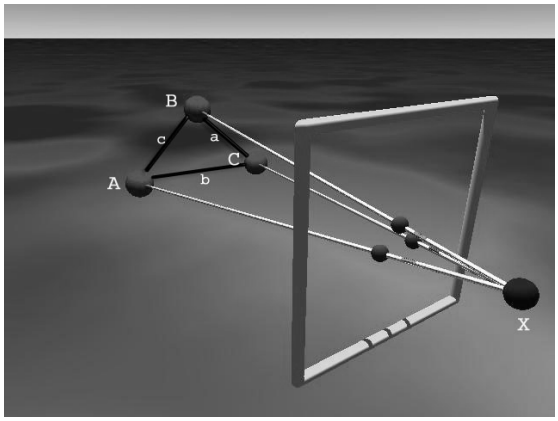

FIGURE 1.1. Modélisation mathématique d'une caméra.

rationnelles en certains paramètres. Désignons par $\mathbb{K}$ un *corps* contenant ces coefficients et par $\overline{\mathbb{K}}$ sa *clôture algébrique*. Les relations $f_1, \ldots, f_m$ entre les variables $x_1, \ldots, x_n$, appartiennent donc à l'anneau des polynômes $\mathbb{K}[x_1, \ldots, x_n]$, noté également $\mathbb{K}[\mathbf{x}]$. Parfois, dans le cas d'une variable (resp. deux ou trois variables), nous utilisons la notation $\mathbb{K}[x]$ (resp. $\mathbb{K}[x, y]$ ou $\mathbb{K}[x, y, z]$). Les monômes sont notés $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ pour $\alpha = (\alpha_1, \ldots, x_n) \in \mathbb{N}^n$. Le degré de $\mathbf{x}^\alpha$ est $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Pour représenter les éléments de $\mathbb{K}[\mathbf{x}]$, nous ordonnons les monômes suivant un ordre total. Les polynômes sont donc des listes ordonnées de termes définis par des coefficients et des exposants. Le degré d'un polynôme est le maximum des degrés des monômes à coefficients non nuls qui le constituent. Ainsi, nous étendons aux polynômes multivariables, les notions de *coefficient dominant*, *monôme dominant* et *terme dominant*, une fois que l'ordre sur les monômes est fixé. Par convention, le coefficient dominant, le monôme dominant et le terme dominant du polynôme nul sont nuls.

A partir de l'ensemble de contraintes $f_1 = 0, \ldots, f_m = 0$, nous en construisons d'autres, celles définies par l'*idéal de* $\mathbb{K}[\mathbf{x}]$ *engendré* par $f_1, \ldots, f_m$.

On peut se demander si tout idéal de $\mathbb{K}[\mathbf{x}]$ est engendré par un nombre fini de polynômes.

***Définition* 1.1.** *Un anneau A commutatif et unitaire est dit* noethérien *si tout idéal de A est engendré par un nombre fini d'éléments.*

***Proposition* 1.2.** *Les propriétés suivantes sont équivalentes dans un anneau commutatif et unitaire A :*

i) Tout idéal de A est engendré par un nombre fini d'éléments,

ii) Toute suite croissante d'idéaux de A est stationnaire,
iii) Tout ensemble d'idéaux de A admet un élément maximal.

Démonstration. Voir exercice 1.2. □

***Théorème* 1.3.** *L'anneau $\mathbb{K}[\mathbf{x}]$ est noethérien.*

Démonstration. Cette preuve est similaire à celle proposée par Hilbert dans ses célèbres travaux sur la théorie des invariants [**Hil93**].

Comme les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$, l'anneau $\mathbb{K}$ est noethérien. Nous procédons par récurrence sur le nombre de variables n. Pour cela, il suffit de montrer que si A est un anneau noethérien, alors $A[x]$ (où x est une nouvelle variable) l'est aussi.

Soit I un idéal de $A[x]$. L'ensemble J des coefficients dominants des éléments de I est un idéal de A. Il est donc engendré par un nombre fini d'éléments non nuls $c_1, \ldots, c_s$. Notons $f_1, \ldots, f_s$ des éléments de I dont les coefficients dominants sont respectivement $c_1, \ldots, c_s$.

Soit $f \in I$ de degré $\delta \geq d = \max \deg f_i$ et de coefficient dominant c. Nous avons $c = \sum_{i=1}^{s} c_i\, r_i$, avec $r_i \in A$. L'élément

$$f - \sum_{i=1}^{s} r_i\, x^{\delta - \deg f_i} f_i$$

de I est de degré $< \delta$. Nous pouvons donc réécrire tout polynôme de I modulo $f_1, \ldots, f_s$ en un élément de I de degré $< d$.

Pour chaque $i \in \{0, \ldots, d-1\}$, soit J_i l'ensemble des coefficients dominants des polynômes de I de degré i. Comme J_i est un idéal de A, il est donc engendré par un nombre fini d'éléments non nuls $c_{i,1}, \ldots, c_{i,k_i}$. Notons $f_{i,1}, \ldots, f_{i,k_i}$ des polynômes de I de degré i dont les coefficients dominants sont respectivement $c_{i,1}, \ldots, c_{i,k_i}$. Le même argument que précédemment montre que tout $f \in I$ de degré $d > i$ se réduit modulo $f_{i,1}, \ldots, f_{i,k_i}$ en un élément de I de degré $< i$. Ceci montre que l'idéal I est engendré par $f_1, \ldots, f_s$ et $f_{i,1}, \ldots, f_{i,k_i}$, $i = 0, \ldots, d-1$. □

Dans le cas d'une variable, nous avons un résultat plus fort :

***Proposition* 1.4.** *Tout idéal de $\mathbb{K}[x]$ est engendré par un seul polynôme.*

Démonstration. Voir exercice 1.1. □

1.2. Solutions

L'objet principal de ce cours est l'étude de l'ensemble des solutions d'un système d'équations polynomiales F de $\mathbb{K}[\mathbf{x}]$; c'est-à-dire l'ensemble $\mathcal{Z}_{\mathbb{K}}(F)$

(ou $\mathcal{Z}(F)$ s'il n'y a pas d'ambiguïté sur le corps $\mathbb{K}$) des points ζ de $\mathbb{K}^n$ qui vérifient $f(\zeta) = 0$ pour tout $f \in F$. Un tel ensemble est appelé une *variété algébrique* de $\mathbb{K}^n$. Nous considérons souvent $\mathcal{Z}_{\overline{\mathbb{K}}}(F)$, l'ensemble des solutions de F dans $\overline{\mathbb{K}}^n$ au lieu de $\mathcal{Z}_{\mathbb{K}}(F) \subset \mathbb{K}^n$.

Les polynômes $f_1, \ldots, f_m$ définissent le même ensemble de solutions que l'idéal I qu'ils engendrent : $\mathcal{Z}_{\mathbb{K}}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{K}}(I)$.

Il est facile de vérifier que la réunion finie et l'intersection quelconque de variétés algébriques sont des variétés algébriques. De plus, $\emptyset = \mathcal{Z}(\mathbb{K}[\mathbf{x}])$ et $\mathbb{K}^n = \mathcal{Z}(\{0\})$ sont des variétés algébriques. Donc les variétés algébriques sont les fermés d'une *topologie* définie sur $\mathbb{K}^n$, dite de *Zariski*. Elle est non-séparée si le corps $\mathbb{K}$ est infini (i.e. si $x \neq y$, il n'existe pas deux ouverts disjoints contenant respectivement x et y).

Si V est une variété algébrique, une *sous-variété algébrique* de V est une variété algébrique incluse dans V.

***Définition* 1.5.** *Une variété algébrique V est dite irréductible si $V = V_1 \cup V_2$, avec V_1 et V_2 deux sous-variétés de V, alors $V_1 = \emptyset$ ou $V_2 = \emptyset$.*

***Proposition* 1.6.** *Toute variété algébrique V se décompose de manière unique en une réunion finie de sous-variétés algébriques irréductibles de V, appelées composantes irréductibles de V.*

Démonstration. Voir exercice 1.5. □

Problème(suite) :

Pour le problème de positionnement de la caméra , nous allons dans un premier temps considérer toutes les solutions (x_1, x_2, x_3) à coordonnées complexes du système (1.1). Puis nous nous restreindrons à celles dont les coordonnées sont réelles et positives, qui correspondent à une position physique de la caméra.

Cette démarche est classique. L'étude algébrique des systèmes polynomiaux, issus des domaines d'applications, fournit des informations sur toutes les solutions dont les coordoonnées appartiennent à la clôture algébrique du corps des coefficients des équations. Les informations sur les « vraies » solutions du problème étudié sont obtenues par une analyse « physique » de celui-ci (par exemple, dans ce problème, en prenant en compte les signes des variables x_i).

La formule de résolution des équations du second degré appliquée aux deux premières équations de (1.1) permet d'exprimer x_2 et x_3 en fonction de x_1. En substituant x_2 et x_3 dans la dernière équation et en « chassant » les radicaux, nous obtenons une équation de degré 8 en x_1 (sauf dans des cas dégénérés). Cette dernière admet 8 solutions complexes, et par conséquent, il y a au plus 16 positions possibles (symétriques par rapport au plan défini par A, B, C)

pour le centre X de la caméra.

1.3. Correspondance entre l'algèbre et la géométrie

Pour résoudre le système $f_1 = \cdots = f_m = 0$, l'approche algébrique consiste à considérer que les inconnues $x_1, \ldots, x_n$ vérifient ces équations et toutes celles qui s'en déduisent. En d'autres termes, on se place dans l'algèbre quotient $\mathcal{A}=\mathbb{K}[\mathbf{x}]/I$, où I désigne l'idéal engendré par $f_1, \ldots, f_m$. L'étude des propriétés de cette algèbre permet de déduire des informations pertinentes sur l'ensemble des solutions $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$. Nous allons analyser cette correspondance entre l'algèbre des polynômes (i.e. les idéaux de $\mathbb{K}[\mathbf{x}]$) et la géométrie (i.e. les variétés algébriques de $\mathbb{K}^n$).

***Définition* 1.7.** *Soit Y une partie de $\mathbb{K}^n$. On définit*

$$\mathcal{I}(Y) = \{f \in \mathbb{K}[\mathbf{x}] \ : f(a) = 0, \forall a \in Y\}.$$

L'ensemble $\mathcal{I}(Y)$ est un idéal de $\mathbb{K}[\mathbf{x}]$, appelé l'idéal de Y. D'après le théorème 1.3, il est engendré par un nombre fini d'éléments.

***Proposition* 1.8.** *Si Y et Z sont deux sous-ensembles de $\mathbb{K}^n$, alors*

$$\mathcal{I}(Y \cup Z) = \mathcal{I}(Y) \cap \mathcal{I}(Z).$$

Démonstration. Voir exercice 1.4. □

***Définition* 1.9.** *Un idéal I de $\mathbb{K}[\mathbf{x}]$ est dit premier si*

$$\forall\, (f, g) \in \mathbb{K}[\mathbf{x}]^2 \ , \ fg \in I \Longrightarrow f \in I \text{ ou } \ \mathrm{g} \in \mathrm{I}.$$

La proposition suivante montre l'importance de la notion d'idéal premier.

***Proposition* 1.10.** *Une variété algébrique V est irréductible si, et seulement si, son idéal $\mathcal{I}(V)$ est premier.*

Démonstration. Voir exercice 1.4. □

Il est facile de vérifier que si V est une variété, alors $\mathcal{Z}(\mathcal{I}(V)) = V$. Mais la question « réciproque » : si I est un idéal de $\mathbb{K}[\mathbf{x}]$, « quel est l'idéal $\mathcal{I}(\mathcal{Z}(I))$? » est plus délicate. Une réponse partielle est donnée grâce au *théorème fondamental de l'algèbre : tout polynôme d'une variable de degré d et à coefficients dans $\mathbb{K}$ admet d racines dans $\overline{\mathbb{K}}$ (chaque racine est comptée autant de fois que sa multiplicité).* Donc si $f \in \mathbb{K}[x]$, alors $f = \alpha \prod_{i=1}^{k} (x - z_i)^{m_i}$, où

$\alpha \in \mathbb{K} \setminus \{0\}, m_i \in \mathbb{N}^*, z_i \in \overline{\mathbb{K}}$, et $z_i \neq z_j$ pour $i \neq j$. Nous pouvons vérifier que

$$\mathcal{I}(\mathcal{Z}(f)) = \Big(\prod_{i=1}^{k}(x - z_i)\Big) = \Big(\frac{f}{\mathrm{pgcd}(f, \frac{df}{dx})}\Big).$$

Le polynôme $\prod_{i=1}^{k}(x - z_i)$ est à coefficients dans $\mathbb{K}$.

La réponse à la question précédente, dans le cas multivariable, est donnée par le *théorème des zéros de Hilbert*.

***Définition* 1.11.** *Un idéal $I \neq \mathbb{K}[\mathbf{x}]$ est dit maximal si pour tout idéal J tel que $I \subset J$, on a $J = I$ ou $J = \mathbb{K}[\mathbf{x}]$.*

Notons qu'un idéal I de $\mathbb{K}[\mathbf{x}]$ est maximal si, et seulement si, $\mathbb{K}[\mathbf{x}]/I$ est un corps (voir exercice 1.12).

Si $(a_1, \ldots, a_n) \in \mathbb{K}^n$, l'idéal $(x_1 - a_1, \ldots, x_n - a_n)$ est maximal et nous allons voir que si le corps $\mathbb{K}$ est algébriquement clos, tout idéal maximal de $\mathbb{K}[\mathbf{x}]$ est de cette forme.

***Définition* 1.12.** *Soient B un anneau et A un sous-anneau de B. Un élément $b \in B$ est dit entier sur A si b est racine d'une équation d'une variable de la forme $x^m + a_1 x^{m-1} + \cdots + a_m \in A[x]$.*

L'anneau B est une extension entière de A si tout élément de B est entier sur A.

***Lemme* 1.13.** *Soient A, B, C trois anneaux tels que $A \subset B \subset C$ tels que l'extension B de A est entière. Alors tout élément $c \in C$ entier sur B est aussi entier sur A.*

Démonstration. Voir exercice 1.10. □

***Lemme* 1.14.** *Soient B un anneau intègre et A un sous-anneau de B tels que l'extension $A \subset B$ est entière. Alors A est un corps si, et seulement si, B est un corps.*

Démonstration. Supposons que A est un corps et soit $b \in B \setminus \{0\}$. Il existe $m \in \mathbb{N}$ et $(a_1, \ldots, a_m) \in A^m$ tels que $b^m + a_1 b^{m-1} + \cdots + a_m = 0$. Comme B est intègre, on peut supposer que $a_m \neq 0$, donc inversible dans A. Il en découle que $1 = b(-a_m^{-1} b^{m-1} - \cdots - a_m^{-1} a_{m-1})$. Ainsi, b est inversible dans B.

Réciproquement, supposons que B est un corps et soit $a \in A \setminus \{0\}$. L'élément a est inversible dans B, et a^{-1} vérifie $a^{-m} + a_1 a^{1-m} + \cdots + a_m = 0$, avec $m \in \mathbb{N}$ et $(a_1, \ldots, a_m) \in A^m$. Nous en déduisons que $a(-a_m a^{m-1} - \cdots - a_1) = 1$, et donc a est inversible dans A. □

***Lemme* 1.15.** *Soit A un anneau de type fini sur un corps K (i.e. $A = K[a_1, \ldots, a_m]$, avec $a_1, \ldots, a_m \in A$). Alors il existe des éléments $b_1, \ldots, b_r$ de*

A algébriquement indépendants sur K tels que l'extension $K[b_1, \ldots, b_r] \subset A$ est entière.

Rappelons que les éléments $b_1, \ldots, b_r$ de A sont algébriquement indépendants sur K si le seul polynôme f à coefficients dans K qui satisfait $f(b_1, \ldots, b_r) = 0$ est le polynôme nul.

Démonstration. Supposons que $a_1, \ldots, a_m$ sont algébriquement liés sur K, i.e. $(a_1, \ldots, a_m)$ est solution d'un polynôme non nul $f \in K[x_1, \ldots, x_m]$. Soit $r \in \mathbb{N}$ et pour $i = 2, \ldots, m$, posons $c_i = a_i - a_1^{r^{i-1}}$. Chaque monôme $a_1^{\alpha_1} \ldots a_m^{\alpha_m}$ de $f(a_1, \ldots, a_m)$ s'écrit sous la forme $a_1^{\alpha_1 + r\alpha_2 + \cdots + r^{m-1}\alpha_m} + g(a_1, c_2, \ldots, c_m)$, où g est un polynôme de degré inférieur strictement à $\alpha_1 + r\alpha_2 + \cdots + r^{m-1}\alpha_m$. Choisissons l'entier r tel que toutes les expresssions $\alpha_1 + r\alpha_2 + \cdots + r^{m-1}\alpha_m$ soient différentes pour les différents multi-indices $(\alpha_1, \ldots, \alpha_m)$ des monômes de $f(a_1, \ldots, a_m)$. Ainsi, a_1 est entier sur $K[c_2, \ldots, c_m]$. En itérant ce procédé et en utilisant le lemme 1.13, nous construisons $b_1, \ldots, b_r$ tels que A soit une extension entière de $K[b_1, \ldots, b_r]$. □

***Théorème* 1.16.** *Soit $\mathbb{K}$ un corps algébriquement clos (i.e. $\overline{\mathbb{K}} = \mathbb{K}$). Alors tout idéal maximal de $\mathbb{K}[\mathbf{x}]$ est de la forme $\mathfrak{m}_\zeta = (x_1 - \zeta_1, \ldots, x_n - \zeta_n)$, avec $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{K}^n$.*

Démonstration. Soit $\mathfrak{m}$ un idéal maximal. L'anneau de type fini $K = \mathbb{K}[\mathbf{x}]/\mathfrak{m}$ est un corps. D'après le lemme 1.15, il existe $(b_1, \ldots, b_r) \in K^r$ tel que l'extension $\mathbb{K}[b_1, \ldots, b_r] \subset K$ est entière. En utilisant le lemme 1.14, nous déduisons que $\mathbb{K}[b_1, \ldots, b_r]$ est un corps et donc $r = 0$. Par conséquent, l'extension de corps $\mathbb{K} \subset K$ est algébrique, et comme $\mathbb{K}$ est algébriquement clos, $K = \mathbb{K}$.

Considérons l'application $f \in \mathbb{K}[\mathbf{x}] \mapsto \overline{f} \in \mathbb{K}[\mathbf{x}]/\mathfrak{m} = K = \mathbb{K}$. Pour $i = 1, \ldots, n$, notons $\zeta_i = \overline{x_i}$. Nous avons $(x_1 - \zeta_1, \ldots, x_n - \zeta_n) \subset \mathfrak{m}$, et donc $(x_1 - \zeta_1, \ldots, x_n - \zeta_n) = \mathfrak{m}$.

□

Il existe plusieurs preuves du théorème 1.16 dans la littérature, dont une utilisant le résultant de Sylvester (voir [**CLO92**], [**BM04**]).

Le résultat suivant est une conséquence directe du théorème 1.16.

***Théorème* 1.17.** *Soit $\mathbb{K}$ un corps algébriquement clos. Si V est une variété algébrique de $\mathbb{K}^n$, alors $\mathcal{I}(V) = \mathbb{K}[\mathbf{x}]$ si et seulement si $V = \emptyset$.*

Démonstration. Si l'idéal $\mathcal{I}(V) = \mathbb{K}[\mathbf{x}]$, il est clair que $V = \mathcal{Z}(\mathcal{I}(V))$ est vide. Réciproquement, si l'idéal $\mathcal{I}(V) \neq \mathbb{K}[\mathbf{x}]$, il est inclus dans un idéal maximal $(x_1 - \zeta_1, \ldots, x_n - \zeta_n)$ de $\mathbb{K}[\mathbf{x}]$. Ainsi, $V \neq \emptyset$, car il contient $(\zeta_1, \ldots, \zeta_n)$. □

***Définition* 1.18.** *Soit I un idéal de $\mathbb{K}[\mathbf{x}]$. Le* radical *de I est*

$$\sqrt{I} = \{g \in \mathbb{K}[\mathbf{x}] : \exists m \in \mathbb{N},\ g^m \in I\}.$$

Il est facile de vérifier que l'ensemble $\sqrt{I}$ est bien un idéal. Un idéal I est dit radical si $\sqrt{I} = I$. En particulier, un idéal premier est radical.

Le résultat suivant est la clé de la correspondance algèbre-géométrie. Nous en donnons une preuve basée sur l'astuce dite de Rabinowitch.

***Théorème* 1.19 (Théorème des zéros de Hilbert).** *Etant donné un corps algébriquement clos $\mathbb{K}$. Alors pour tout idéal I de $\mathbb{K}[\mathbf{x}]$, $\mathcal{I}(\mathcal{Z}_{\mathbb{K}}(I)) = \sqrt{I}$.*

Démonstration. D'après le théorème 1.3, I est engendré par $f_1, \ldots, f_m$. Soit g un élément de $\mathcal{I}(\mathcal{Z}_{\mathbb{K}}(I))$, c'est-à-dire tel que $\mathcal{Z}(f_1, \ldots, f_m) \subset \mathcal{Z}(g)$. Si z est une nouvelle variable, la variété algébrique $\mathcal{Z}(f_1, \ldots, f_m, 1 - z\, g)$ de $\mathbb{K}^{n+1}$ est vide. Donc d'après le théorème 1.17, $(f_1, \ldots, f_m, 1 - z\, g) = \mathbb{K}[\mathbf{x}, z]$. Il existe alors des polynômes $h_1, \ldots, h_m, h$ tels que

$$1 = \sum_{i=1}^{m} h_i(\mathbf{x}, z)\, f_i(\mathbf{x}) + h(\mathbf{x}, z)\,(1 - z\, g(\mathbf{x}))\,.$$

En remplaçant z par $\dfrac{1}{g}$ dans cette identité polynomiale et en réduisant au même dénominateur, nous obtenons

$$g^d = \sum_{i=1}^{m} f_i(\mathbf{x}) g_i(\mathbf{x}) \quad , \quad \text{avec } d \in \mathbb{N} \ \text{ et } \ g_i \in \mathbb{K}[\mathbf{x}].$$

Ainsi, $g \in \sqrt{I}$ et $\mathcal{I}(\mathcal{Z}_{\mathbb{K}}(I)) \subset \sqrt{I}$. L'inclusion inverse est immédiate. □

***Remarque* 1.20.** L'hypothèse $\mathbb{K}$ *algébriquement clos* dans le théorème 1.19 est nécessaire, comme le montre l'exemple suivant : si $\mathbb{K} = \mathbb{R}$ et $I = (x_1^2 + 1)$, $\mathcal{I}(\mathcal{Z}_{\mathbb{R}}(I)) = \mathcal{I}(\emptyset) = \mathbb{R}[\mathbf{x}] \supsetneq \sqrt{I} = (x_1^2 + 1)$. Pour une version du théorème des zéros dans le cadre réel, voir [**BCR87**], [**BR90**], [**Lom91**], [**GVL93**].

Nous venons de voir qu'il y a une correspondance entre les objets algébriques (les idéaux de $\mathbb{K}[\mathbf{x}]$) et les objets géométriques (les variétés algébriques de $\mathbb{K}^n$), réalisée par les deux opérations $\mathcal{Z}$ et $\mathcal{I}$. Si le corps $\mathbb{K}$ est algébriquement clos, cette correspondance est une bijection entre les idéaux maximaux de $\mathbb{K}[\mathbf{x}]$ et les points de $\mathbb{K}^n$, les idéaux premiers de $\mathbb{K}[\mathbf{x}]$ et les variétés irréductibles de $\mathbb{K}^n$, les idéaux radicaux de $\mathbb{K}[\mathbf{x}]$ et les variétés algébriques de $\mathbb{K}^n$.

***Exemple* 1.21.** *En appliquant le théorème 1.19, nous avons*

$$\begin{aligned} \sqrt{(x_1^3 - x_2, x_1^2\, x_2 - x_1\, x_2, x_2^3 - x_1)} &= \mathcal{I}(\{(0,0),(1,1)\}) \\ &= (x_1, x_2) \cap (x_1 - 1, x_2 - 1). \end{aligned}$$

Nous verrons dans la section suivante que tout idéal se décompose en une intersection finie d'idéaux « élémentaires », dans le même esprit que cet exemple.

1.4. Décomposition primaire

Nous avons vu que toute variété algébrique se décompose en une réunion finie de composantes irréductibles (proposition 1.6). Dans le cas d'une variable, cette décomposition correspond à la factorisation d'un polynôme en produit de facteurs premiers entre-eux. Dans le cas multivariable, cette décomposition se généralise en l'intersection d'idéaux primaires (voir définition 1.23). Nous rappelons les résultats généraux concernant la décomposition primaire dans $\mathbb{K}[\mathbf{x}]$ (le contenu de cette section reste vrai dans un anneau noethérien quelconque). Pour plus de détails, consulter [**AM69**].

***Proposition* 1.22.** *Si $\mathbb{K}$ est un corps algébriquement clos, tout idéal radical de $\mathbb{K}[\mathbf{x}]$ se décompose en une intersection finie d'idéaux premiers.*

Démonstration. Soit I un idéal radical. La variété algébrique $\mathcal{Z}(I)$ admet une décomposition en composantes irréductibles $\mathcal{Z}(I) = V_1 \cup \ldots \cup V_s$. D'après le théorème de zéros de Hilbert et la proposition 1.8,

$$I = \sqrt{I} = \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(V_1) \cap \cdots \cap \mathcal{I}(V_s).$$

De plus, les idéaux $\mathcal{I}(V_i)$ sont premiers (proposition 1.10). □

Pour décomposer un idéal (non nécessairement radical) de $\mathbb{K}[\mathbf{x}]$, il faut affiner la notion d'idéal premier.

***Définition* 1.23.** *Un idéal Q de $\mathbb{K}[\mathbf{x}]$ est primaire si*

$$\forall (f,g) \in \mathbb{K}[\mathbf{x}]^2,\ f\,g \in Q \text{ et } f \notin Q \Longrightarrow g \in \sqrt{Q}.$$

Il est évident qu'un idéal premier est en particulier primaire.

Si l'idéal Q est primaire, $P = \sqrt{Q}$ est premier. C'est le plus petit idéal premier contenant Q. Dans ce cas, Q est dit *P-primaire.*

Si I est un idéal de $\mathbb{K}[\mathbf{x}]$ et $g \in \mathbb{K}[\mathbf{x}]$, l'idéal $\{f \in \mathbb{K}[\mathbf{x}] \ : fg \in I\}$ est appelé l'idéal quotient de I par g, et il est noté $(I : g)$. L'idéal engendré par les éléments de I et par g est noté (I, g).

***Définition* 1.24.** *Un idéal I est dit indécomposable s'il n'existe pas d'idéaux $I_1 \neq I$ et $I_2 \neq I$ vérifiant $I = I_1 \cap I_2$.*

***Lemme* 1.25.** *Soient $g \in \mathbb{K}[\mathbf{x}]$, I un idéal de $\mathbb{K}[\mathbf{x}]$ et m un entier positif tels que $(I : g^{m+1}) = (I : g^m)$. Alors $I = (I : g) \cap (I, g^m)$.*

Démonstration. L'inclusion $I \subset (I : g) \cap (I, g^m)$ est évidente.

Soit $h \in (I : g) \cap (I, g^m)$. Il existe alors $f \in I$ et $q \in \mathbb{K}[\mathbf{x}]$ vérifiant $h = f + qg^m$. Comme $h\,g = f\,g + qg^{m+1} \in I$, nous avons $qg^{m+1} \in I$ et

$q \in (I : g^{m+1}) = (I : g^m)$. Ainsi, $qg^m \in I$ et donc $h \in I$. □

***Proposition* 1.26.** *Si l'idéal I est indécomposable, alors il est primaire.*

Démonstration. Soit $(f, g) \in \mathbb{K}[\mathbf{x}]^2$ tel que $f\,g \in I$ et $f \notin I$. Puisque la suite d'idéaux $\{(I : g^n)\}_{n\in\mathbb{N}}$ est croissante, d'après la proposition 1.2 et le théorème 1.3, il existe $m \in \mathbb{N}$ vérifiant $(I : g^m) = (I : g^{m+1})$. En utilisant le lemme 1.25, $I = (I : g) \cap (I, g^m)$. Et comme I est indécomposable et $f \in (I : g) \setminus I$, $(I, g^m) = I$, c'est-à-dire $g \in \sqrt{I}$. □

***Théorème* 1.27.** *Tout idéal I de $\mathbb{K}[\mathbf{x}]$ se décompose en une intersection finie d'idéaux indécomposables.*

Démonstration. Si l'idéal I n'est pas indécomposable, c'est l'intersection de deux idéaux $I_1 \supsetneq I$ et $I_2 \supsetneq I$. Si I_1 et I_2 sont indécomposables, alors I est l'intersection de deux idéaux indécomposables. Sinon, le même argument s'applique à I_1 et/ou I_2. En itérant ceci et en utilisant le théorème 1.3, I s'écrit comme une intersection finie d'idéaux indécomposables. □

Le corollaire suivant se déduit de la proposition 1.26.

***Corollaire* 1.28.** *Tout idéal de $\mathbb{K}[\mathbf{x}]$ se décompose en une intersection finie d'idéaux primaires.*

Une telle décomposition s'appelle une *décomposition primaire*.

***Définition* 1.29.** *Une décomposition primaire $I = \bigcap_{i=1}^r Q_i$ de l'idéal I de $\mathbb{K}[\mathbf{x}]$ est dite* minimale *si les idéaux premiers $\sqrt{Q_i}$ sont tous distincts et si pour tout $i \in \{1, \ldots, r\}$, $Q_i \not\supset \bigcap_{j\neq i} Q_j$.*

***Lemme* 1.30.** *Si I et J sont deux idéaux primaires ayant le même radical P, alors $I \cap J$ est P-primaire.*

Démonstration. Soit $(f, g) \in \mathbb{K}[\mathbf{x}]^2$ tel que $f\,g \in I \cap J$, $f \notin I \cap J$, et supposons que $f \notin I$. Comme I est primaire, $g \in \sqrt{I} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$. □

***Théorème* 1.31.** *Tout idéal de l'anneau $\mathbb{K}[\mathbf{x}]$ admet une décomposition primaire minimale.*

Démonstration. Le corollaire 1.28 assure l'existence d'une décomposition primaire $I = \bigcap_{i=1}^r Q_i$ pour tout idéal I. Supposons que deux idéaux distincts Q_i et Q_j aient le même radical. D'après le lemme 1.30, $Q_{i,j} = Q_i \cap Q_j$ est primaire. Donc en regroupant les idéaux primaires ayant le même radical, nous obtenons une décomposition de I en idéaux primaires ayant des radicaux distincts deux à deux.

Si dans une telle décomposition, un idéal Q_i contient $\bigcap_{j\neq i} Q_j$, nous l'omettons et obtenons $I = \bigcap_{j\neq i} Q_j$. En répétant ceci, si nécessaire, nous aboutissons à une décomposition primaire minimale de I. □

Une décomposition primaire minimale n'est pas *forcément unique* comme le montre l'exemple simple suivant :

***Exemple* 1.32.** *Dans l'anneau $\mathbb{K}[x, y]$, l'idéal*

$$(xy, y^2) = (y) \cap (x, y^2) = (y) \cap (x + y, y^2).$$

Par contre un idéal radical admet une seule décomposition primaire minimale (voir exercice 1.14).

Nous allons voir que les *idéaux premiers associés* (i.e. les radicaux des composantes primaires d'une décomposition minimale) sont uniquement déterminés. Pour les caractériser, nous avons besoin du lemme suivant :

***Lemme* 1.33.** *Soit Q un idéal P-primaire (i.e. Q est primaire et $\sqrt{Q} = P$). Si $f \in \mathbb{K}[\mathbf{x}]$, alors*
i) $f \in Q \Longrightarrow (Q : f) = \mathbb{K}[\mathbf{x}]$,
ii) $f \notin Q \Longrightarrow (Q : f)$ est P-primaire,
iii) $f \notin P \Longrightarrow (Q : f) = Q$.

Démonstration. i) et iii) découlent des définitions.

ii) Déterminons le radical de $(Q : f)$. Soit $g \in (Q : f)$. Comme $f \notin Q$ et $fg \in Q$, nous déduisons que $g \in P$. Ainsi, $Q \subset (Q : f) \subset P$, et $\sqrt{(Q : f)} = P$. L'idéal $(Q : f)$ est P-primaire. En effet, soit $(g, h) \in \mathbb{K}[\mathbf{x}]^2$ qui satisfait $gh \in (Q : f)$, c'est-à-dire $ghf \in Q$, et $g \notin P$. Puisque Q est primaire, $h \in (Q : f)$. □

***Lemme* 1.34.** *Si $P, P_1, \ldots, P_m$ sont des idéaux premiers de $\mathbb{K}[\mathbf{x}]$ qui vérifient $P = P_1 \cap \ldots \cap P_m$, alors il existe i tel que $P = P_i$.*

Démonstration. Voir exercice 1.13. □

***Théorème* 1.35.** *Soit $I = \bigcap_{i=1}^r Q_i$ une décomposition primaire minimale de l'idéal I. Si $f \in \mathbb{K}[\mathbf{x}]$ est tel que $\sqrt{(I : f)}$ est premier, alors $\sqrt{(I : f)} = \sqrt{Q_i}$ pour un $i \in \{1, \ldots, r\}$. Réciproquement, tous les idéaux premiers $\sqrt{Q_i}$ sont de cette forme.*

Démonstration. D'après le lemme 1.33, pour tout $f \in \mathbb{K}[\mathbf{x}]$,

$$(I : f) = (\bigcap_{i=1}^{r} Q_i : f) = \bigcap_{i=1}^{r} (Q_i : f) = \bigcap_{\{i : f \notin Q_i\}} (Q_i : f),$$

et $\sqrt{(I:f)} = \bigcap_{\{i:f\notin Q_i\}} \sqrt{Q_i}$. Si l'idéal $\sqrt{(I:f)}$ est premier, il existe i tel que $\sqrt{(I:f)} = \sqrt{Q_i}$ (lemme 1.34). Réciproquement, comme la décomposition est minimale, pour chaque $i \in \{1,\ldots,r\}$, il existe un polynôme f_i tel que $f_i \notin Q_i$ et $f_i \in \bigcap_{j\neq i} Q_j$. En utilisant le lemme 1.33, nous déduisons que $\sqrt{Q_i} = \sqrt{(Q_i:f_i)} = \sqrt{(I:f_i)}$. □

Les idéaux primaires d'une décomposition minimale d'un idéal I sont appelés les *composantes primaires* de I.

***Remarque* 1.36.** Même si un idéal peut avoir plusieurs décompositions primaires minimales, le nombre de composantes primaires et les radicaux des idéaux primaires sont uniques dans les différentes décompositions primaires minimales d'un même idéal (voir exercice 1.14).

***Définition* 1.37.** *Soit $I = Q_1 \cap \ldots \cap Q_r$ une décomposition primaire minimale de I. L'ensemble $\{\sqrt{Q_i} : 1 \leq i \leq r\}$, qui est indépendant de la décomposition choisie, est appelé l'ensemble des idéaux associés de I. Il sera noté* $\mathrm{Ass}(I)$.

Dans l'exemple 1.32, l'idéal (xy, y^2) admet deux composantes primaires et $\mathrm{Ass}((xy,y^2)) = \{(y),(x,y)\}$.

***Proposition* 1.38.** *Soient $f \in \mathbb{K}[\mathbf{x}]$ et I un idéal de $\mathbb{K}[\mathbf{x}]$. Si f n'appartient à aucun élément de* $\mathrm{Ass}(I)$*, alors $(I:f) = I$.*

Démonstration. Soit $I = Q_1 \cap \ldots \cap Q_r$ une décomposition primaire minimale de I. D'après le lemme 1.33, nous avons

$$(I:f) = (Q_1:f) \cap \ldots \cap (Q_r:f) = Q_1 \cap \ldots \cap Q_r = I.$$

□

***Définition* 1.39.** *Soit $I = Q_1 \cap \ldots \cap Q_r$ une décomposition primaire minimale de l'idéal I de $\mathbb{K}[\mathbf{x}]$. Une composante primaire Q_i de I est dite* immergée *s'il existe $j \neq i$ tel que $\sqrt{Q_j} \subset \sqrt{Q_i}$. Une composante primaire est dite* isolée *s'elle n'est pas immergée.*

Dans l'exemple 1.32, la composante (y) est isolée et (x,y) (respectivement $(x+y, y^2)$) est immergée.

***Remarque* 1.40.** Les composantes primaires isolées, d'un idéal I, dans les différentes décompositions primaires minimales sont uniques (voir exercice 1.14). Les composantes immergées ne le sont pas, comme le montre l'exemple 1.32. Du point de vue géométrique, ces dernières sont « invisibles », et donc elles sont une source de beaucoup de difficultés en géométrie algébrique effective (voir [**CGH88**], [**Kol88**],[**Kol99**], [**EL99**]). Obtenir la décomposition primaire d'un idéal de $\mathbb{K}[\mathbf{x}]$ est un problème délicat (voir [**GTZ88**], [**EHV92**], [**Mon02**]).

Problème(suite) :

Dans le problème de positionnement de la caméra, si $A = (-1, 0, 0)$, $B = (0, 1, 0)$, $C = (1, 0, 0)$ *et le centre* X *est sur l'arc* $\mathcal{C}$ *du cercle circonscrit au triangle* ABC, *allant de* A *à* C *sans passer par* B. *Le système (1.1) devient :*

$$\begin{cases} x_1^2 + x_2^2 - \sqrt{2}\, x_1\, x_2 - 2 = 0 \\ x_1^2 + x_3^2 - 4 = 0 \\ x_2^2 + x_3^2 - \sqrt{2}\, x_2\, x_3 - 2 = 0. \end{cases} \tag{1.2}$$

Pour tout autre point de cet arc de cercle $\mathcal{C}$, *les angles de vues des segments* (A, B), (B, C) *et* (A, C) *sont les mêmes. L'ensemble des solutions de ce système contient donc les vecteurs* (x_1, x_2, x_3) *correspondant aux points de* $\mathcal{C}$. *La différence entre la première et la troisième équation de (1.2) conduit à*

$$(x_1 + x_3 - \sqrt{2}\, x_2)\,(x_1 - x_3) = 0. \tag{1.3}$$

L'ensemble des solutions contient la variété algébrique définie par l'idéal $P_{\mathcal{C}}$ *engendré par* $x_1 + x_3 - \sqrt{2}\, x_2$ *et* $x_1^2 + x_3^2 - 4$. *Cet idéal est premier car* $x_1^2 + x_3^2 - 4$ *est irréductible.*

Y-a-t-il d'autres solutions ? Celles-ci sont sur l'intersection des trois tores obtenus par rotation du cercle $\mathcal{C}$ *autour des segments* (A, B), (B, C), (A, C), *correspondant à un angle de vue constant. D'après l'équation (1.3), les autres solutions vérifient* $x_1 - x_3 = 0$, *ce qui conduit aux solutions* $\xi_1 = (-\sqrt{2}, 0, -\sqrt{2})$, $\xi_2 = (\sqrt{2}, 0, \sqrt{2})$, $\xi_3 = (\sqrt{2}, 2, \sqrt{2})$, $\xi_4 = (-\sqrt{2}, -2, -\sqrt{2})$.

Comme ξ_3 *et* ξ_4 *annulent les polynômes de* $P_{\mathcal{C}}$, $\xi_3, \xi_4 \in \mathcal{Z}(P_{\mathcal{C}})$, *le radical de l'idéal* I *engendré par le système d'équations (1.2) se décompose sous la forme*

$$\sqrt{I} = P_{\mathcal{C}} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \ ,$$

où $\mathfrak{m}_i$ *désigne l'idéal maximal définissant le point* ξ_i,$i = 1, 2, 3, 4$.

Comme $P_{\mathcal{C}}$ *est premier, pour* $g = x_1 - x_3$, *nous avons* $(I : g) = P_{\mathcal{C}}$ *et* $(I : g^2) = (I : g) = P_{\mathcal{C}}$. *De plus,*

$$(I, g) = (x_2^2 - \sqrt{2}\, x_1\, x_2, x_1^2 - 2, x_1 - x_3) = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \cap \mathfrak{m}_4.$$

Nous déduisons d'après le lemme 1.25, la décomposition primaire

$$I = (I : g) \cap (I, g) = P_{\mathcal{C}} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \cap \mathfrak{m}_4.$$

Les composantes premières $\mathfrak{m}_3$ *et* $\mathfrak{m}_4$ *sont immergées dans* $P_{\mathcal{C}}$, *nous pouvons donc simplifier la décomposition de* I *en* $I = P_{\mathcal{C}} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2$, *et ainsi* $I = \sqrt{I}$.

1.5. Quelques invariants numériques d'une variété algébrique

Plusieurs invariants numériques peuvent être associés à une variété algébrique. Les principaux sont la dimension et le degré. Nous les abordons dans cette section et les étudierons, en détail, dans un autre chapitre.

1.5.1. Dimension d'une variété algébrique. — La dimension d'une variété algébrique V peut être définie de plusieurs façons. Intuitivement, c'est « le nombre maximal de degré de liberté » que peut avoir un point se « déplaçant » dans V. Nous donnons ici deux définitions équivalentes de cette notion.

***Définition* 1.41.** *La* dimension topologique *d'une variété V est la longueur maximale d d'une suite*

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d$$

de sous-variétés non vides et irréductibles de V. Elle est notée $\dim_{\mathrm{Tg}}(V)$.

***Remarque* 1.42.** Il est clair que la dimension topologique d'une variété algébrique non vide de $\mathbb{K}^n$ est au plus n.

Si $V \subset W$, alors $\dim_{\mathrm{Tg}}(V) \leq \dim_{\mathrm{Tg}}(W)$.

Si $V = V_1 \cup \ldots \cup V_r$ est la décomposition de la variété V en composantes irréductibles, alors $\dim_{\mathrm{Tg}}(V) = \max\{\dim_{\mathrm{Tg}}(V_1), \ldots, \dim_{\mathrm{Tg}}(V_r)\}$.

***Exemple* 1.43.** *Soit I l'idéal monomial $(x_1\,x_2, x_1\,x_3)$ de $\mathbb{K}[x_1, x_2, x_3]$. La variété $V = \mathcal{Z}(I) = \mathcal{Z}(x_1) \cup \mathcal{Z}(x_2, x_3)$. Nous avons*

$$\mathcal{Z}(x_1, x_2, x_3) \subsetneq \mathcal{Z}(x_1, x_2) \subsetneq \mathcal{Z}(x_1),$$

et donc $\dim_{\mathrm{Tg}}(V) = 2$.

L'équivalent algébrique de la dimension topologique est la notion de la dimension de Krull.

***Définition* 1.44.** *La* dimension de Krull *d'un anneau $\mathcal{A}$ est la longueur maximale r d'une suite*

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

d'idéaux premiers de $\mathcal{A}$. Elle est notée $\dim_{\mathrm{Krull}}(\mathcal{A})$.

***Exemple* 1.45.** *Si $\mathcal{A} = \mathbb{K}[x_1, x_2, x_3]/I$, avec $I = (x_1\,x_2, x_1\,x_3)$, nous avons la suite*

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3)$$

d'idéaux premiers dans $\mathcal{A}$ (car ce sont des premiers de $\mathbb{K}[\mathbf{x}]$ qui contiennent I). Ainsi, $\dim_{\mathrm{Krull}}(\mathcal{A}) = 2$.

Ces deux notions de dimension sont compatibles avec la correspondance algèbre-géométrie :

***Proposition* 1.46.** *Pour tout idéal I de $\mathbb{K}[\mathbf{x}]$, nous avons*

$$\dim_{\mathrm{Krull}}(\mathbb{K}[\mathbf{x}]/I) = \dim_{\mathrm{Tg}}(\mathcal{Z}_{\overline{\mathbb{K}}}(I)).$$

Démonstration. Les idéaux premiers de $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ sont en bijection avec les idéaux premiers de $\mathbb{K}[\mathbf{x}]$ qui contiennent I. D'après l'exercice 1.13, ils contiennent un des idéaux premiers de $Ass(I)$ et définissent donc une variété algébrique incluse dans l'une des composantes irrédutibles de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$. Les idéaux premiers de $\mathcal{A}$ sont en correspondance avec les sous-variétés irréductibles de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$. Par conséquent, la dimension de Krull de $\mathcal{A}$ est la même que la dimension topologique de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$. □

Une variété algébrique X formée de points isolés est de dimension 0, car les idéaux premiers associés à $\mathcal{I}(X)$ sont maximaux.

Une variété algébrique de dimension 1 est une *courbe*, une variété de dimension 2 est une *surface*, et une variété de dimension $n-1$ de l'espace $\mathbb{K}^n$ (qui est de dimension n) est appelée une *hypersurface*.

1.5.2. Degré d'une variété algébrique. — Le degré d'une variété V exprime d'une certaine manière la « complexité » apparente de celle-ci. Plus le degré est élevé et plus il faut s'attendre à une variété « tordue ». Voici une définition géométrique de cette notion.

***Définition* 1.47.** *Le* degré *de $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ est la dimension du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/(I, l_1, \ldots, l_d)$, où $l_1, \ldots, l_d$ sont des formes linéaires génériques (i.e. dont les coefficients n'appartiennent pas à une variété algébrique) et d la dimension de Krull de $\mathcal{A}$. Il sera noté* $\deg_L(\mathcal{A})$.

Nous verrons que ce degré est le nombre de points de $V(I) \cap V(l_1, \ldots, l_d)$.

***Exemple* 1.48.** *Un espace linéaire est une variété algébrique de degré* 1.

Une hypersurface $\mathcal{Z}(f)$, avec f sans facteur carré, est une variété algébrique de degré $\deg f$. *En effet, l'intersection de $\mathcal{Z}(f)$ et d'une droite générique est formée de* $\deg f$ *points (comptés avec multiplicité).*

Problème(suite) :

Nous avons décomposé les solutions du système (1.2) en une composante de dimension 1 *définie par l'idéal $P_{\mathcal{C}}$, et des points ξ_1, ξ_2 de dimension* 0. *L'ensemble de ces solutions est donc de dimension* 1.

Pour obtenir son degré, nous ajoutons une équation linéaire générique $l(x_1, x_2, x_3) = 0$ *et calculons la dimension de $\mathcal{A} = \mathbb{K}[x_1, x_2, x_3]/(I, l(x_1, x_2, x_3))$.*

Comme $\xi_1, \xi_2, \xi_3, \xi_4$ ne satisfont pas cette équation générique, la dimension de $\mathcal{A}$ est aussi celle de

$$\mathbb{K}[x_1, x_2, x_3]/(x_1^2 + x_3^2 - 4, x_1 + x_3 - \sqrt{2}\, x_2, l(x_1, x_2, x_3)).$$

Nous vérifions que cet espace vectoriel est de dimension 2 *(et de base* $\{1, x_1\}$*). Le degré de la variété* $\mathcal{Z}(I)$ *est donc* 2.

Des algorithmes permettant de calculer ces invariants numériques associés à une variété algébrique sont décrits dans le chapitre 4.

1.6. Un peu de géométrie projective

La géométrie affine peut se révèler insuffisante pour bien comprendre des problèmes de nature géométrique. Par exemple, l'intersection de deux droites affines distinctes n'est pas toujours un point. Ou encore, la projection d'une variété affine n'est pas toujours une variété affine comme le montre l'exemple de la projection sur l'axe des x de l'hyperbole d'équation $x\,y - 1 = 0$, qui est

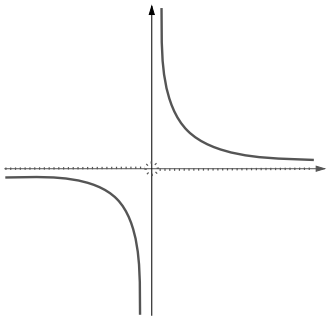

FIGURE 1.2. Une hyperbole et sa projection.

$\mathbb{K} \setminus \{0\}$. Nous reviendrons sur ces questions au chapitre 5.

C'est pour cela que l'on introduit la géométrie projective. Beaucoup de problèmes deviennent plus simples et plus clairs lorsqu'ils sont énoncés dans le cadre projectif.

L'*espace projectif* $\mathbb{P}^n(\mathbb{K})$ (ou $\mathbb{P}^n$ s'il n'y a pas d'ambiguïté sur le corps $\mathbb{K}$) est le quotient de $\mathbb{K}^{n+1} \setminus \{0\}$ par la relation d'équivalence de colinéarité. Un point de $\mathbb{P}^n$ est noté $(a_0 : \cdots : a_n)$.

Soit f un polynôme homogène de $\mathbb{K}[x_0, \ldots, x_n]$. Si f s'annule au point $(a_0, \ldots, a_n)$ de $\mathbb{K}^{n+1}$, alors $f(\lambda(a_0, \ldots, a_n)) = 0$ pour tout $\lambda \in \mathbb{K}$. Nous dirons que $(a_0 : \cdots : a_n)$ est un zéro de f, et notons $f(a_0 : \cdots : a_n) = 0$.

***Définition* 1.49.** *La* variété algébrique projective *de* $\mathbb{P}^n$ *définie par des polynômes homogènes* $f_1, \ldots, f_m$ *de* $\mathbb{K}[x_0, \ldots, x_n]$ *est l'ensemble*

$$\mathcal{Z}_{\mathbb{P}^n}(f_1, \ldots, f_m) = \{a \in \mathbb{P}^n : f_1(a) = \cdots = f_m(a) = 0\}.$$

De la même façon que dans le cadre affine, les variétés projectives définissent une topologie sur $\mathbb{P}^n$, dite de Zariski. Les variétés projectives irréductibles sont aussi définies comme dans le cas affine.

Nous rappelons qu'un idéal I de $\mathbb{K}[\mathbf{x}]$ est dit *homogène* s'il est engendré par des polynômes homogènes.

***Définition* 1.50.** *Soit Z un sous-ensemble de $\mathbb{P}^n$. L'ensemble $\mathcal{I}(Z)$ des polynômes de $\mathbb{K}[x_0, \ldots, x_n]$ qui s'annulent en tout point de Z est un idéal homogène, appelé l'idéal de Z et noté $\mathcal{I}(Z)$.*

***Proposition* 1.51.**

1. *Soient I et J deux idéaux homogènes de $\mathbb{K}[x_0, \ldots, x_n]$. Si $I \subset J$, alors $\mathcal{Z}_{\mathbb{P}^n}(J) \subset \mathcal{Z}_{\mathbb{P}^n}(I)$.*
2. *Si $Z \subset W$ sont deux sous-ensembles de $\mathbb{P}^n$, alors $\mathcal{I}(W) \subset \mathcal{I}(Z)$.*
3. *Une variété projective est irréductible si, et seulement si, son idéal homogène est premier.*
4. *Toute variété projective se décompose en une réunion finie unique de sous-variétés projectives irréductibles.*
5. *Soit $\mathbb{K}$ un corps algébriquement clos. Si I est un idéal homogène de $\mathbb{K}[x_0, \ldots, x_n]$, alors $\mathcal{Z}_{\mathbb{P}^n(\mathbb{K})}(I) = \emptyset$ si, et seulement si, $(x_0, \ldots, x_n) \subset \sqrt{I}$.*
6. *Soit $\mathbb{K}$ un corps algébriquement clos. Si I est un idéal homogène de $\mathbb{K}[x_0, \ldots, x_n]$ tel que $(x_0, \ldots, x_n) \not\subset \sqrt{I}$, alors $\mathcal{I}(\mathcal{Z}_{\mathbb{P}^n(\mathbb{K})}(I)) = \sqrt{I}$.*

Démonstration. Voir l'exercice 1.18. □

Notons $H_\infty = \{a = (a_0 : \cdots : a_n) \in \mathbb{P}^n : a_0 = 0\}$ et $O = \{a \in \mathbb{P}^n : a_0 \neq 0\}$. Alors l'espace projectif $\mathbb{P}^n = H_\infty \cup O$. La variété H_∞ s'appelle l'*hyperplan à l'infini*. L'ouvert O de $\mathbb{P}^n$ est homéomorphe à $\mathbb{K}^n$ via l'application

$$\begin{array}{rcl} \phi : O & \longrightarrow & \mathbb{K}^n \\ (a_0 : \cdots : a_n) & \mapsto & \left(\dfrac{a_1}{a_0}, \ldots, \dfrac{a_n}{a_0}\right). \end{array}$$

L'espace affine $\mathbb{K}^n$ peut être alors vu comme un ouvert de $\mathbb{P}^n$ et l'espace projectif $\mathbb{P}^n$ comme $H_\infty \cup \mathbb{K}^n$.

***Proposition* 1.52.** *Si V est une variété projective de $\mathbb{P}^n$, alors $\phi(V \cap O)$ est une variété affine de $\mathbb{K}^n$.*

Démonstration. La variété $V = \mathcal{Z}_{\mathbb{P}^n}(I)$, où I est un idéal homogène radical. Il est clair que $\phi(V \cap O) = \mathcal{Z}\big(f(1, x_1, \ldots, x_n) : f \in I\big)$. □

La trace d'une variété projective de $\mathbb{P}^n$ sur son ouvert affine $\mathbb{K}^n$ est bien une variété affine.

1.7. Exercices

***Exercice* 1.1.**

1. *Théorème fondamental de l'algèbre :* Montrer que tout polynôme non constant à coefficients dans $\mathbb{K}$ admet au moins une racine dans $\overline{\mathbb{K}}$.
2. Montrer que tout idéal de $\mathbb{K}[x]$ est engendré par un seul polynôme.

***Exercice* 1.2.** Montrer que les propriétés suivantes sont équivalentes dans un anneau A commutatif et unitaire.

1. Tout idéal de A est engendré par un nombre fini d'éléments.
2. Toute suite croissante d'idéaux de A est stationnaire.
3. Tout ensemble d'idéaux de A admet un élément maximal (pour l'inclusion).

***Exercice* 1.3.**

1. Soit Y un sous-ensemble de $\mathbb{K}^n$. Montrer que $\overline{Y}$ (le plus petit fermé contenant Y pour la topologie de Zariski) est l'ensemble des solutions de tous les polynômes qui s'annulent sur Y.
2. En déduire que si V est une variété algébrique, alors $\mathcal{Z}\big(\mathcal{I}(V)\big) = V$.

***Exercice* 1.4.**

1. Vérifier que la réunion finie et l'intersection quelconque de variétés algébriques sont des variétés algébriques.
2. Si Y et Z sont deux sous-ensembles de $\mathbb{K}^n$, montrer que $\mathcal{I}(Y \cup Z) = \mathcal{I}(Y) \cap \mathcal{I}(Z)$.
3. Montrer qu'une variété algébrique V est irréductible si, et seulement si, son idéal $\mathcal{I}(V)$ est premier.
4. Soit V une variété algébrique de $\mathbb{K}^n$. Montrer que les propriétés suivantes sont equivalentes :
   i) V est irréductible,
   ii) L'intersection de deux ouverts non vides de V est non vide,
   iii) Tout ouvert non vide de V est partout dense dans V.

***Exercice* 1.5. Décomposition d'une variété en sous-variétés irréductibles.** Soit V une variété algébrique de $\mathbb{K}^n$.

1. Si $\zeta \notin V$, montrer que $\mathcal{I}(V \cup \{\zeta\}) \subsetneq \mathcal{I}(V)$.
2. Si V n'est pas une réunion finie de sous-variétés irréductibles, montrer qu'il existe une suite infinie de variétés V_i telle que $V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots$
3. En déduire que V se décompose de façon unique comme une réunion minimale de sous-variétés irréductibles $V = V_1 \cup \ldots \cup V_d$, où V_i n'est pas contenu dans V_j si $i \neq j$.

***Exercice* 1.6.** Soient I et J deux idéaux de $\mathbb{K}[\mathbf{x}]$.

1. Est-ce que $\mathcal{Z}(I) \setminus \mathcal{Z}(J)$ est une variété algébrique ?
2. Montrer que $\mathcal{Z}(I) \setminus \mathcal{Z}(J)$ est la projection d'une variété algébrique (en introduisant une nouvelle variable).