## Mémoire

**Auteur :** Di Zinno, Augustin
**Promoteur(s) :** Mathonet, Pierre; Michel, Lucas
**Faculté :** Faculté des Sciences
**Diplôme :** Master en sciences mathématiques, à finalité approfondie
**Année académique :** 2024-2025
**URI/URL :** http://hdl.handle.net/2268.2/22977

Faculté des Sciences
Département de Mathématique

# Élimination des quantificateurs sur un champ réel clos : Principe de Tarski-Seidenberg et Décomposition cylindrique algébrique

Mémoire de fin d'études présenté en vue de l'obtention du titre de
*Master en Sciences Mathématiques, à finalité approfondie*

Année académique 2024-2025

*Auteur :*
Augustin Di Zinno

*Promoteur :*
Pierre Mathonet

*Co-Promoteur :*
Lucas Michel

# Remerciements

Je tiens tout particulièrement à remercier mon promoteur, Pierre Mathonet, ainsi que mon co-promoteur, Lucas Michel, pour leur grande disponibilité et leurs précieux conseils, qui ont grandement contribué au bon développement de ce travail.

Je remercie également mes parents, qui m'ont toujours soutenu et permis de suivre mes études dans les meilleures conditions, ainsi que toutes les personnes que j'ai pu côtoyer durant ces cinq années au B37 ou dans la vie universitaire de manière générale.

# Table des matières

# Introduction

Le problème d'élimination des quantificateurs apparaît dans le cursus d'études en mathématiques dès l'école secondaire. Quand on se demande si un polynôme de degré deux à coefficients réels admet une racine réelle, on analyse en fait la formule

$$\exists X \in \mathbb{R} : aX^2 + bX + c = 0,$$

où $a, b, c \in \mathbb{R}$ sont tels que $a \neq 0$. Le discriminant permet alors d'écrire une formule équivalente sans quantificateur, à savoir

$$b^2 - 4ac \geq 0.$$

Plus tard, dans la théorie des systèmes linéaires, on peut également se poser la question d'existence de solution pour un système donné. Par exemple, pour $A \in \mathbb{R}_n^m$ et $B \in \mathbb{R}^m$, la formule

$$\exists X \in \mathbb{R}^n : AX = B,$$

est équivalente à la formule sans quantificateur

$$\mathrm{rg}(A) = \mathrm{rg}(A|B).$$

De même, si $m = n$, alors la formule

$$\forall B \in \mathbb{R}^n, \exists X \in \mathbb{R}^n : AX = B,$$

est équivalente à la formule sans quantificateur

$$\det(A) \neq 0.$$

On constate que dans ces exemples simples, si on considère $a, b, c, A, B$ comme des variables, on part d'une formule avec quantificateurs en les variables $a, b, c, A, B, X$, où la variable $X$ est quantifiée, et on montre qu'elle est équivalente à une formule sans quantificateur, formée d'expressions polynomiales en (les composantes de) $a, b, c, A, B$.

Le problème général traité dans ce mémoire est l'élimination des quantificateurs pour des formules formées à l'aide de connecteurs booléens et de quantificateurs, et de formules atomiques données par des égalités et inégalités polynomiales, où, de façon générale, les polynômes en question sont à coefficients dans des champs réels clos.

Le résultat principal est alors le Principe de Tarski-Seidenberg qui énonce que toute formule de ce type est bien équivalente à une formule sans quantificateurs. Ce résultat est énoncé par Alfred Tarski dans les années 1930 et démontré dans les années 1950, par lui-même, et amélioré par Abraham Seidenberg.

Par la suite, divers mathématiciens vont fournir une nouvelle méthode d'élimination ou une amélioration d'une méthode existante. Nous allons nous intéresser à celle introduite par l'américain Georges Edwin Collins en 1974 ; la Décomposition Cylindrique Algébrique (abrégée CAD).

Cette méthode va, à un ensemble fini de polynômes à $n$ indéterminées, associer une décomposition finie de l'espace $\mathbf{R}^n$ (où $\mathbf{R}$ est un champ réel clos). Chaque "morceau" de cette décomposition est appelé cellule ; il est défini par des fonctions semi-algébriques et le caractère cylindrique s'exprime par une propriété de projection des cellules, garantie par la méthode de construction. La décomposition est faite pour que chaque polynôme soit de signe constant sur chacune des cellules. On peut alors observer dans quelles cellules la formule est vérifiée en évaluant les polynômes en un point de chaque cellule. Cette technique permet d'obtenir une élimination des quantificateurs implémentable en pratique.

L'objectif de ce mémoire est donc de prouver le Principe de Tarski-Seidenberg et ensuite d'expliciter un algorithme de construction de la CAD, et de montrer comment cette technique permet l'élimination des quantificateurs.

Le chapitre 1 contient essentiellement des résultats préliminaires et rappels d'algèbre mais aussi quelques résultats concernant les polynômes symétriques dont nous avons besoin dans le chapitre suivant.

Dans celui-ci, nous étudions les champs réels clos, qui fournissent le cadre naturel pour le problème que nous considérons, et nous présentons finalement des résultats d'analyse sur les champs réels clos, ainsi que les résultats de Sylvester et Sturm qui permettent la localisation des racines de polynômes.

Dans le chapitre 3, nous posons précisément le problème de l'élimination des quantificateurs et détaillons toutes les étapes de la preuve du Principe de Tarski-Seidenberg.

Le chapitre 4 contient une étude des fonctions et ensembles semi-algébriques et la transposition dans ce cadre de résultats classiques de l'analyse, tandis que dans le chapitre 5, nous développons des outils algébriques qui serviront à la construction de la CAD : discriminants, résultants et sous-résultants.

Ces outils nous permettent d'enfin construire les CAD dans le dernier chapitre. Nous y donnons bien sûr une définition précise des CAD et nous démontrons le théorème d'existence, mais nous montrons aussi comment la CAD permet d'effectuer une élimination des quantificateurs.

# Chapitre 1

# Préliminaires algébriques

Dans ce chapitre, nous présentons les résultats d'algèbre nécessaires dans ce mémoire. Cela nous permet aussi de fixer les notations et conventions. La plupart des résultats de rappels sont énoncés sans démonstration, celles-ci figurant dans des cours de la formation de bachelier de l'ULiège. Dans la première section, on donnera cependant le détail de la construction du corps des fractions d'un anneau intègre. Ensuite, après quelques rappels sur les polynômes univariés et extensions de champs, on s'intéressera dans la section 1.3 aux polynômes multivariés et en particulier aux polynômes symétriques.

## 1.1 Anneau intègre et corps des fractions

Nous considérons dans ce qui suit, travailler dans un anneau commutatif unitaire $\mathbf{D}$ où on supposera que $0 \neq 1$. Nous noterons $\mathbf{D}_0 = \mathbf{D} \setminus \{0\}$.

**Définition 1.1.1.** Un anneau commutatif unitaire $(\mathbf{D}, +, \cdot)$ est dit intègre s'il est non nul et si pour tout $a, b \in \mathbf{D}$ tels que $ab = 0$ alors $a = 0$ ou $b = 0$.

Nous détaillons ici la construction du corps des fractions associé à un anneau intègre. Cette construction suit exactement les mêmes lignes que la construction de l'ensemble des rationnels $\mathbb{Q}$ à partir de l'anneau des entiers $\mathbb{Z}$ faite dans [9]. L'équivalence, la multiplication et l'addition sont définies de la même manière que celles des fractions.

**Proposition 1.1.2.** *Si* $\mathbf{D}$ *est un anneau intègre, alors la relation* $\sim$ *définie sur* $\mathbf{D} \times \mathbf{D}_0$ *par*

$$(a, b) \sim (c, d) \text{ si et seulement si } ad = cb$$

*est une relation d'équivalence.*

*Démonstration.* Il est évident que la relation est symétrique et réflexive. De plus, si $(a, b), (c, d), (e, f) \in D \times D_0$ sont tels que $ad = cb$ et que $cf = ed$, alors en multipliant ces égalités par respectivement $f$ et $b$, on a

$$adf = cbf \text{ et } cfb = edb.$$

Par commutativité on a alors que $afd = ebd$. Autrement dit, $(af - be)d = 0$, par intégrité de l'anneau on en déduit que $af - be = 0$ et donc que $af = be$. La relation est donc bien transitive et est donc bien une relation d'équivalence. □

**Définition 1.1.3.** Soit $\mathbf{D}$ un anneau intègre. On définit $\mathbf{K}$ le corps des fractions de $\mathbf{D}$ comme étant

$$\mathbf{K} = \mathbf{D} \times \mathbf{D}_0 \,/\sim,$$

muni des opérations

$$+ : \mathbf{K} \times \mathbf{K} \to \mathbf{K} : ([(a,b)],[(c,d)]) \mapsto [(ad+bc,bd)].$$

et

$$\cdot : \mathbf{K} \times \mathbf{K} \to \mathbf{K} : ([(a,b)],[(c,d)]) \mapsto [(ac,bd)].$$

Pour que la définition soit complète, il est nécessaire de démontrer que ces opérations sont bien définies et munissent bien $\mathbf{K}$ d'une structure de corps.

**Proposition 1.1.4.** *L'addition et la multiplication sur* $\mathbf{K}$ *sont bien définies.*

*Démonstration.* Tout d'abord, remarquons que si $(a,b)$ et $(c,d)$ sont des éléments de $\mathbf{D} \times \mathbf{D}_0$, alors $bd \neq 0$, car l'anneau est intègre. Montrons ensuite que le produit est indépendant du choix des représentants. Supposons que $(a,b) \sim (a',b')$ et que $(c,d) \sim (c',d')$, c'est-à-dire que $ab' = ba'$ et $cd' = dc'$.
Pour l'addition, on doit montrer que

$$[(ad+bc,bd)] = [(a'd'+b'c',b'd')]$$

c'est-à-dire

$$(ad+bc)b'd' = bd(a'd'+b'c').$$

Or, on a

$$(ad+bc)b'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd'+b'c').$$

Pour la multiplication, il faut montrer que

$$[(ac,bd)] = [(a'c',b'd')]$$

c'est-à-dire

$$acb'd = bda'c'.$$

Or, on a

$$acb'd' = (ab')(cd') = (a'b)(c'd) = bda'c'.$$

□

**Proposition 1.1.5.** *L'ensemble* $\mathbf{K}$ *muni de ces deux opérations est bien un corps. Le neutre de l'addition est* $[(0,1)]$ *et celui de la multiplication est* $[(1,1)]$. *Pour tout* $(a,b) \in \mathbf{D} \times \mathbf{D}_0$ *tel que* $[(a,b)] \neq [(0,1)]$, *l'inverse de* $[(a,b)]$ *est* $[(b,a)]$.

*Démonstration.* Soient $(a,b),(c,d),(e,f)$ des éléments quelconques dans $\mathbf{D}\times\mathbf{D}_0$.

1. L'addition est associative :

$$\begin{aligned}([(a,b)]+[(c,d)])+[(e,f)] &= [(ad+bc,bd)]+[(e,f)]\\ &= [((ad+bc)f+bde,bdf)]\\ &= [(adf+bcf+bde,bdf)]\\ &= [(adf+b(cf+de),bdf)]\\ &= [(a,b)]+[(cf+de,df)] = [(a,b)]+([(c,d)]+[(e,f)]).\end{aligned}$$

2. L'élément $[(0,1)]$ est neutre pour l'addition :

$$[(0,1)]+[(a,b)] = [(0b+1a,1b)] = [(a,b)] = [(a1+b0,b1)] = [(a,b)]+[(0,1)]$$

3. Tout élément admet un opposé, l'opposé de $[(a,b)]$ étant $[(-a,b)]$. On a

$$[(a,b)]+[(-a,b)] = [(ab+b(-a),bb)] = [(0,b)] = [(0,1)]$$

et de même on a $[(-a,b)]+[(a,b)] = [(0,1)]$.

4. L'addition est commutative : on a

$$[(a,b)]+[(c,d)] = [(ad+bc,bd)] = [(cb+da,db)] = [(c,d)]+[(a,b)]$$

étant donné la commutativité de l'addition et de la multiplication dans $D$.

5. La multiplication est associative : on a

$$\begin{aligned}([(a,b)]\cdot[(c,d)])\cdot[(e,f)] &= [(ac,bd)]\cdot[(e,f)]\\ &= [((ac)e,(bd)f]\\ &= [(a(ce),b(df))]\\ &= [(a,b)]\cdot[(ce,df)] = [(a,b)]\cdot([(c,d)]\cdot[(e,f)])\end{aligned}$$

étant donné l'associativité de la multiplication dans $\mathbf{D}$.

6. L'élément $[(1,1)]$ est neutre pour la multiplication. On a

$$[(a,b)]\cdot[(1,1)] = [(a1,b1)] = [(a,b)] = [(1a,1b)] = [(1,1)]\cdot[(a,b)].$$

7. La multiplication est commutative : on a

$$[(a,b)]\cdot[(c,d)] = [(ac,bd)] = [(ca,db)] = [(c,d)]\cdot[(a,b)]$$

étant donné la commutativité de la multiplication dans $\mathbf{D}$.

8. La multiplication distribue l'addition :

$$\begin{aligned}[(a,b)]\cdot([(c,d)]+[(e,f)]) &= [(a,b)]\cdot[(cf+de,df)]\\ &= [(a(cf+de),bdf)]\\ &= [(acf+ade,bdf)] = [(acf+ade,bdf)]\cdot[(1,1)]\\ &= [(acf+ade,bdf)]\cdot[(b,b)] = [(acbf+bdae,bbdf)]\\ &= [(ac,bd)]+[(ae,bf)] = [(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)].\end{aligned}$$

9. Tout élément non nul admet un inverse. Si $[(a,b)] \neq [(0,1)]$ alors $a \neq 0$ et $[(b,a)]$ est l'inverse de $[(a,b)]$. On a en effet

$$[(b,a)]\cdot[(a,b)] = [(ba,ab)] = [(1,1)].$$

Et donc $(\mathbf{K},+,[(0,1)],\cdot,[(1,1)])$ possède bien une structure de corps commutatif. □

**Proposition 1.1.6.** *L'anneau* $\mathbf{D}$ *est plongé dans son corps des fractions via*

$$p : \mathbf{D} \to \mathbf{K} : a \mapsto [(a,1)].$$

*Démonstration.* Pour montrer qu'il s'agit d'un plongement, il faut vérifier qu'il s'agit d'un homomorphisme injectif. Commençons par montrer l'injectivité.
Si $a, b \in \mathbf{D}$ sont tels que $p(a) = p(b)$, autrement dit, $[(a,1)] = [(b,1)]$ alors $a.1 = 1.b$ d'où $a = b$. Ensuite, il faut vérifier qu'il s'agit d'un homomorphisme d'anneaux. On a

$$p(a+b) = [(a+b,1)] = [(a,1)] + [(b,1)] = p(a) + p(b),$$

mais également

$$p(a.b) = [(a.b,1)] = [(a,1)].[(b,1)] = p(a)p(b)$$

et enfin, $p(1) = [(1,1)]$ et $p(0) = [(0,1)]$ qui sont les neutres pour la multiplication et pour l'addition dans le corps des fractions. □

## 1.2 Rappels sur les polynômes et extensions de champs

### 1.2.1 Polynômes univariés

**Définition 1.2.1.** Un polynôme sur un anneau $\mathbf{D}$ est une suite $(a_n)_{n\in\mathbb{N}} \in \mathbf{D}^{\mathbb{N}}$ telle que il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N, a_n = 0$. Si $P = (a_n)_{n\in\mathbb{N}}$ est un polynôme non nul de $\mathbf{D}$, son degré est

$$d = \max\{n \in \mathbb{N} : a_n \neq 0\}.$$

On note alors

$$P = a_d X^d + \ldots + a_1 X + a_0,$$

et

$$\mathrm{lcof}(P) = a_d.$$

L'ensemble des polynômes sur $\mathbf{D}$ est noté $\mathbf{D}[X]$ et l'ensemble des polynômes sur $\mathbf{D}$ de degré inférieur ou égal à $n$ est noté $\mathbf{D}_n[X]$. Si $P = 0$ alors $\deg(P) = -\infty$ par convention.

**Définition 1.2.2.** Soit $P \in \mathbf{D}[X]$, noté $P = a_d X^d + \ldots + a_1 X + a_0$. On considère la fonction polynomiale associée définie par

$$f_P : \mathbf{D} \to \mathbf{D} : x \mapsto a_d x^d + \ldots + a_1 x + a_0.$$

Dans ce mémoire, on travaille uniquement sur des anneaux infinis, on peut donc confondre polynôme et fonction polynomiale sans problème. On notera $P$ ou $P(X)$ le polynôme et $P(x)$ l'évaluation en $x \in \mathbf{D}$ de la fonction polynomiale associée.

On rappelle également que $\mathbf{D}[X]$ est muni d'une structure d'anneau via les opérations qui généralisent ce que l'on connaît des puissances et fonctions polynomiales sur $\mathbb{R}$.

Dans ce qui va suivre, on supposera que $\mathbf{D}$ est intègre car nous allons considérer son corps des fractions $\mathbf{K}$.

**Proposition 1.2.3.** *Si* $\mathbf{D}$ *est un anneau intègre, alors* $\mathbf{D}[X]$ *est également un anneau intègre.*

*Démonstration.* Considérons

$$P = a_p X^p + \ldots + a_0$$

et

$$Q = b_q X^q + \ldots + b_0$$

des polynômes non-nuls de $\mathbf{D}[X]$. Le terme de plus haut degré de $PQ$ est alors $a_p b_q$, et il est non nul étant donné que $a_p, b_q \neq 0$ et que $\mathbf{D}$ est intègre. □

Maintenant qu'on a défini l'anneau des polynômes à coefficients dans un anneau $\mathbf{D}$ supposé intègre, nous cherchons à le munir d'une opération de division. Pour cela, on considère le corps des fractions $\mathbf{K}$ de $\mathbf{D}$ et on prolonge le plongement de $\mathbf{D}$ dans $\mathbf{K}$ par le prolongement de $\mathbf{D}[X]$ dans $\mathbf{K}[X]$ défini par

$$p : \mathbf{D}[X] \to \mathbf{K}[X] : a_n X^n + \ldots + a_0 \mapsto [(a_n, 1)]X^n + \ldots + [(a_0, 1)].$$

On vérifie sans difficulté qu'il s'agit toujours d'un plongement.

Le résultat suivant, démontré dans [8], nous garantit alors qu'on peut effectuer une division dans $\mathbf{K}[X]$.

**Proposition 1.2.4.** *Si* $\mathbf{K}$ *est un champ, alors* $\mathbf{K}[X]$ *est euclidien. C'est à dire que* $\mathbf{K}[X]$ *admet une division euclidienne. De plus, les quotients et les restes sont uniques.*

On a désormais tout ce qu'il faut pour parler de division. Soient $P, Q \in \mathbf{D}[X]$, formellement si on souhaite effectuer une division euclidienne de $P$ par $Q$, on les plonge dans $\mathbf{K}[X]$ où $\mathbf{K}$ est le corps des fractions de $\mathbf{D}$. On dit alors que $Q$ divise $P$ si le reste de la division euclidienne dans $\mathbf{K}[X]$ de leur image par le plongement est nul. Dans la définition qui suit on ne parle pas de plongement afin de ne pas alourdir les notations, mais c'est sous-entendu. Il en va de même pour les définitions suivantes.

**Définition 1.2.5.** Soit $P, Q \in \mathbf{D}[X]$. On dit que $Q$ divise $P$ s'il existe $A \in \mathbf{K}[X]$ tel que

$$P = AQ.$$

De plus, on dit que $P$ est un multiple de $Q$.

**Exemple 1.2.6.** Considérons $P = X^3 + 3X^2 + 2X$ et $Q = 3X$ des polynômes de $\mathbb{Z}[X]$. On a que $Q$ divise $P$ car

$$X^3 + 3X^2 + 2X = (\frac{1}{3}X^2 + X + \frac{2}{3})3X,$$

donc il existe $A \in \mathbb{Q}[X]$ tel que $P = AQ$ avec

$$A = \frac{1}{3}X^2 + X + \frac{2}{3}.$$

**Définition 1.2.7.** Soient $P, Q \in \mathbf{D}[X]$. Un plus grand commun diviseur de $P$ et $Q$, noté $\text{pgcd}(P, Q)$, est un polynôme $G \in \mathbf{K}[X]$ tel que $G$ divise $P$ et $Q$ tel que tout diviseur de $P$ et de $Q$ divise $G$.

**Remarque 1.2.8.** Au vu de la définition 1.2.7 on remarque que si $G_1$ et $G_2$ sont deux pgcd de $P$ et $Q$ alors ils sont proportionnels selon un élément de $\mathbf{K}_0$.

**Définition 1.2.9.** Deux polynômes $P, Q \in \mathbf{D}[X]$ sont premiers entre eux si $\text{pgcd}(P, Q) \in \mathbf{K}_0$.

**Exemple 1.2.10.** Si on considère $P = X+1$, et $Q = X^2+1$ alors $\text{pgcd}(P, Q) = 1$ donc $P$ et $Q$ sont premiers entre eux. Tandis que si on considère $Q = X^2-1$ alors $\text{pgcd}(P, Q) = X+1$ et donc $P$ et $Q$ ne sont pas premiers entre eux.

**Définition 1.2.11.** Soient $P, Q \in \mathbf{D}[X]$. Un plus petit commun multiple de $P$ et de $Q$, noté $\text{ppcm}(P, Q)$ est un polynôme $G \in \mathbf{K}[X]$ tel que $G$ est un multiple de $P$ et de $Q$ tel que tout multiple de $P$ et $Q$ est également multiple de $G$.

**Remarque 1.2.12.** On peut obtenir $\text{ppcm}(P, Q)$ par $\frac{PQ}{\text{pgcd}(P,Q)}$. Au vu de la remarque 1.2.8, le pgcd est défini à un facteur inversible près, il en va donc de même pour le ppcm.

**Exemple 1.2.13.** Considérons $P = X^2 + 3X + 2$ et $Q = 3X$ des polynômes de $\mathbb{Z}[X]$. On a

$$(X)P = (\frac{1}{3}X^2 + X + \frac{2}{3})Q$$

donc $3X^3 + 9X^2 + 6X$ et $\frac{1}{2}X^3 + \frac{3}{2}X^2 + X$ sont, par exemple, tous deux des ppcm de $P$ et de $Q$ (ces ppcm sont égaux au facteur multiplicatif inversible 6 près).

### 1.2.2 Rappels sur les champs

Voici quelques définitions et résultats démontrés en bachelier que nous utiliserons durant ce mémoire. Ceux-ci qui concernent les champs et les extensions de champ sont démontrés dans [8] et [5].

**Définition 1.2.14.** Si $\mathbf{K}$ est un champ alors une extension de champ $\mathbf{K}_1$ de $\mathbf{K}$ est dite algébrique si tout élément de $\mathbf{K}_1$ est racine d'un polynôme de $\mathbf{K}[X]$.

**Définition 1.2.15.** Un champ $\mathbf{K}$ est algébriquement clos si tout polynôme de $\mathbf{K}[X]$ se factorise complètement dans $\mathbf{K}$.

**Théorème 1.2.16.** *Tout champ admet une extension algébriquement close.*

**Remarque 1.2.17.** Un champ $\mathbf{K}$ est algébriquement clos si et seulement si tout polynôme de $\mathbf{K}[X]$ admet une racine dans $\mathbf{K}$.

*Démonstration.* Le premier sens est direct par définition d'un champ algébriquement clos. La réciproque nécessite une simple récurrence sur le degré du polynôme. □

**Définition 1.2.18.** Soit un champ $\mathbf{K}$. Une extension de champ de $\mathbf{K}$ est une clôture algébrique de $\mathbf{K}$ si cette extension est algébriquement close et si elle est minimale pour cette propriété.

**Théorème 1.2.19.** *Soient un champ* $\mathbf{K}$ *et* $\mathbf{C}$ *une extension de champ de* $\mathbf{K}$ *qui est algébriquement close. Alors il existe* $\overline{\mathbf{K}}$ *une unique clôture algébrique de* $\mathbf{K}$ *incluse dans* $\mathbf{C}$.

**Définition 1.2.20.** Un anneau commutatif intègre est factoriel si tout élément non nul et non inversible est un produit fini d'éléments irréductibles et si la factorisation est unique à permutation près et à facteurs inversibles près.

**Proposition 1.2.21.** *Si* $\mathbf{K}$ *est un champ alors l'anneau des polynômes* $\mathbf{K}[X]$ *est factoriel.*

**Théorème 1.2.22.** *Soit* $\mathbf{K}$ *un champ et* $P \in \mathbf{K}[X]$ *un polynôme irréductible sur* $\mathbf{K}$. *Alors* $\mathbf{K}[X]/\langle P\rangle$ *est une extension de champ de* $\mathbf{K}$. *De plus,* $P$ *admet une racine dans* $\mathbf{K}[X]/\langle P\rangle$ *qui est* $X + \langle P\rangle$.

## 1.3 Polynômes multivariés et polynômes symétriques

On peut étendre la définition 1.2.1 afin de considérer des polynômes en plusieurs indéterminées. Pour ce faire, on construit l'ensemble $\mathbf{D}[X_1, \ldots, X_n]$ récursivement en définissant

$$\mathbf{D}[X_1, \ldots, X_n] = (\mathbf{D}[X_1, \ldots, X_{n-1}])[X_n].$$

Donc si $P \in \mathbf{D}[X_1, \ldots, X_n]$, $P$ s'écrit sous la forme

$$P = P_d X_n^d + \ldots + P_1 X_n + P_0$$

où $P_0, \ldots, P_d \in \mathbf{D}[X_1, \ldots, X_{n-1}]$. En développant entièrement cette expression, on obtient une expression de la forme

$$P = \sum_{j=0}^{J} c_j \prod_{k=1}^{n} X_k^{\alpha_{j,k}}.$$

avec $J \in \mathbb{N}$ et pour tout $j \in \{0 \ldots, J\}, k \in \{1, \ldots, n\}$, $c_j \in \mathbf{D}$ et $\alpha_{j,k} \in \mathbb{N}$. Le degré d'un tel polynôme est défini comme le degré maximum de ses monômes qu'on définit comme suit

$$\deg(\prod_{k=1}^{n} X_k^{\alpha_{j,k}}) = \sum_{k=1}^{n} \alpha_{j,k}.$$

De plus, pour tout $k \in \{1, \ldots, n\}$, nous notons $\deg_{X_k}(P)$ et $\mathrm{lcof}_{X_k}(P)$ le degré et le terme de plus haut degré du polynôme multivarié $P$ vu comme un polynôme univarié à coefficients dans l'anneau $\mathbf{D}[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$.

**Exemple 1.3.1.** Considérons $P = X_1X_2^2X_4 - 2X_3X_4 + 5X_1^3X_4 \in \mathbb{Z}[X_1, X_2, X_3, X_4]$. Le degré de ses monômes sont respectivement, $1+2+1 = 4$, $1+1 = 2$ et $3+1 = 4$. Dès lors, $\deg(P) = 4$. De plus,

$$\begin{aligned}
&\deg_{X_1}(P) = 3 \text{ et } \mathrm{lcof}_{X_1}(P) = 5X_4,\\
&\deg_{X_2}(P) = 2 \text{ et } \mathrm{lcof}_{X_2}(P) = X_1X_4,\\
&\deg_{X_3}(P) = 1 \text{ et } \mathrm{lcof}_{X_3}(P) = -2X_4,\\
&\deg_{X_4}(P) = 1 \text{ et } \mathrm{lcof}_{X_4}(P) = X_1X_2^2 - 2X_3 + 5X_1^3.
\end{aligned}$$

Maintenant qu'on a défini les polynômes multivariés, nous allons définir les polynômes symétriques. Cette partie est basée sur [7, chap. IV.6] et a pour but d'obtenir le résultat 1.3.14 qui nous indique que si les racines de $P \in \mathbf{F}[X]$ notées $x_1, \ldots, x_n \in \mathbf{C}$ (où $\mathbf{C}$ est un champ algébriquement clos contenant le champ $\mathbf{F}$) et si $Q \in \mathbf{F}[X_1, \ldots, X_n]$ est un polynôme symétrique en $X_1, \ldots, X_n$ alors $Q(x_1, \ldots, x_n) \in \mathbf{F}$. Cette proposition nous servira dans la démonstration du théorème 2.2.3 qui caractérise les champs réels clos. Commençons par donner quelques définitions et résultats nécessaires dans la suite de la section.

On commence naturellement par définir ce qu'est un polynôme symétrique.

**Définition 1.3.2.** Un polynôme $P \in \mathbf{D}[X_1, \ldots, X_n]$ est dit symétrique si

$$P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

pour toute permutation $\sigma$ de $\{1, \ldots, n\}$.

**Définition 1.3.3.** Soit $n \in \mathbb{N}_0$, pour tout $k \in \{1, \ldots, n\}$ on définit le polynôme $s_k^{(n)} \in \mathbf{D}[X_1, \ldots, X_n]$ par

$$s_k^{(n)} = \sum_{1 \le j_1 < \ldots < j_k \le n} X_{j_1} \ldots X_{j_k}.$$

Ces polynômes sont les polynômes symétriques élémentaires en $(X_1, \ldots, X_n)$. On remarque que pour tout $k \in \{1, \ldots, n\}$,

$$\deg(s_k^{(n)}) = k.$$

Par ailleurs, le polynôme $s_k^{(n)}$ est obtenu en sommant les produits de k indéterminées distinctes parmi $n$, de toutes les façons possibles. On peut donc le réécrire de la façon suivante :

$$s_k^{(n)} = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=k}} \prod_{i \in I} X_i.$$

Il est alors clair que ceux-ci sont bien symétriques. De plus, on prend la convention que $s_0^{(n)} = 1$ et $s_k^{(n)} = 0$ pour tout $k \notin \{0, \dots, n\}$.

**Exemple 1.3.4.** En appliquant cette définition, on montre que les polynômes symétriques élémentaires de $\mathbb{Z}[X_1, X_2, X_3]$ sont

$$\begin{aligned} s_1^{(3)} &= X_1 + X_2 + X_3, \\ s_2^{(3)} &= X_1X_2 + X_2X_3 + X_1X_3, \\ s_3^{(3)} &= X_1X_2X_3. \end{aligned}$$

**Lemme 1.3.5.** *Soit $n \in \mathbb{N}_0$, on a*

$$s_k^{(n)} + s_{k-1}^{(n)} X_{n+1} = s_k^{(n+1)}$$

*pour tout $k \in \{1, \dots, n+1\}$.*

*Démonstration.* Au vu de la définition 1.3.3, $s_k^{(n)}$ est la somme des produits de $k$ éléments dans $\{X_1, \dots, X_n\}$. Autrement dit, c'est la somme des produits de $k$ éléments dans $\{X_1, \dots, X_{n+1}\}$ ne contenant pas $X_{n+1}$. De même, $s_{k-1}^{(n)}$ est la somme des produits de $k-1$ éléments dans $\{X_1, \dots, X_n\}$. Si on multiplie le terme précédent par $X_{n+1}$ on obtient la somme des produits de $k$ éléments dans $\{X_1, \dots, X_n, X_{n+1}\}$ qui contiennent $X_{n+1}$. Dès lors, $s_k^{(n)} + s_{k-1}^{(n)} X_{n+1}$ est la somme des produits de $k$ éléments dans $\{X_1, \dots, X_{n+1}\}$. Autrement dit, c'est $s_k^{(n+1)}$. □

**Lemme 1.3.6.** *Soit $n \in \mathbb{N}_0$, on a*

$$(X - X_1) \dots (X - X_n) = X^n - s_1^{(n)} X^{n-1} + \dots + (-1)^n s_n^{(n)}.$$

*Démonstration.* Procédons par récurrence sur $n$. Si $n = 1$, c'est direct car $s_1^{(1)} = X_1$. Supposons le résultat vérifié pour $n$ et prouvons le pour $n+1$. Par hypothèse de récurrence, on a

$$(X - X_1) \dots (X - X_{n+1}) = (X^n - s_1^{(n)} X^{n-1} + \dots + (-1)^n s_n^{(n)})(X - X_{n+1}).$$

On réécrit alors la somme avec un symbole sommatoire afin d'obtenir

$$\left( \sum_{k=0}^{n} (-1)^k s_k^{(n)} X^{n-k} \right) (X - X_{n+1}).$$

En distribuant ce produit, on a alors

$$\left(\sum_{k=0}^{n}(-1)^k s_k^{(n)} X^{n+1-k}\right) - \left(\sum_{k=0}^{n}(-1)^k s_k^{(n)} X_{n+1} X^{n-k}\right).$$

Nous allons alors décaler l'indice sommatoire de la seconde somme pour obtenir

$$\left(\sum_{k=0}^{n}(-1)^k s_k^{(n)} X^{n+1-k}\right) - \left(\sum_{k=1}^{n+1}(-1)^{k-1} s_{k-1}^{(n)} X_{n+1} X^{n+1-k}\right).$$

Par convention, $s_{-1}^{(n)} = s_{n+1}^{(n)} = 0$, on a alors

$$\left(\sum_{k=0}^{n+1}(-1)^k s_k^{(n)} X^{n+1-k}\right) - \left(\sum_{k=0}^{n+1}(-1)^{k-1} s_{k-1}^{(n)} X_{n+1} X^{n+1-k}\right).$$

On réunit les deux sommes afin d'obtenir

$$\sum_{k=0}^{n+1}(-1)^k (s_k^{(n)} + s_{k-1}^{(n)} X_{n+1}) X^{n+1-k}.$$

Au vu du lemme 1.3.5, on obtient finalement

$$\sum_{k=0}^{n+1}(-1)^k s_k^{(n+1)} X^{n+1-k},$$

ce qui est bien l'expression recherchée. □

**Définition 1.3.7.** Soit un polynôme $P \in \mathbf{D}[X_1, \ldots, X_n]$. On définit le polynôme symétrique associé à $P$, noté $P(s_1^{(n)}, \ldots, s_n^{(n)})$, qui est le polynôme de $\mathbf{D}[X_1, \ldots, X_n]$ où on a remplacé dans $P$ les expressions de $X_j$ par le polynôme $s_j^{(n)} \in \mathbf{D}[X_1, \ldots, X_n]$ pour tout $j \in \{1, \ldots, n\}$.

**Exemple 1.3.8.** Considérons le polynôme $P \in \mathbb{Z}[X_1, X_2, X_3]$ défini par

$$P = X_1^2 X_3 - 4X_2^2 X_1,$$

Le polynôme symétrique associé est alors le polynôme

$$P(s_1^{(3)}, s_2^{(3)}, s_3^{(3)}) \in \mathbb{Z}[X_1, X_2, X_3]$$

défini par

$$P(s_1^{(3)}, s_2^{(3)}, s_3^{(3)}) = (X_1 + X_2 + X_3)^2 (X_1 X_2 X_3) - 4(X_1 X_2 + X_1 X_3 + X_2 X_3)^2 (X_1 + X_2 + X_3).$$

Par la suite, on aura besoin de connaître le degré de polynôme symétrique associé à $P$ afin d'effectuer une récurrence dans la démonstration du théorème 1.3.12. Pour cela, on peut associer au polynôme $P$ un nombre, ce nombre est son poids, défini comme suit.

**Définition 1.3.9.** On définit le poids d'un monôme $cX_1^{\alpha_1} \dots X_n^{\alpha_n}$ comme étant $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n$. On étend cette définition à tout polynôme $P \in \mathbf{D}[X_1, \dots, X_n]$ en définissant son poids comme le maximum des poids de ses monômes.

**Proposition 1.3.10.** *Soit $P \in \mathbf{D}[X_1, \dots, X_n]$. Le poids de $P$ est égal au degré du polynôme $P(s_1^{(n)}, \dots, s_n^{(n)})$.*

*Démonstration.* Supposons que le polynôme $P$ ne contient qu'un seul monôme. On a

$$P = cX_1^{\alpha_1} \dots X_n^{\alpha_n}.$$

On a alors

$$P(s_1^{(n)}, \dots, s_n^{(n)}) = c \prod_{k=1}^{n} (s_k^{(n)}(X_1, \dots, X_n))^{\alpha_k}.$$

Étant donné que $\deg(s_k^{(n)}) = k$, le degré de $P(s_1^{(n)}, \dots, s_n^{(n)})$ est donné par

$$\sum_{k=1}^{n} \deg(s_k^{(n)})\alpha_k = \sum_{k=1}^{n} k\alpha_k.$$

Ce qui est égal au poids de $P$. □

**Exemple 1.3.11.** Reprenons l'exemple 1.3.8. Le poids du polynôme

$$P = X_1^2 X_3 - 4X_2^2 X_1,$$

est 5. C'est exactement le degré du polynôme symétrique associé

$$P(s_1^{(3)}, s_2^{(3)}, s_3^{(3)}) = (X + Y + Z)^2(XYZ) - 4(XY + XZ + YZ)^2(X + Y + Z).$$

En partant de n'importe quel polynôme $P \in \mathbf{D}[X_1, \dots, X_n]$ on peut obtenir son polynôme symétrique associé $P(s_1^{(n)}, \dots, s_n^{(n)}) \in \mathbf{D}[X_1, \dots, X_n]$. Le théorème suivant montre que réciproquement, à partir d'un polynôme symétrique $P$, on peut trouver un polynôme $Q$ dont $P$ est le polynôme symétrique associé.

**Théorème 1.3.12.** *Soit $P \in \mathbf{D}[X_1, \dots, X_n]$ un polynôme symétrique de degré $d$. Alors il existe un polynôme $Q \in \mathbf{D}[X_1, \dots, X_n]$ de poids $\leq d$ tel que*

$$P = Q(s_1^{(n)}, \dots, s_n^{(n)}).$$

*Démonstration.* Procédons à une double récurrence. Tout d'abord sur le nombre $n \in \mathbb{N}_0$ d'indéterminées, puis sur le degré $d \in \mathbb{N}$ de $P$. Tout d'abord, si $n = 1$ le résultat est direct car $s_1^{(1)} = X_1$ et donc $Q = P$ convient. Supposons le résultat vérifié pour $n-1$ indéterminées et démontrons que c'est toujours le cas pour $n \geq 2$. Effectuons la récurrence sur le degré $d$ du polynôme $P$. Si $d = 0$ alors $P$ est une constante et le résultat est évident. Supposons que le résultat est vérifié pour les polynômes de degrés $< d$ (en supposant $d > 0$). Soit $P \in \mathbf{D}[X_1, \ldots, X_n]$ de degré $d$, on applique l'hypothèse de récurrence (sur $n$) au polynôme $P(X_1, \ldots, X_{n-1}, 0)$. Il existe alors un polynôme $Q_1 \in \mathbf{D}[X_1, \ldots, X_{n-1}]$ de poids $\leq d$ tel que

$$P(X_1, \ldots, X_{n-1}, 0) = Q_1(s_1^{(n-1)}, \ldots, s_{n-1}^{(n-1)}).$$

Par la proposition 1.3.10, on sait que

$$\deg(Q_1(s_1^{(n)}, \ldots, s_{n-1}^{(n)})) \leq d.$$

Considérons le polynôme $P_1 \in \mathbf{D}[X_1, \ldots, X_n]$ défini par

$$P_1 = P - Q_1(s_1^{(n)}, \ldots, s_{n-1}^{(n)})$$

qui est de degré $\leq d$. De plus, comme $P$ et $Q_1(s_1^{(n)}, \ldots, s_{n-1}^{(n)})$ sont symétriques, $P_1$ l'est également. Par ce qui précède, on a

$$P_1(X_1, \ldots, X_{n-1}, 0) = 0.$$

On en déduit que $X_n$ est un facteur de $P_1$, et par symétrie, que $s_n^{(n)}$ est un facteur de $P_1$. Dès lors, il existe un polynôme $P_2 \in \mathbf{D}[X_1, \ldots, X_n]$ tel que

$$P_1 = s_n^{(n)} P_2$$

et donc $\deg(P_2) \leq d - n < d$. Par hypothèse de récurrence (sur $d$), il existe $Q_2 \in \mathbf{D}[X_1, \ldots, X_n]$ de poids $\leq d - n$ tel que

$$P_2 = Q_2(s_1^{(n)}, \ldots, s_n^{(n)}).$$

On en déduit alors que

$$P = Q_1(s_1^{(n)}, \ldots, s_{n-1}^{(n)}) + s_n^{(n)} Q_2(s_1^{(n)}, \ldots, s_n^{(n)}).$$

Le polynôme $Q \in \mathbf{D}[X_1, \ldots, X_n]$ défini par

$$Q = Q_1 + X_n Q_2$$

convient. □

Ce théorème est un des deux résultats dont on a besoin pour la preuve de la proposition 1.3.14. Le deuxième est le lemme qui suit, pour lequel on considère un champ $\mathbf{F}$.

**Lemme 1.3.13.** *Soit $P \in \mathbf{F}[X]$ un polynôme de degré $n$. Si ses racines sont $x_1, \ldots, x_n$ dans un champ algébriquement clos $\mathbf{C}$ contenant $\mathbf{F}$. Alors pour tout $k \in \{1, \ldots, n\}$, on a*

$$s_k^{(n)}(x_1, \ldots, x_n) \in \mathbf{F}\,.$$

*Démonstration.* Supposons que $P$ est monique. On a $P = (X - x_1)\ldots(X - x_n)$. Par le lemme 1.3.6, on a que

$$P = X^n - s_1^{(n)}(x_1, \ldots, x_n)X^{n-1} + \ldots + (-1)^n s_n^{(n)}(x_1, \ldots, x_n) \in \mathbf{F}[X].$$

On en déduit que $s_k^{(n)}(x_1, \ldots, x_n) \in \mathbf{F}$ car par définition d'un polynôme, cette décomposition est unique. □

On peut désormais démontrer le résultat qui a motivé cette section et dont on se sert dans la démonstration du théorème 2.2.3.

**Proposition 1.3.14.** *Soit $f \in \mathbf{F}[X]$ un polynôme de degré $n$, de racines $x_1, \ldots, x_n$ (répétées selon leur multiplicité respective) dans un champ algébriquement clos $\mathbf{C}$ contenant $\mathbf{F}$. Si un polynôme $P \in \mathbf{F}[X_1, \ldots, X_n]$ est symétrique, alors*

$$P(x_1, \ldots, x_n) \in \mathbf{F}\,.$$

*Démonstration.* Pour tout $k \in \{1, \ldots, n\}$, on pose $e_k = s_k^{(n)}(x_1, \ldots, x_n)$. Comme $f \in \mathbf{F}[X]$, par le lemme 1.3.13, $e_k \in \mathbf{F}$. De plus, par le théorème 1.3.12, il existe $Q \in \mathbf{F}[X_1, \ldots, X_n]$ tel que

$$P = Q(s_1^{(n)}, \ldots, s_n^{(n)}).$$

Dès lors, $P(x_1, \ldots, x_n) = Q(e_1, \ldots, e_n) \in \mathbf{F}$. □

# Chapitre 2

# Champs réels clos

Dans cette section nous allons introduire les notions de champ réel et de champ réel clos. La théorie des champs réels clos a été développée au début du $20^e$ siècle par les mathématiciens allemands Emil Artin et Otto Schreier. Cette théorie a notamment été utilisée par Artin afin de résoudre le $17^e$ problème de Hilbert [1, p. 91].

Nous développons la théorie des champs réels clos dans ce travail car c'est dans ce contexte que nous allons en grande partie travailler dans la suite. Ce chapitre est principalement inspiré de [2, chap. 1].

## 2.1 Champs ordonnés et réels

Dans un premier temps, nous allons définir les anneaux et les champs ordonnés et introduire la notion de champ réel.

**Définition 2.1.1.** Un champ (resp. anneau) ordonné est un couple $(\mathbf{F}, \leq)$ où $\mathbf{F}$ est un champ (resp. anneau) et $\leq$ un ordre total sur $\mathbf{F}$ compatible avec l'addition, c'est à dire que si $x \leq y$ alors pour tout $z \in \mathbf{F}$ on a

$$x + z \leq y + z$$

et compatible avec la multiplication, c'est à dire que si $0 \leq x$ et $0 \leq y$ on a

$$0 \leq xy.$$

Par abus de langage, on parlera d'un anneau ou un champ ordonné $\mathbf{F}$ s'il n'y a pas de risque de confusion et on notera également $y \geq x$ si $x, y \in \mathbf{F}$ satisfont $x \leq y$.

**Définition 2.1.2.** Soit $\mathbf{F}$ un champ ordonné. On définit la valeur absolue sur $\mathbf{F}$ par

$$|\cdot| : \mathbf{F} \to \mathbf{F} : x \mapsto \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

**Proposition 2.1.3.** *Soit* $\mathbf{F}$ *un champ ordonné et* $x \in \mathbf{F}$*, alors* $x^2$ *est positif. En particulier, on a* $-1 < 0 < 1$*.*

*Démonstration.* Pour tout $x \in \mathbf{F}$, on a $x^2 = (-x)^2$. Or si $x < 0$ on a $0 = x + (-x) < 0 + (-x) = -x$ donc $-x > 0$. Si $x \geq 0$ c'est direct par définition d'un champ ordonné. Si $x < 0$ alors $-x > 0$ donc $x^2 = (-x)^2 > 0$. □

Comme exemple d'anneau ordonné, on peut citer $\mathbb{Z}$, avec l'ordre usuel, tandis que $\mathbb{Q}$, muni de l'ordre usuel est un champ ordonné. Pour dépasser ces exemples simples, regardons les anneaux de polynômes.

**Exemple 2.1.4.** L'anneau des polynômes à coefficients dans un anneau ordonné est lui-même un anneau ordonné. En effet, si $\mathbf{F}$ est un anneau ordonné, on peut munir $\mathbf{F}[X]$ de l'ordre suivant. Soit $P, Q \in \mathbf{F}[X]$ tels que

$$P = p_n X^n + \ldots + p_0 \text{ et } Q = q_m X^m + \ldots + q_0$$

On note $P < Q$ si et seulement si il existe $k \in \mathbb{N}$ tel que

$$p_k < q_k \text{ et } p_i = q_i$$

pour tout $i < k$ (c'est en fait, l'ordre lexicographique sur les polynômes). De plus, soient $P, Q \in \mathbf{F}[X]$ tels que $P, Q > 0$. Alors on a $P + Q > 0$, $PQ > 0$ et si $Q|P$ alors $\frac{P}{Q} > 0$. En effet, il suffit de regarder le terme de plus petit degré du polynôme obtenu.

**Exemple 2.1.5.** De plus, si $\mathbf{F}$ est un anneau intègre, alors par la proposition 1.2.3 on sait que $\mathbf{F}[X]$ est également un anneau intègre et on peut alors considérer son corps des fractions, noté $\mathbf{F}(X)$. Montrons que $\mathbf{F}(X)$ peut également être ordonné. Soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2} \in \mathbf{F}(X)$.On définit alors que

$$\frac{P_1}{Q_1} < \frac{P_2}{Q_2}$$

si et seulement si

$$(P_2 Q_1 - P_1 Q_2)(Q_1 Q_2) > 0$$

pour l'ordre de $\mathbf{F}[X]$ et

$$\frac{P_1}{Q_1} = \frac{P_2}{Q_2}$$

si et seulement si

$$(P_2 Q_1 - P_1 Q_2)(Q_1 Q_2) = 0.$$

Vérifions que $\mathbf{F}(X)$ muni de cette relation est un champ ordonné. En effet, il suffit de regarder le terme de plus petit degré du polynôme obtenu.

1. La réflexivité se vérifie directement.

2. La relation est transitive. En effet, soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3} \in \mathbf{F}(X)$ tels que

$$\frac{P_1}{Q_1} \leq \frac{P_2}{Q_2} \text{ et } \frac{P_2}{Q_2} \leq \frac{P_3}{Q_3}.$$

Montrons que

$$\frac{P_1}{Q_1} \leq \frac{P_3}{Q_3}.$$

On a

$$(P_2Q_1 - P_1Q_2)(Q_1Q_2) \geq 0 \text{ et } (P_3Q_2 - P_2Q_3)(Q_2Q_3) \geq 0$$

En multipliant ces inéquations par $(Q_3)^2$ et $(Q_1)^2$ respectivement

$$(Q_1Q_2Q_3)(P_2Q_1Q_3 - P_1Q_2Q_3) \geq 0 \text{ et } (Q_1Q_2Q_3)(P_3Q_1Q_2 - P_2Q_1Q_3) \geq 0$$

En sommant ces inégalités, et en divisant par $Q_2^2$ on obtient que

$$(P_3Q_1 - P_1Q_3)(Q_1Q_3) \geq 0$$

et donc

$$\frac{P_1}{Q_1} \leq \frac{P_3}{Q_3}.$$

3. La relation est antisymétrique. Soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2} \in \mathbf{F}(X)$ tels que

$$\frac{P_1}{Q_1} \geq \frac{P_2}{Q_2} \text{ et } \frac{P_1}{Q_1} \leq \frac{P_2}{Q_2}.$$

On a alors

$$\frac{P_1}{Q_1} = \frac{P_2}{Q_2}.$$

Sinon, on aurait

$$\frac{P_1}{Q_1} < \frac{P_2}{Q_2} \text{ et } \frac{P_1}{Q_1} > \frac{P_2}{Q_2}.$$

Autrement dit,

$$(P_1Q_2 - P_2Q_1)(Q_1Q_2) > 0$$

et

$$(P_1Q_2 - P_2Q_1)(Q_1Q_2) < 0.$$

Cela est impossible étant donné qu'il s'agit d'un ordre sur $\mathbf{F}[X]$.

L'ensemble $\mathbf{F}(X)$ est donc muni d'une relation d'ordre. De plus, cet ordre est total car le terme de plus petit degré de

$$(P_1Q_2 - P_2Q_1)(Q_1Q_2)$$

est forcément soit nul (si polynôme nul) auquel cas $\frac{P_1}{Q_1} = \frac{P_2}{Q_2}$, soit strictement positif auquel cas $\frac{P_1}{Q_1} > \frac{P_2}{Q_2}$ ou enfin strictement négatif auquel cas on a $\frac{P_1}{Q_1} < \frac{P_2}{Q_2}$.

Enfin, cet ordre fait de $\mathbf{F}(X)$ un champ ordonné car il est compatible avec l'addition et la multiplication. En effet, si $\frac{P_1}{Q_1}, \frac{P_2}{Q_2} > 0$, on a

$$\frac{P_1}{Q_1}\frac{P_2}{Q_2} = \frac{P_1P_2}{Q_1Q_2} > 0$$

car $(P_1Q_1)(P_2Q_2) = (P_1P_2)(Q_1Q_2)$. Cet ordre est donc compatible avec la multiplication. De plus, soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}$ tels que

$$\frac{P_1}{Q_1} \leq \frac{P_2}{Q_2}.$$

On a

$$\frac{P_1}{Q_1} + \frac{P_3}{Q_3} = \frac{P_1Q_3 + P_3Q_1}{Q_1Q_3}$$

et

$$\frac{P_2}{Q_2} + \frac{P_3}{Q_3} = \frac{P_2Q_3 + P_3Q_2}{Q_2Q_3}.$$

Dès lors,

$$\frac{P_1}{Q_1} + \frac{P_3}{Q_3} \leq \frac{P_2}{Q_2} + \frac{P_3}{Q_3}$$

si et seulement si

$$((P_2Q_3 + P_3Q_2)(Q_1Q_3) - (P_1Q_3 + P_3Q_1)(Q_2Q_3))\,(Q_1Q_2Q_3^2) \geq 0$$

En divisant par $Q_3^4$, on obtient

$$(P_2Q_1 - P_1Q_2)(Q_1Q_2) \geq 0.$$

Cette inégalité est équivalente à l'hypothèse $\frac{P_1}{Q_1} \leq \frac{P_2}{Q_2}$. L'ordre est donc compatible avec l'addition. On a alors montré que le corps des fractions $\mathbf{F}(X)$ muni de cette relation est un champ ordonné.

En réalité, on peut adapter l'exemple précédent afin de montrer de manière générale que le corps des fractions d'un anneau intègre ordonné est un champ ordonné.

**Proposition 2.1.6.** *Un champ ordonné est toujours de caractéristique nulle.*

*Démonstration.* $1 > 0$ donc $1 + 1 > 0 + 1 > 0$ ainsi de suite on a $\sum_{k=1}^{n} 1 > 0$ pour tout $n \in \mathbb{N}_0$ et donc le champ est de caractéristique nulle. □

On va désormais définir la notion de cône d'un champ ordonné. Cette définition est utile car on verra dans la proposition 2.1.10 qu'il y a une équivalence entre certains cônes du champ $\mathbf{F}$ et les ordres possibles pour le champ $\mathbf{F}$.

**Définition 2.1.7.** Un cône d'un champ $\mathbf{F}$ est un sous-ensemble C de $\mathbf{F}$ tel que pour tout $x, y \in \mathrm{C}$, on a

1) $x + y \in \mathrm{C}$
2) $xy \in \mathrm{C}$
3) $\mathbf{F}^{(2)} = \{x^2 : x \in \mathbf{F}\} \subseteq \mathrm{C}$

Un cône est dit propre si $-1 \notin \mathrm{C}$.

En général un sous-ensemble "propre" d'un ensemble signifie qu'il est non vide et strictement inclus dans cet ensemble. La proposition suivante justifie la définition utilisée ici.

**Proposition 2.1.8.** *Soit* $\mathbf{F}$ *un champ ordonné et* C *un cône de* $\mathbf{F}$. *Si* $-1 \in \mathrm{C}$ *alors* $\mathrm{C} = \mathbf{F}$.

*Démonstration.* Soit $x \in \mathbf{F}$, comme $\{x^2 : x \in \mathbf{F}\} \subseteq \mathrm{C}$ et $-1 \in \mathrm{C}$, on a

$$x = \left(\frac{1}{2}\right)^2 \left((x+1)^2 + (-1)(x + (-1))^2\right) \in \mathrm{C}.$$

□

**Définition 2.1.9.** Soit $(\mathbf{F}, \leq)$ un champ ordonné. Le sous-ensemble

$$\mathrm{P} = \{x \geq 0 : x \in \mathbf{F}\}$$

est appelé le cône positif de $\mathbf{F}$.

**Proposition 2.1.10.** *Si* $(\mathbf{F}, \leq)$ *est un champ ordonné alors le cône positif de* $\mathbf{F}$ *est un cône propre satisfaisant*

$$\mathrm{P} \cup -\mathrm{P} = \mathbf{F}$$

*où* $-\mathrm{P} = \{-x : x \in \mathrm{P}\}$. *Réciproquement, si* C *est un cône propre d'un champ* $\mathbf{F}$ *satisfaisant cette propriété alors il existe un unique ordre* $\leq$ *sur* $\mathbf{F}$ *dont* C *est le cône positif. Cet unique ordre est défini par*

$$x \leq y \Leftrightarrow y - x \in \mathrm{C}.$$

*Démonstration.* Montrons que P est un cône. Si on a $x, y \geq 0$, par la définition d'un champ ordonné, on sait que $x + y \geq x \geq 0$ et que $xy \geq 0$. Par la proposition 2.1.3, on tire que P est un cône de $\mathbf{F}$. De plus, par cette même proposition, on conclut que P est propre. Enfin, pour tout $x \in \mathbf{F}$, on a $x \geq 0$ ou $-x \geq 0$ donc

$$\mathrm{P} \cup -\mathrm{P} = \mathbf{F}\,.$$

Prouvons la réciproque. Pour l'unicité, on note que si $\leq$ est un ordre sur $\mathbf{F}$, on a bien sûr $x \leq y \Leftrightarrow 0 \leq y - x$. Si C est le cône positif de $\leq$, cette relation équivaut à $y - x \in \mathrm{C}$, donc C définit univoquement $\leq$. Pour l'existence, il faut donc vérifier que

$$x \leq y \Leftrightarrow y - x \in \mathrm{C},$$

définit bien un ordre total sur le champ $\mathbf{F}$.

1) Si $x \leq y$ et $y \leq z$ on a $z - y \in \mathrm{C}$ et $y - x \in \mathrm{C}$ et donc
$$z - x = (z - y) + (y - x) \in \mathrm{C},$$
donc $x \leq z$ et la relation est bien transitive.
2) Soit $x \in \mathbf{F}$, on a $x - x = 0 \in \mathrm{C}$ car $0 = 0^2 \in \mathrm{C}$ donc $x \leq x$, et la relation est réflexive.
3) Si $x \leq y$ on a $y - x \in \mathrm{C}$ et donc $x - y \in -\mathrm{C}$. Or si $x \geq y$ on a $x - y \in \mathrm{C}$ et donc $x - y \in \mathrm{C} \cap -\mathrm{C}$. Donc $x = y$ car $x - y = 0$. En effet, si $x \in \mathrm{C} \cap -\mathrm{C}$ alors $-x \in \mathrm{C} \cap -\mathrm{C}$. Donc si on a $\frac{1}{x} \in \mathrm{C}$, alors
$$-1 = (-1)(x)(\frac{1}{x}) = (-x)(\frac{1}{x}) \in \mathrm{C},$$
ce qui est absurde car le cône est propre. Tandis que si on a $\frac{1}{x} \in -\mathrm{C}$ alors on a $-\frac{1}{x} \in \mathrm{C}$ et on obtient également que $-1 \in \mathrm{C}$. La relation est donc antisymétrique.
4) L'ordre est total car $\mathbf{F} = \mathrm{C} \cup -\mathrm{C}$.

On a bien une relation d'ordre total. Vérifions que le champ $\mathbf{F}$ muni de cet ordre satisfait bien la définition d'un champ ordonné.

5) Si $x \leq y$ on a $y - x \in \mathrm{C}$ donc pour tout $z \in \mathbf{F}$, on a
$$(y + z) - (x + z) = y - x \in \mathrm{C},$$
d'où $x + z \leq y + z$.
6) Si $x \geq 0$ et $y \geq 0$ on a alors $x \in \mathrm{C}$ et $y \in \mathrm{C}$. Dès lors, $xy \in \mathrm{C}$ d'où $xy \geq 0$.

Enfin, le cône positif pour cet ordre est visiblement C. □

**Proposition 2.1.11.** *Soit* $\mathbf{F}$ *un champ ordonné. L'ensemble* $\Sigma_{\mathbf{F}}^{(2)}$ *des sommes de carrés d'éléments de* $\mathbf{F}$ *est un cône. De plus, celui-ci est contenu dans tous les cônes de* $\mathbf{F}$.

*Démonstration.* Si $x, y \in \Sigma_{\mathbf{F}}^{(2)}$, il existe $x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathbf{F}$ tels que
$$x = x_1^2 + \ldots + x_n^2 \text{ et } y = y_1^2 + \ldots + y_m^2,$$
dès lors,
$$x + y = x_1^2 + \ldots + x_n^2 + y_1^2 + \ldots + y_m^2 \in \Sigma_{\mathbf{F}}^{(2)}.$$
De plus,
$$\begin{aligned} xy &= (x_1^2 + \ldots + x_n^2)(y_1^2 + \ldots + y_m^2), \\ &= (x_1^2 y_1^2 + \ldots + x_1^2 y_m^2 + \ldots + x_n^2 y_1^2 + \ldots + x_n^2 y_m^2), \\ &= (x_1 y_1)^2 + \ldots + (x_1 y_m)^2 + \ldots + (x_n y_1)^2 + \ldots + (x_n y_m)^2 \in \Sigma_{\mathbf{F}}^{(2)}. \end{aligned}$$
Enfin, il est évident que $z^2 \in \Sigma_{\mathbf{F}}^{(2)}$ pour tout $z \in \mathbf{F}$. On a donc bien un cône de $\mathbf{F}$. Montrons qu'il est inclus dans tous les cônes de $\mathbf{F}$. C'est direct étant donné que $x^2 \in \mathrm{C}$ pour tout $x \in \mathbf{F}$ et pour tout cône C de $\mathbf{F}$. On conclut étant donné que la somme d'éléments d'un cône est toujours un élément du cône. □

Par la suite, on va définir les champs réels (qui sont les champs pouvant être ordonnés). Dans le théorème 2.1.15, on va montrer qu'il en existe plusieurs définitions équivalentes. Pour démontrer ce théorème nous avons besoin du lemme 2.1.13. Le résultat suivant sert a pouvoir appliquer le lemme de Zorn dans sa démonstration.

**Lemme 2.1.12.** *L'union des éléments d'une chaîne de cônes propres est un cône propre.*

*Démonstration.* Soit $\{\mathrm{C}_i : i \in I\}$ une chaîne de cônes propres, c'est à dire un ensemble de cônes propres totalement ordonné par l'inclusion. Notons

$$\mathrm{C} = \bigcup_{i \in I} \mathrm{C}_i.$$

Montrons que C est un cône. Soient $x, y \in \mathrm{C}$. Étant donné que les cônes de la chaîne sont emboîtés, il existe $i \in I$ tel que $x, y \in \mathrm{C}_i$. Donc $x + y \in \mathrm{C}_i$ et $xy \in \mathrm{C}_i$ d'où $x + y \in \mathrm{C}$ et $xy \in \mathrm{C}$. De plus, $x^2 \in \mathrm{C}_i \subseteq \mathrm{C}$ pour tout $x \in \mathbf{F}$ et pour tout $i \in I$. On en déduit que C est un cône. De même, pour tout $i \in I$, $-1 \notin \mathrm{C}_i$ car les $\mathrm{C}_i$ sont des cônes propres. On en tire que $-1 \notin \mathrm{C}$ qui est donc également un cône propre. □

**Lemme 2.1.13.** *Soit* C *un cône propre de* $\mathbf{F}$ *et* $a \in \mathbf{F}$.

*1) Si* $-a \notin \mathrm{C}$ *alors* $\mathrm{C}[a] = \{x + ay : x, y \in \mathrm{C}\}$ *est un cône propre de* $\mathbf{F}$.

*2) Le cône* C *est contenu dans le cône positif d'un ordre de* $\mathbf{F}$.

*Démonstration.* 1) Soient $(x + ay), (z + at) \in \mathrm{C}[a]$. On a

$$(x + ay) + (z + at) = (x + z) + a(y + t) \in \mathrm{C}[a],$$

$$(x + ay)(z + at) = (xz + a^2yt) + a(xt + yz) \in \mathrm{C}[a],$$

étant donné que C est un cône et que $0 \in \mathrm{C}$, on a

$$\{x^2 : x \in \mathbf{F}\} \subseteq \mathrm{C} \subseteq \mathrm{C}[a],$$

donc $\mathrm{C}[a]$ est un cône de $\mathbf{F}$. Vérifions qu'il est propre. Supposons avoir $-1 = x + ay$ pour $x, y \in \mathrm{C}$. Alors soit $y = 0$, auquel cas on a $-1 = x$ ce qui est absurde car C est un cône propre, soit on a

$$-a = (x + 1)\frac{1}{y} = (x + 1)y\left(\frac{1}{y}\right)^2 \in \mathrm{C},$$

ce qui est également absurde. On en déduit que $-1 \notin \mathrm{C}[a]$.

2) Au vu du lemme 2.1.12, on peut appliquer le lemme de Zorn à l'ensemble des cônes propres ordonnés par l'inclusion. On en déduit qu'il existe un cône propre maximal $\overline{\mathrm{C}}$ contenant C. Par la proposition 2.1.10 il suffit alors de montrer que

$$\overline{\mathrm{C}} \cup -\overline{\mathrm{C}} = \mathbf{F}$$

et on obtient alors l'ordre $\leq$ sur $\mathbf{F}$ défini dans la proposition 2.1.10. Supposons que $-a \notin \overline{\mathrm{C}}$, par ce qui précède, on a que $\overline{\mathrm{C}}[a]$ est un cône propre, donc par maximalité de $\overline{\mathrm{C}}$ on déduit que $\overline{\mathrm{C}} = \overline{\mathrm{C}}[a]$ donc $a \in \overline{\mathrm{C}}$ d'où $-a \in -\overline{\mathrm{C}}$ et $\overline{\mathrm{C}} \cup -\overline{\mathrm{C}} = \mathbf{F}$.

□

Définissons alors les champs réels.

**Définition 2.1.14.** Un champ $\mathbf{F}$ est un champ réel si il peut être ordonné.

Le théorème qui suit nous montre qu'il existe plusieurs définitions équivalentes.

**Théorème 2.1.15.** *Soit un champ* $\mathbf{F}$*, les assertions suivantes sont équivalentes :*
*1)* $\mathbf{F}$ *est un champ réel,*
*2) pour tout* $x_1, \ldots, x_n \in \mathbf{F}$*, si on a*

$$\sum_{i=1}^{n} x_i^2 = 0$$

*cela implique que* $x_1 = \cdots = x_n = 0$*,*
*3)* $-1 \notin \Sigma_{\mathbf{F}}^{(2)}$*,*
*4) le champ* $\mathbf{F}$ *a un cône propre.*

*Démonstration.* 1) $\Rightarrow$ 2) Si $x_1 \neq 0$, par la proposition2.1.3 on a

$$\sum_{i=1}^{n} x_i^2 \geq x_1^2 > 0.$$

2) $\Rightarrow$ 3) On a $1^2 = 1$ donc il n'existe pas $x_1, \ldots, x_n \in \mathbf{F}$ tels que

$$1 + \sum_{i=1}^{n} x_i^2 = 0.$$

3) $\Rightarrow$ 4) Par la proposition 2.1.11 on sait que $\Sigma_{\mathbf{F}}^{(2)}$ est un cône, et par hypothèse il est propre.
4) $\Rightarrow$ 1) Par le lemme 2.1.13 on sait que le cône est contenu dans un cône positif d'un ordre de $\mathbf{F}$.

□

**Exemple 2.1.16.** Dans $\mathbb{C}$, on a $i^2 = -1$ donc par le théorème 2.1.15, on en tire que $\mathbb{C}$ n'est pas un champ réel et donc que celui-ci ne peut pas être ordonné. Par contre, les champs $\mathbb{R}$ et $\mathbb{Q}$ sont des champs réels car on peut les ordonner.

## 2.2 Champs réels clos

Nous allons définir les champs réels clos, un cas particulier de champs réels, car c'est dans ce contexte que nous allons travailler dans les chapitres qui suivent. Nous allons les définir puis montrer qu'il y a plusieurs définitions équivalentes (théorème 2.2.3). Ensuite nous allons voir des résultats équivalents à des résultats d'analyse classique concernant les polynômes à coefficients dans un champ réel clos et des résultats concernant les racines de ces polynômes.

### 2.2.1 Définition et équivalence, exemples

**Définition 2.2.1.** Un champ réel clos $\mathbf{F}$ est un champ réel qui n'a pas d'extension réelle algébrique non triviale. Autrement dit, il n'existe pas de champ réel $\mathrm{F}_1$ algébrique sur $\mathbf{F}$, contenant $\mathbf{F}$ et différent de $\mathbf{F}$.

Le lemme suivant servira dans la démonstration du théorème 2.2.3 et dans la démonstration de la proposition 2.2.9.

**Lemme 2.2.2.** *Si $\mathbf{F}[i] = \mathbf{F}[X]/\langle X^2+1\rangle$ est un champ algébriquement clos, alors les seuls facteurs irréductibles de degré $> 1$ de $\mathbf{F}[X]$ sont de la forme*

$$(X - c - id)(X - c + id) = (X - c)^2 + d^2,$$

*avec $c, d \in \mathbf{F}$ et $d \neq 0$.*

*Démonstration.* Comme $\mathbf{F}[i]$ est algébriquement clos, tout polynôme de $\mathbf{F}[X]$ se factorise complètement dans $(\mathbf{F}[i])[X]$. On regroupe alors les facteurs correspondants à des racines conjuguées n'appartenant pas à $\mathbf{F}$. Donc les seuls polynômes irréductibles sont de degré 1 ou 2. Ceux de degré 2 sont le produit de deux racines conjuguées et ont la forme annoncée. □

**Théorème 2.2.3.** *Soit un champ $\mathbf{F}$, les assertions suivantes sont équivalentes :*

*1) $\mathbf{F}$ est un champ réel clos,*

*2) il y a un (unique) ordre de $\mathbf{F}$ tel que*

$$\{x \geq 0 : x \in \mathbf{F}\} = \{x^2 : x \in \mathbf{F}\},$$

*et tel que tout polynôme $P \in \mathbf{F}[X]$ de degré impair admet une racine dans $\mathbf{F}$,*

*3) l'anneau*

$$\mathbf{F}[i] = \mathbf{F}[X]/\langle X^2+1\rangle,$$

*est un champ algébriquement clos.*

*Démonstration.* 1) $\Rightarrow$ 2) Soit $a \in \mathbf{F}$, si $a \notin \mathbf{F}^{(2)}$, alors

$$\mathbf{F}[\sqrt{a}] = \mathbf{F}[X]/\langle X^2 - a\rangle$$

est une extension algébrique non triviale de $\mathbf{F}$ par le théorème 1.2.22 et donc $\mathbf{F}[\sqrt{a}]$ n'est pas un champ réel. Au vu du théorème 2.1.15 on peut écrire $-1$ sous la forme

$$-1 = \sum_{i=1}^{n} (x_i + \sqrt{a}y_i)^2.$$

Or comme $-1 \in \mathbf{F}$, on en déduit que

$$-1 = \sum_{i=1}^{n} x_i^2 + a(\sum_{i=1}^{n} y_i^2) \in \mathbf{F}\,.$$

Comme $\mathbf{F}$ est réel, on en déduit que

$$-1 \neq \sum_{i=1}^{n} x_i^2,$$

et donc

$$y = \sum_{i=1}^{n} y_i^2 \neq 0.$$

Dès lors, on a

$$\begin{aligned} -a &= \left(\sum_{i=1}^{n} y_i^2\right)^{-1} \left(1 + \sum_{i=1}^{n} x_i^2\right) \\ &= \left(\sum_{i=1}^{n} \left(\frac{y_i}{y}\right)^2\right) \left(1 + \sum_{i=1}^{n} x_i^2\right) \in \Sigma_{\mathbf{F}}^{(2)}, \end{aligned}$$

car par la proposition 2.1.11, $\Sigma_{\mathbf{F}}^{(2)}$ est un cône. On en déduit donc que

$$\mathbf{F}^{(2)} \cup -\Sigma_{\mathbf{F}}^{(2)} = \mathbf{F}\,.$$

Étant donné que $\mathbf{F}^{(2)} \subseteq \Sigma_{\mathbf{F}}^{(2)}$ on a

$$\Sigma_{\mathbf{F}}^{(2)} \cup -\Sigma_{\mathbf{F}}^{(2)} = \mathbf{F},$$

et comme $\mathbf{F}$ est un champ réel, $\Sigma_{\mathbf{F}}^{(2)}$ est un cône propre donc par la réciproque de la proposition 2.1.10, on obtient un unique ordre sur $\mathbf{F}$ tel que

$$\mathrm{P} = \{x \geq 0 : x \in \mathbf{F}\} = \Sigma_{\mathbf{F}}^{(2)} = \mathbf{F}^{(2)}\,.$$

Montrons que si $f \in \mathbf{F}[X]$ est de degré impair alors $f$ admet une racine dans $\mathbf{F}$. Par l'absurde, soit $f \in \mathbf{F}[X]$, de degré $d > 1$ impair n'admettant pas de racine dans $\mathbf{F}$ tel que tous les polynômes de $\mathbf{F}[X]$ de degré impair $< d$ admettent une racine dans $\mathbf{F}$. Comme un polynôme de degré impair a au moins un facteur de degré impair irréductible, on en déduit que $f$ est irréductible. Donc le quotient $\mathbf{F}[X]/\langle f\rangle$ est une extension algébrique non triviale de $\mathbf{F}$. Par hypothèse, cette extension est non réelle, on peut alors écrire $[-1]$ sous la forme

$$[-1] = \sum_{i=1}^{n} [P_i]^2,$$

où $P_1, \ldots, P_n \in \mathbf{F}[X]$ et où $[P]$ désigne la classe de $P$ dans $\mathbf{F}[X]/\langle f\rangle$. Or pour tout $i \in \{1, \ldots, n\}$, il existe $h_i, g_i \in \mathbf{F}[X]$ tels que $\deg(h_i) < d$ et tels que

$$P_i = h_i + g_i f.$$

Il existe alors $h \in \mathbf{F}[X]$ tel que

$$-1 = \sum_{i=1}^{n}(h_i + fg_i)^2 + hf = \sum_{i=1}^{n} h_i^2 + (g_i^2 f + 2h_i g_i)f + hf.$$

En posant

$$g = \sum_{i=1}^{n} g_i^2 f + 2h_i g_i + h,$$

on a alors

$$-1 = \sum_{i=1}^{n} h_i^2 + gf, \tag{2.1}$$

avec $h_1, \ldots, h_n \in \mathbf{F}[X]$ et $g \in \mathbf{F}[X]$ et tel que $\deg(h_i) < d$ pour tout $i \in \{1, \ldots, n\}$. Le coefficient dominant du polynôme $h_1^2 + \ldots + h_n^2$ est de degré $\leq 2d-2$ et au vu du carré, il est forcément de degré pair. Comme $f$ est de degré $d$, on en déduit que $\deg(g) \leq d-2$ et est forcément impair, donc $g$ admet une racine $x \in \mathbf{F}$. En évaluant l'expression (2.1) en $x$, on obtient

$$-1 = \sum_{i=1}^{n} h_i^2(x) \in \mathbf{F},$$

ce qui est contradictoire avec le fait que $\mathbf{F}$ est un champ réel.

2)$\Rightarrow$ 3) Soit $P \in \mathbf{F}[X]$ tel que $\deg(P) = 2^m n$ avec $n$ impair. Montrons par récurrence sur $m$ qu'il existe une racine de $P$ dans $\mathbf{F}[i]$. Si $m = 0$, c'est direct par hypothèse car $\deg(P)$ est impair. Supposons que le résultat est vérifié pour $m-1$ et démontrons le pour $m$. Soit $x_1, \ldots, x_d$ les racines de $P$ dans $\mathbf{C}$ une clôture algébrique de $\mathbf{F}$. On défini les polynômes

$$Q_z = \prod_{1 \leq j < k \leq d} (X - x_j - x_k - z x_j x_k) \text{ avec } z \in \mathbb{Z}\,.$$

Les polynômes $Q_z$ sont symétriques en $x_1, \ldots, x_d$ et donc par la proposition 1.3.14, on en déduit que $Q_z \in \mathbf{F}[X]$ pour tout $z \in \mathbb{Z}$. De plus, on a

$$\deg(Q_z) = \frac{d(d-1)}{2} = \frac{2^m n(2^m n - 1)}{2} = 2^{m-1}(n(2^m n - 1)) = 2^{m-1} n',$$

avec $n'$ impair. Par hypothèse de récurrence, il existe $y_z \in \mathbf{F}[i]$ tel que $Q_z(y_z) = 0$. Donc il existe $j, k \in \{1, \ldots, d\}$, $(j \neq k)$ tels que

$$y_z = x_j + x_k + z x_j x_k \in \mathbf{F}[i].$$

Puisque le nombre de racines est fini, mais qu'à tout $z \in \mathbb{Z}$ correspond un couple $(j,k)$, il existe nécessairement un même couple $(j,k)$ associé à une infinité de racines $y_z \in \mathbb{F}[i]$. Dès lors, par combinaisons linéaires, il s'ensuit que $x_j + x_k \in \mathbb{F}[i]$ et $x_j x_k \in \mathbb{F}[i]$. De plus, $x_j$ et $x_k$ s'écrivent sous la forme

$$\frac{(x_j + x_k) \pm \sqrt{(x_j + x_k)^2 - 4x_j x_k}}{2} \in \mathbf{F}[i].$$

On en déduit que $P$ admet une racine dans $\mathbf{F}[i]$. Montrons désormais que $\mathbf{F}[i]$ est algébriquement clos. Soit $P \in (\mathbf{F}[i])[X]$ et notons $\overline{P}$ son conjugué (le polynôme obtenu en conjuguant tous les coefficients de $P$). Dès lors, $P\overline{P} \in \mathbf{F}[X]$ (car $\overline{P\overline{P}} = P\overline{P}$). Par la première partie de la démonstration, on sait qu'il existe $y \in \mathbf{F}[i]$ tel que

$$P(y)\overline{P}(y) = 0.$$

On en déduit que $P(y) = 0$ ou que $\overline{P}(y) = 0$, auquel cas on a $P(\overline{y}) = 0$ (car $\overline{P}(y) = 0$ donc $P(\overline{y}) = \overline{\overline{P}(y)} = \overline{0} = 0$). Donc on sait que $P$ admet une racine dans $\mathbf{F}[i]$. Par la remarque 1.2.17, $\mathbf{F}[i]$ est donc un champ algébriquement clos.
3)$\Rightarrow$ 1) Comme $\mathbf{F}[i] = \mathbf{F}[X]/\langle X^2+1\rangle$ est un champ, le polynôme $X^2+1$ est irréductible sur $\mathbf{F}$. En effet, dans le cas contraire, il serait le produit de deux polynômes de degré 1 dans $\mathbf{F}[X]$. Si on note $P$ et $Q$ ces polynômes, alors $[P]$ et $[Q]$ sont non nuls dans $\mathbf{F}[X]/\langle X^2+1\rangle$, mais leur produit est nul, une contradiction. Dès lors $-1 \notin \mathbf{F}^{(2)}$, sinon $X^2+1$ admettrait une racine dans $\mathbf{F}$ et serait donc réductible. De plus, soient $a, b, c, d \in \mathbf{F}$ tels que

$$(a+ib) = (c+id)^2,$$

alors

$$(a^2+b^2) = (a+ib)\overline{(a+ib)} = (c^2-d^2+2icd)\overline{(c^2-d^2+2icd)} = (c^2-d^2)^2+4c^2d^2 = (c^2+d^2)^2,$$

donc $\mathbf{F}^{(2)} = \Sigma_{\mathbf{F}}^{(2)}$ d'où $-1 \notin \Sigma_{\mathbf{F}}^{(2)}$ et donc, par le théorème 2.1.15, on en déduit que $\mathbf{F}$ est un champ réel. De plus, $\mathbf{F}[i]$ est l'unique extension algébrique non-triviale de celui-ci et n'est pas réelle. En effet, au vu du lemme 2.2.2, les seuls polynômes irréductibles de $\mathbf{F}[X]$ de degré $> 1$ sont de la forme

$$((X-c)^2+d^2) = (X-c-id)(X-c+id),\ d \neq 0,$$

et $\mathbf{F}[X]/\langle (X-c)^2+d^2\rangle = \mathbf{F}[i]$. □

**Exemple 2.2.4.** L'ensemble des nombres algébriques réels, défini par

$$\mathbb{R}_{alg} = \{x \in \mathbb{R} : \exists P \in \mathbb{Q}[X] : P \neq 0, P(x) = 0\},$$

est un champ (voir [5, Lemme 5.7]), c'est même un champ réel clos. En effet, vérifions le point 2) du théorème 2.2.3. On munit cet ensemble de l'ordre induit par l'ordre usuel de $\mathbb{R}$. Montrons que

$$\{x \geq 0 : x \in \mathbb{R}_{alg}\} = \{x^2 : x \in \mathbb{R}_{alg}\}.$$

Comme ce sont des nombres réels, il est clair que les carrés sont positifs. De plus, soit $x \in \mathbb{R}_{alg}$ un nombre positif. Alors, il existe $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$. Si on a

$$P = a_nX^n + \ldots + a_1X + a_0,$$

alors on considère le polynôme $Q \in \mathbb{Q}[X]$ défini par

$$Q = a_nX^{2n} + \ldots + a_1X^2 + a_0.$$

Comme $x \in \mathbb{R}$ est positif, il existe $y \in \mathbb{R}$ positif tel que $y^2 = x$ et comme $P(x) = 0$, on a $Q(y) = 0$ et on en déduit que $y \in \mathbb{R}_{alg}$. Il reste à montrer que si $P \in \mathbb{R}_{alg}[X]$ est de degré impair, alors $P$ admet une racine dans $\mathbb{R}_{alg}$. Comme $\mathbb{R}_{alg} \subset \mathbb{R}$, on sait qu'il existe une racine $x \in \mathbb{R}$ de $P$. Il reste alors à montrer que $x \in \mathbb{R}_{alg}$. Comme $P \in \mathbb{R}_{alg}[X]$, on a $a_0, \ldots, a_n \in \mathbb{R}_{alg}$. Dès lors, le degré d'extension de $\mathbb{Q}' = \mathbb{Q}(a_0, \ldots, a_n)$ sur $\mathbb{Q}$ est fini (voir [5, Lemme 5.6]). De plus, le degré d'extension de $\mathbb{Q}'(x)$ sur $\mathbb{Q}'$ est également fini (car les puissances de $x$ peuvent être exprimées par $\{x, x^2, \ldots, x^{n-1}\}$). Dès lors,

$$[\mathbb{Q}'(x) : \mathbb{Q}] = [\mathbb{Q}'(x) : \mathbb{Q}'][\mathbb{Q}' : \mathbb{Q}],$$

est donc fini. Comme $\mathbb{Q}(x)$ est un sous-espace de $\mathbb{Q}'(x)$, on en déduit que $[\mathbb{Q}(x) : \mathbb{Q}]$ est fini et donc que $x$ est un nombre algébrique et donc $x \in \mathbb{R}_{alg}$.

### 2.2.2 Clôture réelle d'un champ ordonné

Dans cette section, on va montrer que tout champ réel est inclus dans un champ réel clos. Pour ce faire, on définit la clôture réelle et on montre son existence dans le théorème qui suit.

**Définition 2.2.5.** Une extension algébrique $\mathbf{R}$ d'un champ ordonné $(\mathbf{F}, \leq)$ est appelée une clôture réelle de $\mathbf{F}$ si $\mathbf{R}$ est un champ réel clos et que son unique ordre étend l'ordre de $\mathbf{F}$.

**Théorème 2.2.6.** *Tout champ ordonné $(\mathbf{F}, \leq)$ admet une clôture réelle.*

*Démonstration.* Par le théorème 1.2.16, $\mathbf{F}$ admet un extension algébriquement close $\mathbf{C}$. Par le théorème 1.2.19, $\mathbf{F}$ admet une clôture algébrique $\overline{\mathbf{F}}$ dans $\mathbf{C}$. Considérons $E$ l'ensemble des sous-extensions ordonnées $(\mathbf{K}, \leq)$ avec $\mathbf{F} \subset \mathbf{K} \subset \overline{\mathbf{F}}$ où l'ordre sur $\mathbf{K}$ étend l'ordre sur $\mathbf{F}$. L'ensemble $E$ est ordonné par la relation $(\mathbf{K}, \leq) \prec (\mathbf{K}', \leq)$ si $\mathbf{K} \subset \mathbf{K}'$ et si l'ordre sur $\mathbf{K}'$ étend l'ordre sur $\mathbf{K}$. Par le lemme de Zorn, $E$ admet un élément maximal $(\mathbf{R}, \leq)$. Montrons que $\mathbf{R}$ est un champ réel clos. Pour ce faire, nous allons montrer que pour tout champ réel $\mathbf{K}$ muni d'un ordre qui contient $\mathbf{R}$, l'ordre sur $\mathbf{K}$ va étendre l'ordre de $\mathbf{R}$. Commençons par montrer que tout élément positif de $\mathbf{R}$ est un carré de $\mathbf{R}$. Soit $a \in \mathbf{R}$ un élément positif tel que $\sqrt{a} \notin \mathbf{R}$. Considérons l'ensemble $P$ des éléments de $\mathbf{R}[\sqrt{a}] \subset \overline{\mathbf{F}}$ contenant les éléments de la forme

$$\sum_{i=1}^{n} b_i(c_i + d_i\sqrt{a})^2,$$

avec $b_i, c_i, d_i \in \mathbf{R}$ et $b_i \geq 0$. On en tire que $P$ est un cône propre car si

$$-1 = \sum_{i=1}^{n} b_i(c_i + d_i\sqrt{a})^2 = \sum_{i=1}^{n} b_i(c_i^2 + d_i^2 a + 2c_i d_i\sqrt{a}).$$

alors étant donné que $-1 \in \mathbf{R}$, on a que

$$-1 = \sum_{i=1}^{n} b_i(c_i^2 + d_i^2 a).$$

On en déduit que $-1$ est dans le cône positif de $(\mathbf{R}, \leq)$. Par le lemme 2.1.13, $P$ est contenu dans le cône positif d'un ordre sur $\mathbf{R}[\sqrt{a}]$ qui étend l'ordre de $\mathbf{R}$. Cela contredit le caractère maximal de $(\mathbf{R}, \leq)$. Dès lors, par la proposition 2.1.10, le champ $\mathbf{R}$ admet un unique ordre, dont les positifs sont les carrés. Ce qui implique que si $\mathbf{K}$ est un champ réel tel que $\mathbf{R} \subset \mathbf{K} \subset \overline{\mathbf{F}}$ alors tout ordre de $\mathbf{K}$ étend l'ordre de $\mathbf{R}$ étant donné que la restriction à $\mathbf{R}$ d'un ordre sur $\mathbf{K}$ est un ordre sur $\mathbf{R}$. Dès lors, $\mathbf{K} = \mathbf{R}$ par maximalité de $\mathbf{R}$. On en déduit que $\mathbf{R}$ est un champ réel clos. □

Notons que cette clôture est unique à isomorphisme près (cela n'est pas démontré ici, mais la démonstration peut être trouvée dans [2, p.15].

On peut alors, à partir d'un champ réel $\mathbf{F}$, supposer avoir un champ réel clos $\mathbf{R}$ et un champ algébriquement clos $\mathbf{C}$ tel que $\mathbf{F} \subset \mathbf{R} \subset \mathbf{C}$.

### 2.2.3 Résultats d'analyse

Dans cette sous-section, on va montrer qu'on peut obtenir les analogues des résultats classiques d'analyse réelle pour les polynômes à coefficients dans un champ réel clos. Notamment le théorème des valeurs intermédiaires, le lemme de Rolle et le théorème des accroissements finis. Ces résultats ont bien sûr leur intérêt propre mais sont nécessaires afin de développer le Principe de Tarski-Seidenberg, l'objet du chapitre suivant.

**Définition 2.2.7.** Soient $\mathbf{R}$ un champ réel clos et $a, b \in \mathbf{R}$. On définit les intervalles ouverts

$$]a, b[ = \{x \in \mathbf{R} : a < x < b\},$$

et on procède de même pour définir $[a, b]$, $[a, b[$ et $]a, b]$.

Les intervalles ouverts permettent de définir la topologie d'un champ réel clos. En effet ; le champ réel que l'on considère est une union d'intervalles et l'intersection de deux intervalles est vide ou un intervalle. Ils forment donc une base de topologie.

**Définition 2.2.8.** Soit $\mathbf{R}$ un champ réel clos. La topologie (euclidienne) de $\mathbf{R}$ est la topologie qui a pour base les intervalles ouverts. La topologie sur $\mathbf{R}^n$ est alors la topologie produit.

Passons maintenant au théorème des valeurs intermédiaires, dans les champs réels clos, valable pour les polynômes à coefficients dans de tels champs.

**Proposition 2.2.9.** *(Théorème des valeurs intermédiaires) Soient $\mathbf{R}$ un champ réel clos, $f \in \mathbf{R}[X]$ et $a, b \in \mathbf{R}$ tel que $a < b$. Si $f(a)f(b) < 0$ alors il existe $x \in ]a, b[$ tel que $f(x) = 0$.*

*Démonstration.* Au vu du lemme 2.2.2, on sait que les facteurs irréductibles de $\mathbf{R}[X]$ sont linéaires ou sont de la forme $(X-c)^2+d^2$ avec $d \neq 0$. Un tel facteur prend donc des valeurs strictement positives sur $\mathbf{R}$. Donc si $f(a)f(b) < 0$ il existe un facteur linéaire $g = mX + p$

de $f$ tel que $g(a)g(b) < 0$. On en déduit que $m \neq 0$ et donc que $g(\frac{-p}{m}) = 0$. Dès lors, $f(\frac{-p}{m}) = 0$. Notons $c = \frac{-p}{m}$ et montrons que $c \in ]a, b[$. On a

$$g(a)g(b) = (ma + p)(mb + p) < 0,$$

donc en divisant par $m^2$, on a

$$(a - c)(b - c) < 0.$$

On en déduit que $c \in ]a, b[$. □

Pour écrire le lemme de Rolle et le théorème des accroissements finis pour les polynômes à coefficients dans un champ réel clos, il est nécessaire de définir les dérivées de telles fonctions. La définition généralise la dérivée des fonctions polynomiales de $\mathbf{R}$ dans $\mathbf{R}$.

**Définition 2.2.10.** Soit $f \in \mathbf{R}[X]$ un polynôme à coefficients dans $\mathbf{R}$ un champ réel clos. Alors la dérivée de $f = a_n X^n + \ldots + a_1 X + a_0$ est le polynôme

$$f' = n a_n X^{n-1} + \ldots + 2a_2 X + a_1 \in \mathbf{R}[X].$$

On retombe sur la définition usuelle. On peut donc continuer à utiliser les règles de dérivation usuelles.

L'analogue du lemme de Rolle peut alors être énoncé :

**Proposition 2.2.11.** *(Lemme de Rolle) Soient* $\mathbf{R}$ *un champ réel clos,* $f \in \mathbf{R}[X]$ *et* $a, b \in \mathbf{R}$ *tels que* $a < b$ *et* $f(a) = f(b)$*. Alors il existe* $c \in ]a, b[$ *tel que* $f'(c) = 0$*.*

*Démonstration.* Quitte à translater le polynôme, on peut supposer que $f(a) = f(b) = 0$. De plus, supposons que $a$ et $b$ sont deux racines consécutives de $f$ (si $f$ admet une racine $x \in ]a, b[$ alors on montre qu'il existe un tel $c$ dans $]a, x[ \subset ]a, b[$). On a alors

$$f = (X - a)^m (X - b)^n g,$$

où $g \in \mathbf{R}[X]$ est tel que $g(x) \neq 0$ pour tout $x \in [a, b]$. Par la contraposée de la proposition 2.2.9, $g$ est de signe constant sur $[a, b]$. De plus, on a

$$f' = (X - a)^{m-1} (X - b)^{n-1} g_1,$$

où

$$g_1 = m(X - b)g + n(X - a)g + (X - a)(X - b)g'.$$

Dès lors,

$$g_1(a)g_1(b) = m(a - b)g(a)n(b - a)g(b) < 0.$$

Donc par la proposition 2.2.9, le polynôme $g_1$ admet une racine $c \in ]a, b[$, et cette racine est également une racine de $f'$. □

Le théorème des accroissements finis se généralise également :

**Proposition 2.2.12.** *(Théorème des accroissements finis) Soient* $\mathbf{R}$ *un champ réel clos,* $f \in \mathbf{R}[X]$ *et* $a, b \in \mathbf{R}$ *tels que* $a < b$*. Il existe* $c \in ]a, b[$ *tel que* $f(b) - f(a) = (b - a)f'(x)$*.*

*Démonstration.* Posons

$$g(X) = f(X) - f(a) - (X - a)\frac{f(b) - f(a)}{b - a},$$

on a donc $g(a) = 0$ et $g(b) = 0$. Alors, par la proposition 2.2.11, il existe $c \in ]a, b[$ tel que $g'(c) = 0$. On en déduit alors que

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

□

Classiquement, ce théorème permet de lier le signe de la fonction dérivée à la croissance de la fonction étudiée. Il en est de même ici :

**Corollaire 2.2.13.** *Soit* $\mathbf{R}$ *un champ réel clos,* $f \in \mathbf{R}[X]$ *et* $a, b \in \mathbf{R}$ *tels que* $a < b$*. Si* $f'$ *est strictement positif sur* $]a, b[$ *(resp. négatif) alors* $f$ *est strictement croissant (resp. strictement décroissant) sur* $[a, b]$*.*

*Démonstration.* Traitons le cas strictement positif, le cas strictement négatif se traite de la même manière. Soient $x, y \in [a, b]$ tels que $x < y$. Par la proposition 2.2.12, il existe $z \in ]x, y[$ tel que

$$f(y) - f(x) = (y - x)f'(z).$$

Comme $z \in ]x, y[ \subseteq ]a, b[$ on a $f'(z) > 0$. Donc

$$f(y) > f(x).$$

□

### 2.2.4 Propriétés sur les racines

Dans cette section, nous considérons toujours un champ réel clos $\mathbf{R}$. Nous allons nous intéresser aux racines des polynômes de $\mathbf{R}[X]$ en donnant des résultats qui permettent de "localiser" les racines. Le résultat principal de cette section est le théorème de Sylvester (2.2.19) qui généralise le théorème de Sturm (2.2.21). Ce type de résultat permet en pratique de localiser les racines d'un polynôme et peut être utilisé algorithmiquement, notamment lorsqu'un ordinateur doit localiser les racines réelles d'un polynôme afin d'effectuer une décomposition cylindrique algébrique.

Nous notons $\#E$ le cardinal de l'ensemble $E$.

**Définition 2.2.14.** Soit une suite $(a_0, \ldots, a_k)$ d'éléments de $\mathbf{R}$ avec $a_0 \neq 0$. On définit le nombre de changements de signes de la suite comme

$$\mathrm{cs}(a_0, \ldots, a_k) = \#\{i \in \{0, \ldots, k\} \mid \exists l \in \{i{+}1, \ldots, k\} : (a_i a_l < 0) \wedge (\forall j \in \{i{+}1, \ldots, l{-}1\}, a_j = 0)\}.$$

**Exemple 2.2.15.** Pour calculer $\mathrm{cs}(1,-1,0,-1,1,0,0,1,1,0,0,-1,1)$, on considère la suite sans les 0, c'est-à-dire $(1,-1,-1,1,1,1,-1,1)$. On compte alors le nombre de changements de signes entre ses éléments consécutifs, qui est 4.

Nous aurons besoin dans la suite de quelques propriétés élémentaires de ces changements de signes. Nous les rassemblons dans le résultat technique suivant.

**Lemme 2.2.16.** *Pour $a_0,\dots,a_k \in \mathbf{R}$ tels que $a_0 \neq 0$, on a*

1. $\mathrm{cs}(a_0,\dots,a_k) = \mathrm{cs}(ra_0,\dots,ra_k)$, *pour tout $r \in \mathbf{R}_0$ ;*
2. $\mathrm{cs}(a_0,\dots,a_k) = \mathrm{cs}(a_0,\dots,a_i) + \mathrm{cs}(a_i,\dots,a_k)$ *pour tout $i \in \{1,\dots,k-1\}$ tel que $a_i \neq 0$ ;*
3. $\mathrm{cs}(a_0,a_1,a_2) = 1$ *quel que soit $a_1$, si $a_0a_2 < 0$.*

*Démonstration.* Pour le premier point, on note que $a_j = 0$ si et seulement si $ra_j = 0$, et $a_ia_l < 0$ si et seulement si $(ra_i)(ra_l) < 0$. L'égalité visée découle alors directement de la définition. Pour la seconde assertion, la suite obtenue en retirant les 0 de $(a_0,\dots,a_k)$ est en effet la concaténation des suites obtenues en retirant les 0 dans les suites $(a_0,\dots,a_i)$ et $(a_i,\dots,a_k)$. Enfin, si $a_0$ et $a_2$ sont de signes contraires, soit $a_1 = 0$, alors le nombre de changements de signes est 1 par définition, et si $a_1 \neq 0$, il a le même signe que $a_0$ ou $a_2$, les deux cas étant exclusifs. □

**Définition 2.2.17.** Soit $\mathbf{R}$ un champ réel clos et $f,g \in \mathbf{R}[X]$. La suite de Sturm de $f$ et de $g$ est la suite finie de polynômes $(f_0,\dots,f_k)$ définie par

$$\begin{aligned} f_0 &= f,\\ f_1 &= f'g,\\ f_{i-2} &= f_{i-1}q_i + (-f_i) \end{aligned}$$

où $q_i \in \mathbf{R}[X]$ et $\deg(f_i) < \deg(f_{i-1})$ pour $i \in \{2,\dots,k\}$. De plus, si $a \in \mathbf{R}$ et $f(a) \neq 0$, on définit

$$v(f,g;a) = \mathrm{cs}(f_0(a),\dots,f_k(a)).$$

On remarque que $f_i$ est l'opposé du reste de la division euclidienne de $f_{i-2}$ par $f_{i-1}$, on en déduit que $f_k$ est un pgcd de $f_0 = f$ et de $f_1 = f'g$, mais aussi un pgcd de $f_i$ et $f_{i+1}$ pour tout $i \in \{1,\dots,k-1\}$.

**Exemple 2.2.18.** Considérons les polynômes de $\mathbb{R}[X]$ suivants

$$f = X^3 + X^2 + X + 1 \text{ et } g = X^2.$$

On a alors

$$f' = 3X^2 + 2X + 1,$$

et on obtient, en effectuant des divisions euclidiennes (en tenant compte du changement de signe) que la suite de Sturm associée est

$$\begin{aligned} f_0 &= X^3 + X^2 + X + 1, \\ f_1 &= 3X^4 + 2X^3 + X^2, \\ f_2 &= -X^3 - X^2 - X - 1, \\ f_3 &= X^2 + 2X - 1, \\ f_4 &= 4X, \\ f_5 &= 1, \end{aligned}$$

avec $q_2 = 0$, $q_3 = -3X + 1$, $q_4 = -X + 1$ et $q_5 = \frac{1}{4}X + \frac{1}{2}$. Dans ce cas ci, 0 n'est pas une racine de $f$. On peut alors calculer $v(f, g, 0)$. La suite associée est

$$(1, 0, -1, -1, 0, 1).$$

Son nombre de changements de signe est $v(f, g; 0) = 2$.

**Théorème 2.2.19.** *(Théorème de Sylvester) Soient* $\mathbf{R}$ *un champ réel clos,* $f, g \in \mathbf{R}[X]$ *et* $a, b \in \mathbf{R}$ *tels que ce ne sont pas des racines de* $f$ *et* $a < b$*. Alors*

$$\#\{x \in ]a, b[ : f(x) = 0, g(x) > 0\} - \#\{x \in ]a, b[ : f(x) = 0, g(x) < 0\} = v(f, g; a) - v(f, g; b).$$

*Démonstration.* On considère la suite de Sturm $(f_0, \ldots, f_k)$ obtenue à partir de $f$ et $g$. Puisque $f_k$ divise tous les $f_i$, pour $i = 0, \ldots, k$, on peut définir la suite de polynômes $(g_0, \ldots, g_k)$ par

$$g_i f_k = f_i \text{ pour tout } i \in \{0, \ldots, k\}.$$

Il est utile de remarquer que

1. Le polynôme $g_k$ vaut 1 ;
2. Puisque $f_k$ est le pgcd de $f_i$ et $f_{i+1}$, les polynômes $g_i$ et $g_{i+1}$ sont premiers entre eux, pour tout $i \in \{0, \ldots, k-1\}$ ;
3. En tout point $x \in \mathbf{R}$ tel que $f(x) \neq 0$, on a $f_k(x) \neq 0$, et donc par le lemme 2.2.16,

$$v(f, g; x) = \mathrm{cs}(f_0(x), \ldots, f_k(x)) = \mathrm{cs}(g_0(x), \ldots, g_k(x)). \tag{2.2}$$

Dans ce qui suit, on va décomposer l'intervalle $[a, b]$ en sous-intervalles $[x, y]$ et évaluer $v(f, g; x) - v(f, g; y)$. Si on choisit ces points $x, y$ tels que $f(x)f(y) \neq 0$, et s'il n'y a pas de racine de $g_0, \ldots, g_k$ dans $[x, y]$, alors cette différence est nulle. En effet, on a

$$\begin{aligned} v(f, g; x) - v(f, g; y) &= \mathrm{cs}(f_0(x), \ldots, f_k(x)) - \mathrm{cs}(f_0(y), \ldots, f_k(y)) \\ &= \mathrm{cs}(g_0(x), \ldots, g_k(x)) - \mathrm{cs}(g_0(y), \ldots, g_k(y)) = 0, \end{aligned} \tag{2.3}$$

puisque les polynômes $g_0, \ldots, g_k$ ne changent pas de signe sur l'intervalle $[x, y]$ au vu de la proposition 2.2.9. Il faut bien sûr alors considérer les cas des intervalles $[x, y]$ dans lesquels

figure au moins un zéro de $g_0, \ldots, g_k$. Nous observerons que c'est uniquement quand $[x, y]$ contient des racines de $g_0$ que ce nombre va pouvoir varier.

Procédons au découpage : notons $r_1 < \cdots < r_p$ les racines des polynômes $g_0, \ldots, g_k$ dans $]a, b[$, et notons $r_0 = a$ et $r_{p+1} = b$. Pour tout $i \in \{1, \ldots, p\}$, il existe $\varepsilon_i > 0$ tel que $f'g$ soit de signe constant sur $]r_i - \varepsilon_i[$ et sur $]r_i + \varepsilon_i[$. Choisissons un point $x_i$ dans le premier intervalle et un point $y_i$ dans le second, de sorte qu'aucun des deux ne soit une racine de $f$, et de sorte que $y_i < x_{i+1}$. On a alors évidemment

$$\begin{aligned} v(f,g;a) - v(f,g;b) = (v(f,g;a) - v(f,g;x_1)) + (v(f,g;y_p) - v(f,g;b)) \\ + \sum_{i=1}^{p-1} (v(f,g;y_i) - v(f,g;x_{i+1})) + \sum_{i=1}^{p} (v(f,g;x_i) - v(f,g;y_i)). \quad (2.4) \end{aligned}$$

On va premièrement montrer que les deux premiers termes et la première somme dans le membre de droite sont nuls. Tous les termes que nous avons à calculer sont de la forme $v(f, g; x) - v(f, g; y)$ où les éléments $x < y$ de $[a, b]$ sont tels que $[x, y]$ ne contient aucune racine de $g_0$ (car toute racine de $g_0$ est une racine de $f_0 = f$ et par hypothèse $a$ et $b$ n'en sont pas) et au plus une seule racine (éventuellement simultanée) des polynômes $g_1, \ldots, g_k$.

1. Si $[x, y]$ ne contient aucune racine de $g_1, \ldots, g_k$, alors on a montré à l'équation (2.3), que $v(f, g; x) - v(f, g; y) = 0$,
2. Sinon, notons $c$ l'unique racine des polynômes $g_1, \ldots, g_k$ dans $[x, y]$. Notons également $i_1 < \cdots < i_s$ les indices $i$ tels que $g_i(c) = 0$. On remarque que $i_s < k$, puisque $g_k = 1$, que $i_1 > 0$ par hypothèse, et que les indices $i_1, \ldots, i_s$ ne contiennent aucun couple de nombres consécutifs, puisque $g_i$ et $g_{i+1}$ sont premiers entre eux. On a même pour tout $j \in \{1, \ldots, s\}$,

   $$g_{i_j-1}(c)\, g_{i_j+1}(c) < 0,$$

   car la définition 2.2.17 et la définition des $g_i$ impliquent la relation $g_{i-1} = g_i q_i + (-g_{i+1})$.

   Par le point 3. du lemme 2.2.16, on a donc $\mathrm{cs}(g_{i_j-1}(c), a, g_{i_j+1}(c)) = 1$ quel que soit $a \in \mathbf{R}$. Comme $g_{i_j-1}$ et $g_{i_j+1}$ ne s'annulent pas sur $[x, y]$, ils y gardent un signe constant et on a $\mathrm{cs}(g_{i_j-1}(z), a, g_{i_j+1}(z)) = 1$ quel que soit $a \in \mathbf{R}$, et $z \in [x, y]$. Ainsi, on obtient

   $$\mathrm{cs}(g_{i_j-1}(c), g_{i_j}(c), g_{i_j+1}(c)) = \mathrm{cs}(g_{i_j-1}(z), g_{i_j}(z), g_{i_j+1}(z)), \quad \forall z \in [x, y].$$

   Pour montrer que $v(f, g, z)$ est indépendant de $z \in [x, y]$, il suffit de noter que $v(f, g, z) = \mathrm{cs}(f_0(z), \ldots, f_k(z))$ vaut aussi $\mathrm{cs}(g_0(z), \ldots, g_k(z))$ puisque $z$ n'est pas racine de $f_k$. Par le point 2. du lemme 2.2.16, on peut décomposer cette expression en somme d'expressions du type $\mathrm{cs}(g_{j_1}(z), \ldots, g_{j_t}(z))$ où les polynômes concernés ne s'annulent pas sur $[x, y]$, et d'expressions du type $\mathrm{cs}(g_{i_j-1}(z), g_{i_j}(z), g_{i_j+1}(z))$ qui sont aussi constantes sur $[x, y]$.

Par la formule 2.4, on a donc

$$v(f,g;a) - v(f,g;b) = \sum_{i=1}^{p} (v(f,g;x_i) - v(f,g;y_i)),$$

et on sait que $[x_i, y_i]$ contient une seule racine $r_i \in ]x_i, y_i[$ des polynômes $g_0, \ldots, g_k$.

1. Si $r_i$ n'est pas racine de $g_0$, l'argument ci-dessus montre que $v(f,g;x_i) - v(f,g;y_i) = 0$ ;
2. Si $r_i$ est racine de $g_0$, il n'est pas racine de $g_1$, donc $g_1$ ne s'annule pas sur $[x_i, y_i]$ et en écrivant

   $$\mathrm{cs}(g_0(z), \ldots, g_k(z)) = \mathrm{cs}(g_0(z), g_1(z)) + \mathrm{cs}(g_1(z), \ldots, g_k(z)),$$

   pour tout $z \in [x_i, y_i] \setminus \{r_i\}$, on montre comme plus haut que $\mathrm{cs}(g_1(z), \ldots, g_k(z))$ est indépendant de $z \in [x_i, y_i]$.
   Il reste donc à comparer

   $$\mathrm{cs}(g_0(x_i), g_1(x_i)) = \mathrm{cs}(f_0(x_i), f_1(x_i)) \quad \text{et} \quad \mathrm{cs}(g_0(y_i), g_1(y_i)) = \mathrm{cs}(f_0(y_i), f_1(y_i)).$$

   On le fait en établissant les tableaux de signes possibles pour $f_0 = f$ et $f_1 = f'g$ sur l'intervalle $[x_i, y_i]$. Pour ce faire, on fait les remarques suivantes :
   (a) Puisque $g_0(r_i) = 0$, on a $f(r_i) = 0$, et donc par le corollaire 2.2.13, le signe de $f$ sur $[x_i, r_i[$ et sur $]r_i, y_i[$ est déterminé par le signe de $f'$, qui gouverne la croissance de $f$.
   (b) On a $g(r_i) \neq 0$. Sinon, en notant $m$ la multiplicité de $r_i$ comme racine de $f_0 = f$, on constate que la multiplicité de $r_i$ comme racine de $f_1 = f'g$ est aussi au moins $m$, donc sa multiplicité comme racine de leur pgcd (au signe près) $f_k$ est aussi $m$, et $r_i$ n'est pas alors racine de $g_0$, une contradiction.
   (c) Alors $g$ est de signe constant au voisinage de $r_i$, et comme par construction il est de signe constant sur $[x_i, r_i[$ et $]r_i, y_i]$, il a le signe de $g(r_i)$ sur $[x_i, y_i]$.

   On établit donc tous les tableaux de signes possibles en fonction des huit triplets $(\mathrm{sign}(g), \mathrm{sign}(f'|_{[x_i,r_i[}), \mathrm{sign}(f'|_{]r_i,y_i]}))$ possibles. Les colonnes correspondant à $x_i$ et $y_i$ établissent le signe sur les intervalles contenant $[x_i, r_i[$ et $]r_i, y_i]$ respectivement.

1) $(+,+,+)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $-$ | $0$ | $+$ |
| $f'g$ | $+$ | | $+$ |

2) $(-,+,+)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $-$ | $0$ | $+$ |
| $f'g$ | $-$ | | $-$ |

3) $(+,-,+)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $+$ | $0$ | $+$ |
| $f'g$ | $-$ | | $+$ |

4) $(-,-,+)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $+$ | $0$ | $+$ |
| $f'g$ | $+$ | | $-$ |

5) $(+,+,-)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $-$ | $0$ | $-$ |
| $f'g$ | $+$ | | $-$ |

6) $(-,+,-)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $-$ | $0$ | $-$ |
| $f'g$ | $-$ | | $+$ |

7) $(+,-,-)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $+$ | $0$ | $-$ |
| $f'g$ | $-$ | | $-$ |

8) $(-,-,-)$

| | $x_i$ | $r_i$ | $y_i$ |
|---|---|---|---|
| $f$ | $+$ | $0$ | $-$ |
| $f'g$ | $+$ | | $+$ |

On observe alors que si $g(r_i) > 0$, on a $\mathrm{cs}(f_0(x_i), f_1(x_i)) - \mathrm{cs}(f_0(y_i), f_1(y_i)) = 1$ (voir tableaux $1, 3, 5, 7$) et que si $g(r_i) < 0$, on a $\mathrm{cs}(f_0(x_i), f_1(x_i)) - \mathrm{cs}(f_0(y_i), f_1(y_i)) = -1$ (voir tableaux $2, 4, 6, 8$). On a donc en final

$$v(f, g; a) - v(f, g; b) = \sum_{i=1}^{p} (v(f, g; x_i) - v(f, g; y_i)) = \left( \sum_{\substack{i: g_0(r_i)=0 \\ g(r_i)>0}} 1 \right) - \left( \sum_{\substack{i: g_0(r_i)=0 \\ g(r_i)<0}} 1 \right),$$

et le résultat suit en notant que les conditions $(g_0(x), g(x) > 0)$ et $(f(x), g(x) > 0)$ d'une part et $(g_0(x), g(x) < 0)$ et $(f(x), g(x) < 0)$ d'autre part, sont équivalentes.

□

**Exemple 2.2.20.** Reprenons l'exemple 2.2.18. On a $f(-10) = -909 \neq 0$. On peut alors calculer $v(f, g; -10)$, on trouve que la suite associée est

$$(-909, 28100, 909, 79, -40, 1).$$

Son nombre de changements de signe est $v(f, g; -10) = 3$. Au vu du théorème de Sylvester 2.2.19, on en déduit que dans $]-10, 0[$, il y a une racine de $f$ pour laquelle $g$ est positif de plus que de racine de $f$ pour laquelle $g$ est négatif. En effet, on a

$$f = X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$$

Il n'y donc qu'une seule racine réelle qui est $-1 \in ]-10, 0[$ pour laquelle on a $g(-1) = 1 > 0$.

Le résultat utile en pratique est le suivant, c'est le théorème de Sturm, un cas particulier du théorème de Sylvester. Il permet de compter les racines d'un polynôme sur un intervalle donné.

**Corollaire 2.2.21.** *(Théorème de Sturm) Soient* $\mathbf{R}$ *un champ réel clos,* $f \in \mathbf{R}[X]$ *et* $a, b \in \mathbf{R}$ *tels que ce ne sont pas des racines de* $f$ *et* $a < b$*. Alors*

$$\#\{x \in ]a, b[ : f(x) = 0\} = v(f, 1; a) - v(f; 1, b).$$

*Démonstration.* On applique le théorème de Sylvester en considérant le polynôme constant $g = 1$. En effet, on a

$$\{x \in ]a, b[ : f(x) = 0\} = \{x \in ]a, b[ : f(x) = 0 \wedge 1 = g(x) > 0\},$$

et

$$\{x \in ]a, b[ : f(x) = 0 \wedge 1 = g(x) < 0\} = \emptyset.$$

□

**Lemme 2.2.22.** *Soit* $\mathbf{R}$ *un champ réel clos et soit*

$$f = a_n X^n + \ldots + a_0 \in \mathbf{R}[X] \text{ avec } a_n \neq 0.$$

*Notons*

$$M = 1 + \sum_{i=1}^{n} \left| \frac{a_{n-i}}{a_n} \right|.$$

*Alors* $f(x) \neq 0$ *pour tout* $x \notin ]-M, M[$. *De plus, le signe de* $f$ *sur* $[M, +\infty[$ *(resp.* $]-\infty, -M]$*) est celui de* $a_n$ *(resp.* $(-1)^n a_n$*).*

*Démonstration.* Soit $x \in \mathbf{R}$ tel que $|x| \geq M$ et posons $b_i = \frac{a_i}{a_n}$, pour $i \in \{0, \ldots, n-1\}$. Dès lors, on a

$$f(x) = a_n x^n (1 + b_{n-1} x^{-1} + \ldots + b_0 x^{-n}).$$

On constate que le second facteur est toujours positif. En effet, on a, vu la définition de $M$ :

$$|b_{n-1} x^{-1} + \ldots + b_0 x^{-n}| \leq (|b_{n-1}| + \ldots + |b_0|) M^{-1} < 1.$$

On en tire que $f(x)$ ne s'annule pas si $|x| \geqslant M$, et qu'il a le même signe que $a_n x^n$, donc le signe de $(-1)^n a_n$ ou $a_n$ selon que $x$ est négatif ou positif. □

**Corollaire 2.2.23.** *Soient* $\mathbf{R}$ *un champ réel clos,* $f, g \in \mathbf{R}[X]$ *et* $(f_0 \ldots, f_k)$ *la suite de Sturm de* $f$ *et de* $g$. *Notons* $v(f, g; +\infty)$ *(resp.* $v(f, g; -\infty)$*) le nombre de changements de signe de la suite de coefficients de terme du plus haut degré de* $(f_0, \ldots, f_k)$ *(resp.* $f_0(-X), \ldots, f_k(-X)$*). Alors*

$$\#\{x \in \mathbf{R} : f(x) = 0 \wedge g(x) > 0\} - \#\{x \in \mathbf{R} : f(x) = 0 \wedge g(x) < 0\} = v(f, g; -\infty) - v(f, g; +\infty).$$

*Démonstration.* Par lemme 2.2.22 il existe un $M$ suffisamment grand pour que toutes les racines réelles de $f_0, \ldots, f_k$ soient dans $]-M, M[$. Dans ce cas, $v(f, g; +\infty) = v(f, g; M)$ et $v(f, g; -\infty) = v(f, g; -M)$. Le théorème de Sylvester 2.2.19 permet de conclure. □

# Chapitre 3

# Principe de Tarski-Seidenberg

Maintenant qu'on a passé en revue les bases de la théorie sur les champs réels clos, on va l'utiliser pour développer le Principe de Tarski-Seidenberg. Il s'agit d'effectuer une élimination des quantificateurs sur des formules définies à l'aide de quantificateurs et polynômes, à coefficients dans un champ réel clos. Dans la première section de ce chapitre, nous définissons plus formellement ce langage. Cette section est inspirée de [1, chap. 2.3] tandis que le reste du chapitre est basé sur [2, chap. 1.4].

## 3.1 Langage des champs ordonnés

On considère un champ réel clos $\mathbf{R}$. Définissons le langage des champs ordonnés à coefficients dans $\mathbf{R}$.

**Définition 3.1.1.** Un atome du langage est $P = 0$ ou $P > 0$ avec $P \in \mathbf{R}[X_1, \ldots, X_n]$.
On définit alors simultanément les formules du langage ainsi que $\mathrm{Free}(\Phi)$ l'ensemble des variables libres d'une formule $\Phi$ comme suit :

- Un atome $P = 0$ ou $P > 0$ où $P \in \mathbf{R}[X_1, \ldots, X_n]$ est une formule ayant $\{X_1, \ldots, X_n\}$ comme variables libres.
- Si $\Phi_1$ et $\Phi_2$ sont des formules alors $\Phi_1 \wedge \Phi_2$ et $\Phi_1 \vee \Phi_2$ sont des formules et on a

$$\mathrm{Free}(\Phi_1 \wedge \Phi_2) = \mathrm{Free}(\Phi_1 \vee \Phi_2) = \mathrm{Free}(\Phi_1) \cup \mathrm{Free}(\Phi_2)$$

- Si $\Phi$ est une formule alors $\neg\Phi$ aussi et $\mathrm{Free}(\Phi) = \mathrm{Free}(\neg\Phi)$
- Si $\Phi$ est une formule et $X \in \mathrm{Free}(\Phi)$ alors $(\exists X)\Phi$ et $(\forall X)\Phi$ sont également des formules et on a

$$\mathrm{Free}((\exists X)\Phi) = \mathrm{Free}((\forall X)\Phi) = \mathrm{Free}(\Phi)\backslash\{X\}$$

De plus, on définit la formule $\varphi \Rightarrow \psi$ comme étant la formule $\neg(\psi) \vee \varphi$.
Une formule sans quantificateur est une formule dans laquelle aucun quantificateur $(\forall, \exists)$ n'apparaît.

**Définition 3.1.2.** On appelle combinaison booléenne d'équations et d'inéquations polynomiales une formule sans quantificateur dans le langage des champs ordonnés.

**Remarque 3.1.3.** Chaque formule sans quantificateur peut être mise sous forme normale disjonctive. De plus, on peut éliminer la négation afin que chaque formule sans quantificateur $\Psi(X)$ s'écrive sous la forme

$$\Psi(X) = \bigvee_{j=1}^{J} \bigwedge_{i=1}^{s_j} P_{i,j}(X) *_{i,j} 0,$$

où $P_{i,j} \in \mathbf{R}[X]$ avec $X = (X_1, \ldots, X_n)$ et $*_{i,j} \in \{<, =, >\}$ pour tout $j \in \{1, \ldots, J\}$ et $i \in \{1, \ldots, s_j\}$.

**Définition 3.1.4.** La réalisation d'une formule $\Phi$ avec des variables libres contenues dans $\{X_1, \ldots, X_n\}$ est

$$\text{Reali}(\Phi) = \{x \in \mathbf{R}^n : \Phi(x) \text{ est vrai } \}$$

On le définit par induction sur la construction des formules :

- $\text{Reali}(P = 0) = \{x \in \mathbf{R}^n : P(x) = 0\}$
- $\text{Reali}(P \neq 0) = \{x \in \mathbf{R}^n : P(x) \neq 0\}$
- $\text{Reali}(\Phi_1 \wedge \Phi_2) = \text{Reali}(\Phi_1) \cap \text{Reali}(\Phi_2)$
- $\text{Reali}(\Phi_1 \vee \Phi_2) = \text{Reali}(\Phi_1) \cup \text{Reali}(\Phi_2)$
- $\text{Reali}(\neg\Phi) = \mathbf{R}^n \setminus \text{Reali}(\Phi)$
- $\text{Reali}((\exists Y)\Phi) = \{x \in \mathbf{R}^{n-1} : \exists y \in \mathbf{R}, (x, y) \in \text{Reali}(\Phi)\}$
- $\text{Reali}((\forall Y)\Phi) = \{x \in \mathbf{R}^n : \forall y \in \mathbf{R}, (x, y) \in \text{Reali}(\Phi)\}$

Deux formules $\Phi$ et $\Psi$ telles que $\text{Free}(\Phi) = \text{Free}(\Psi) = \{X_1, \ldots, X_n\}$ sont équivalentes si $\text{Reali}(\Psi) = \text{Reali}(\Phi)$.

**Exemple 3.1.5.** Considérons les formules $\Phi \coloneqq XY = 0$ et $\Theta \coloneqq (\exists X)\Phi$. On a alors

$$\begin{aligned}\text{Reali}(\Phi) =& \{(x, y) \in \mathbf{R}^2 : xy = 0\} = \{(x, 0) : x \in \mathbf{R}\} \cup \{(0, y) : y \in \mathbf{R}\},\\ \text{Reali}(\Theta) =& \{y \in \mathbf{R} : \exists x \in \mathbf{R} : (x, y) \in \text{Reali}(\Phi)\} = \{y \in \mathbf{R} : \exists x \in \mathbf{R} : xy = 0\} = \mathbf{R}\,.\end{aligned}$$

**Exemple 3.1.6.** Dans les champs réels clos, la formule

$$\exists X \in \mathbf{R} : aX^2 + bX + c = 0$$

est équivalente à la formule

$$(a = 0 \wedge b = 0 \wedge c = 0) \vee (a = 0, b \neq 0) \vee (a \neq 0, \neg(b^2 - 4ac < 0)).$$

Nous avons donc éliminé le quantificateur $\exists$. En effet, la formule équivalente est une formule sans quantificateur.

## 3.2 Le résultat principal

Dans cette section, on énonce et démontre le résultat principal du chapitre ; le Principe de Tarski-Seidenberg qui permet d'effectuer une élimination des quantificateurs dans le langage des champs ordonnés. Ce principe est énoncé par Tarski en 1931, et il en donne une preuve existentielle en 1951. Quant à Seidenberg, il fournira une approche plus concrète en 1954. La première sous-section présente les notations et l'énoncé

### 3.2.1 Énoncé

Rappelons la définition de la fonction signe dans le cadre des champs réels (clos).

**Définition 3.2.1.** Soit $\mathbf{R}$ un champ réel clos. On définit

$$\mathrm{sign}_{\mathbf{R}} : \mathbf{R} \to \{-1, 0, 1\} : a \mapsto \mathrm{sign}_{\mathbf{R}}(a) = \begin{cases} 1 & \text{si } a > 0 \\ 0 & \text{si } a = 0 \\ -1 & \text{si } a < 0 \end{cases}$$

Lorsque le contexte est clair, on la notera sign.

Le Principe de Tarski-Seidenberg énoncé ci-dessous traite de polynômes à $n+1$ variables. Il étudie des systèmes d'égalités et d'inégalités pour un nombre fini de telles fonctions. Pour simplifier les notations, on note $Y = (Y_1, \ldots, Y_n)$. On considère $s$ fonctions $f_1, \ldots, f_s \in \mathbb{Z}[Y][X]$ que l'on le décompose si nécessaire en

$$f_i(X, Y) = h_{i,m_i}(Y)X^{m_i} + \ldots + h_{i,0}(Y). \tag{3.1}$$

Enfin, le système est déterminé par une fonction $\varphi$ qui à chaque indice $i \leq s$ associe le signe que $f_i$ doit prendre.

**Théorème 3.2.2.** *(Tarski-Seidenberg) Pour tout $f_1, \ldots, f_s \in \mathbb{Z}[Y][X]$ et toute fonction $\varphi : \{1, \ldots, s\} \to \{-1, 0, 1\}$, il existe une combinaison booléenne $\mathcal{B}(Y)$ d'équations et d'inéquations polynomiales avec des polynômes de $\mathbb{Z}[Y]$ telle que pour tout champ réel clos $\mathbf{R}$ et pour tout $y \in \mathbf{R}^n$, le système*

$$\begin{cases} \mathrm{sign}(f_1(X, y)) & = \varphi(1) \\ & \vdots \\ \mathrm{sign}(f_s(X, y)) & = \varphi(s) \end{cases}$$

*admet une solution $x \in \mathbf{R}$ si et seulement si $\mathcal{B}(y)$ est vrai dans $\mathbf{R}$.*

En terme des notations de la section 3.1, ce résultat nous dit que pour toute formule de la forme

$$\Phi(X, Y) = \bigwedge_{i=1}^{s} P_i(X, Y) *_i 0$$

où $*_i \in \{<, >, =\}$ et $P_i \in \mathbb{Z}[X, Y]$ pour tout $i \in \{1, \ldots, s\}$, il existe une formule sans quantificateur $\mathcal{B}(Y)$ à coefficients dans $\mathbb{Z}$ telle que si on note $\Theta(Y) = (\exists X)\Phi(X, Y)$ alors on a Reali($\Theta$) = Reali($\mathcal{B}$). De plus, au vu de la remarque 3.1.3, on peut exprimer toute formule sans quantificateur $\Psi(X, Y)$ comme une disjonction de formules ayant la même forme que $\Phi(X, Y)$. Supposons avoir une telle forme normale disjonctive,

$$\Psi(X, Y) = \bigvee_{j=1}^{J} \Phi_j(X, Y) = \bigvee_{j=1}^{J} \bigwedge_{i=1}^{s_j} P_{i,j}(X, Y) *_{i,j} 0.$$

Alors si on considère la formule

$$\Theta(Y) = (\exists X)\Psi(X, Y) = \bigvee_{j=1}^{n} (\exists X)\Phi_j(X, Y).$$

On peut alors éliminer le quantificateur de $\Theta$, il suffit de considérer la formule sans quantificateur qui est la disjonction des formules sans quantificateur obtenues en éliminant le quantificateur des formules $(\exists X)\Phi_j(X, Y)$.

Nous montrerons dans la section 3.3 que ce résultat s'étend pour toute formule dans le langage des champs ordonnés.

La démonstration du théorème 3.2.2 nécessite quelques résultats préliminaires. C'est l'objet de la section suivante.

### 3.2.2 Preuve

Dans la suite, on aura besoin de formaliser les tableaux de signes associés aux fonctions polynomiales. Les notations sont précisées dans la définition suivante. Remarquons que dans l'énoncé 3.2.2, on évalue en un élément $y$, et on est donc amené à considérer des polynômes à une variable.

**Définition 3.2.3.** Soient $f_1, \ldots, f_s \in \mathbf{R}[X]$.

i) On note $x_1 < \ldots < x_N$ les racines dans $\mathbf{R}$ des $f_i$ non identiquement nuls ;

ii) On note $x_0 = -\infty$ et $x_{N+1} = +\infty$ ;

iii) On note $I_k = ]x_k, x_{k+1}[$ et sign($f_i(I_k)$) le signe de $f_i$ sur $I_k$ (cf. proposition 2.2.9) ;

iv) On note $\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_s)$ la matrice de dimension $s \times (2N + 1)$ dont la $i$-ème rangée est

$$\mathrm{sign}(f_i(I_0)), \mathrm{sign}(f_i(x_1)), \mathrm{sign}(f_i(I_1)), \ldots, \mathrm{sign}(f_i(x_N)), \mathrm{sign}(f_i(I_N));$$

v) Si on note $m = \max(\{\deg(f_i) = i \in \{1, \ldots, s\}\})$ alors $N \leq sm$. On note $W_{s,m}$ l'union disjointe des ensembles de matrices dont les éléments appartiennent à $\{-1, 0, 1\}$ ayant $s$ rangées et $2l + 1$ colonnes avec $l \in \{0, \ldots, sm\}$.

Concrètement, la matrice $\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_s)$ est exactement le tableau de signes des polynômes $f_1, \ldots, f_s$. L'ensemble $W_{s,m}$ est l'ensemble (fini) de toutes les "matrices de tableaux de signes" pour $s$ fonctions et avec un nombre de racines inférieur ou égal à $sm$.

**Exemple 3.2.4.** Considérons les polynômes suivants,

$$f_1 = X^2 - 1 \text{ et } f_2 = X^3 - 2X^2 + X - 2 = (X-2)(X^2+1).$$

Leurs racines dans $\mathbb{R}$ sont $x_1 = -1, x_2 = 1$ et $x_3 = 2$ et on a

$$\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2) = \begin{pmatrix} 1 & 0 & -1 & 0 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 0 & 1 \end{pmatrix}.$$

**Lemme 3.2.5.** *Soit $\varphi : \{1, \ldots, s\} \to \{-1, 0, 1\}$ une fonction. Il existe un ensemble $\mathrm{W}(\varphi) \subseteq \mathrm{W}_{s,m}$ tel que pour tout champ réel clos $\mathbf{R}$ et pour tout $f_1, \ldots, f_s \in \mathbf{R}_m[X]$ le système*

$$\begin{cases} \mathrm{sign}(f_1(X))) & = \varphi(1) \\ & \vdots \\ \mathrm{sign}(f_s(X)) & = \varphi(s) \end{cases}$$

*a une solution $x \in \mathbf{R}$ si et seulement si $\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_s) \in \mathrm{W}(\varphi)$.*

*Démonstration.* Il suffit de considérer l'ensemble $\mathrm{W}(\varphi) \subseteq \mathrm{W}_{s,m}$ des matrices dont une des colonnes est $(\varphi(1) \cdots \varphi(s))$. Cet ensemble convient bien car $(\varphi(1) \cdots \varphi(s))$ est la $k$-ième colonne de $\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_s)$ si et seulement si $\mathrm{sign}(f_i(I_k)) = \varphi(i)$ pour tout $i \in \{1, \ldots, s\}$. Or $\mathrm{sign}(f_i(x))$ étant constant sur les $I_k$, c'est équivalent à l'existence d'un $x \in \mathbf{R}$ qui vérifie le système. □

Le coeur du Principe de Tarski-Seidenberg découle du lemme qui va suivre. Il nous dit qu'on peut obtenir le tableau de signe d'une suite de polynômes à partir d'un autre tableau de signes, comportant plus de polynômes, mais de degrés inférieurs. Illustrons cela avec l'exemple suivant.

**Exemple 3.2.6.** Reprenons les polynômes de l'exemple 3.2.4. Montrons comment obtenir $\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2)$ à partir de $\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2', g_1, g_2)$ où

$$f_2' = 3(X-1)(X - \frac{1}{3}) \ , \ g_1 = 2(X-2) \text{ et } g_2 = \frac{-2}{9}(X+8)$$

sont respectivement la dérivée de $f_2$, le reste de la division euclidienne de $f_2$ par $f_1$ et le reste de la division euclidienne de $f_2$ par $f_2'$.

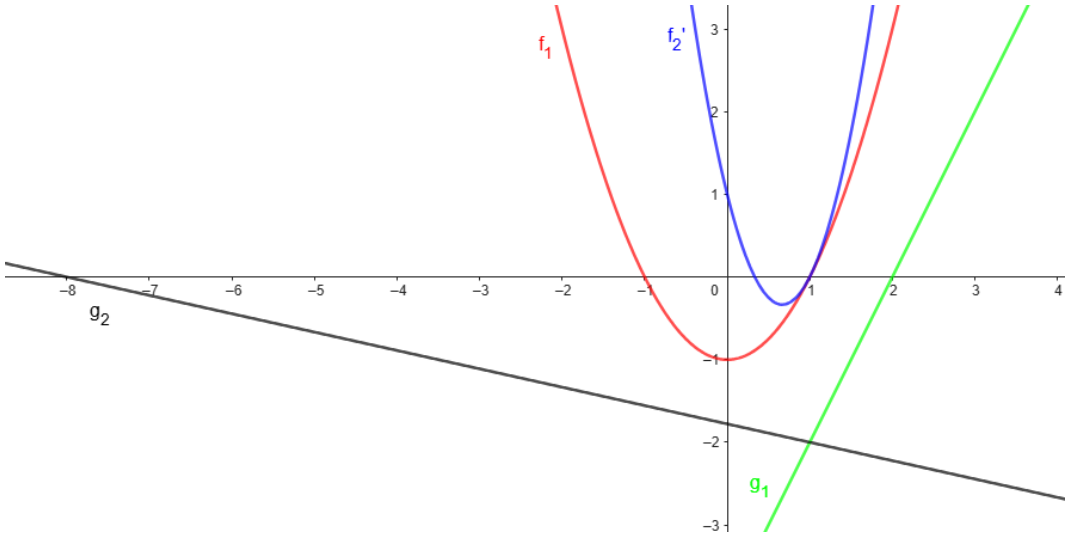


FIGURE 3.1 – Graphes des polynômes $f_1$, $f_2'$, $g_1$ et $g_2$.

Supposons avoir à notre disposition le tableau de signe de ces polynômes, qui est représenté par la matrice

$$\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2', g_1, g_2) = \begin{pmatrix} 1 & 1 & 1 & 0 & -1 & -1 & -1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & -1 & 0 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 1 \\ 1 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{pmatrix}$$

et notons $x_1, \ldots, x_5$ les racines de $f_1, f_2', g_1, g_2$ dans $\mathbb{R}$ (on sait qu'il en existe autant au vu de la matrice).

Parmi les racines $\{x_1, \ldots, x_5\}$, on extrait celles de $f_1, f_2'$ qui sont donc $x_{i_1} = x_2, x_{i_2} = x_3, x_{i_3} = x_4$ (cela découle des colonnes pour lesquelles on trouve un zéro dans les deux premières rangées du tableau). De plus, par définition de $g_1, g_2$, il existe $q_1, q_2 \in \mathbf{R}[X]$ tels que

$$f_2(x) = f_1(x)q_1(x) + g_1(x) = f_2'(x)q_2(x) + g_2(x).$$

Dès lors, on trouve que

$$f_2(x_{i_1}) = g_1(x_{i_1}) \ , \ f_2(x_{i_2}) = g_2(x_{i_2}) \ , \ f_2(x_{i_3}) = g_1(x_{i_3}) = g_2(x_{i_3}).$$

On connaît donc le signe de $f_2$ en ces points. De plus, on connaît le signe de $f_2'$ sur le tableau de signes déterminé par ces points, on peut donc en tirer, grâce au théorème des valeurs intermédiaires 2.2.9 et au corollaire 2.2.13, dans quel intervalle de ce tableau $f_2$ possède une racine. Dans ce cas, $f_2$ possède uniquement une racine dans l'intervalle $]x_{i_3}, +\infty[$ car

$$\mathrm{sign}_{\mathbb{R}}(f_2'(]x_{i_3}, +\infty[) = 1 \text{ et } \mathrm{sign}_{\mathbb{R}}(f_2(x_{i_3})) = \mathrm{sign}_{\mathbb{R}}(g_1(x_{i_3})) = -1$$

or comme $\lim_{x\to+\infty} f_2(x) = +\infty$, on en déduit que $f_2$ possède une unique racine dans $]x_{i_3}, +\infty[$.

On sait alors que $f_1$ et $f_2$ possèdent 3 racines dans $\mathbb{R}$. En effet, on a $x_{i_1}, x_{i_3}$ et un $x > x_{i_3}$. Notons $y_1, y_2, y_3$ ces trois racines. Il est temps de construire la matrice $\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2)$. Cette matrice est de dimension $7 \times 2$. Il y a donc 14 éléments à chercher. Commençons par la rangée associée à $f_1$. On a que

$$f_1(y_1) = 0 \text{ et } f_1(y_2) = 0.$$

De plus, en se basant sur le tableau de signe connu, on en déduit que $f_1$ est négatif entre $y_1$ et $y_2$ et positif partout ailleurs. Cherchons désormais les éléments de la rangée associée à $f_2$. On a

$$f_2(y_1) = f_2(x_{i_1}) = g_1(x_{i_1}) < 0$$

mais aussi

$$f_2(y_2) = g_1(x_{i_3}) < 0$$

et enfin,

$$f_2(y_3) = 0.$$

Ensuite, on a

$$\mathrm{sign}_{\mathbb{R}}(f_2(]-\infty, y_1[)) = -\mathrm{sign}_{\mathbb{R}}(f_2'(]-\infty, x_1[)) = -1$$

car $f_2(x)$ et $f_2'(x)$ sont de signes opposés pour des valeurs $x$ suffisamment petites (voir le lemme2.2.22). Par un raisonnement similaire, on a

$$\mathrm{sign}_{\mathbb{R}}(f_2(]y_3, +\infty[)) = \mathrm{sign}_{\mathbb{R}}(f_2'(]x_5, +\infty[)) = 1.$$

Ensuite,

$$\mathrm{sign}_{\mathbb{R}}(f_2(]y_1, y_2[)) = \mathrm{sign}_{\mathbb{R}}(g_1(y_1)) = -1$$

car $f_2$ ne change pas de signe dans cet intervalle et $f_2(x_2) > 0$. De même,

$$\mathrm{sign}_{\mathbb{R}}(f_2(]y_2, y_3[)) = \mathrm{sign}_{\mathbb{R}}(g_1(y_2)) = -1.$$

On peut alors construire la matrice, qui est

$$\mathrm{SIGN}_{\mathbb{R}}(f_1, f_2) = \begin{pmatrix} 1 & 0 & -1 & 0 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 0 & 1 \end{pmatrix}$$

ce qui est bien la matrice qu'on cherchait à obtenir.

Ces raisonnements se généralisent et on a le lemme suivant, qui indique qu'on peut en général déterminer le tableau de signe de $f_1, \ldots, f_s$ en fonction du tableau de signe d'autres polynômes de degré inférieur.

**Lemme 3.2.7.** *Il existe une fonction $\Phi : \mathrm{W}_{2s,m} \to \mathrm{W}_{s,m}$ tel que pour tout champ réel clos $\mathbf{R}$ et pour toute suite $f_1, \ldots, f_s \in \mathbf{R}_m[X]$ telle que $\deg(f_s) > 1$ et $f_1, \ldots, f_{s-1}$ sont non identiquement nuls, on a*

$$\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_s) = \Phi(\mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)),$$

*où $f_s'$ est la dérivée de $f_s$ et $g_1, \ldots, g_s$ sont les restes de la division euclidienne de $f_s$ par $f_1, \ldots, f_{s-1}$ et $f_s'$ respectivement.*

*Démonstration.* Soient $x_1 < \cdots < x_N$ les racines dans $\mathbf{R}$ de $f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s$, non identiquement nuls. On a $N \leq 2sm$ puisqu'il y a $2s$ polynômes de degrés inférieurs à $m$. Parmi ces racines, notons $x_{i_1}, \ldots, x_{i_M}$ les racines dans $\mathbf{R}$ de $f_1, \ldots, f_{s-1}, f'_s$. Ces racines, et donc la sous-suite $i_1, \ldots, i_M$ sont complètement déterminées par la matrice

$$\Omega = \mathrm{SIGN}_{\mathbf{R}}(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s).$$

En effet, par définition, on trouve les indices $i_1, \ldots, i_M$ en déterminant les colonnes contenant un 0 dans les $s$ premières rangées de $\Omega$. Par convention, notons $i_0 = 0$, $i_{M+1} = N+1$, $x_0 = -\infty$, $x_{N+1} = +\infty$. Par définition de $x_{i_1}, \ldots, x_{i_k}$, pour tout $k \in \{1, \ldots, M\}$, il existe (au moins un) $j \in \{1, \ldots, s\}$ tel que

$$f_j(x_{i_k}) = 0 \text{ si } j \in \{1, \ldots, s-1\},$$

et

$$f'_s(x_{i_k}) = 0 \text{ si } j = s.$$

En connaissant $\Omega$, on peut construire une fonction qui à chaque $k \in \{1, \ldots, M\}$ associe un indice $j$ satisfaisant la condition ci-dessus. La fonction

$$\Theta : \{1, \ldots, M\} \to \{1, \ldots, s\},$$

est donc telle que

$$f_s(x_{i_k}) = g_{\Theta(k)}(x_{i_k}). \tag{3.2}$$

En effet, pour tout $j \in \{1, \ldots, s-1\}$, au vu de la division euclidienne, il existe $q_j \in \mathbf{R}[X]$ tel que

$$f_s = f_j q_j + g_j,$$

et il existe $q_s \in \mathbf{R}[X]$ tel que

$$f_s = q_s f'_s + g_s.$$

La relation 3.2 est donc satisfaite, puisque pour tout $k \in \{1, \ldots, M\}$, $f_{\Theta(k)}(x_{i_k}) = 0$, si $\Theta(k) < s$ $f'_{\Theta(k)}(x_{i_k}) = 0$ si $\Theta(k) = s$.

Montrons maintenant que $\Omega$ permet de déterminer exactement pour $k \in \{0, \ldots, M\}$ si $x_{i_k}$ est une racine de $f_s$ et le nombre de racines que $f_s$ admet dans $\left]x_{i_k}, x_{i_{k+1}}\right[$.

1. Premièrement $f_s(x_{i_k}) = 0$ si et seulement si $g_{\Theta(k)}(x_{i_k}) = 0$, par (3.2), et cette information est déterminée par $\Omega$.
2. Ensuite, $f_s$ admet une racine dans $\left]x_{i_k}, x_{i_{k+1}}\right[$ ($k \in \{1, \ldots, M-1\}$ et $M > 1$), si et seulement si
$$\mathrm{sign}(g_{\Theta(k)}(x_{i_k}))\mathrm{sign}(g_{\Theta(k+1)}(x_{i_{k+1}})) = -1,$$
et dans ce cas cette racine est unique. En effet, puisque $f'_s$ ne s'annule pas dans l'intervalle $\left]x_{i_k}, x_{i_{k+1}}\right[$ il y garde un signe constant, et $f_s$ est donc strictement croissant ou strictement décroissant sur $\left[x_{i_k}, x_{i_{k+1}}\right]$ selon le signe de $f'_s$. Si $f_s(c) = 0$ pour un $c \in \left]x_{i_k}, x_{i_{k+1}}\right[$ et par exemple $f_s$ est strictement croissant, alors on a $f_s(x_{i_k}) <$

$0 < f_s(x_{i_{k+1}})$, et par (3.2), $g_{\Theta(k)}(x_{i_k})$ et $g_{\Theta(k+1)}(x_{i_{k+1}})$ sont de signes contraires. On procède de même si $f_s$ est strictement décroissant. Réciproquement, si cette condition est satisfaite, alors $f_s(x_{i_k})$ et $f_s(x_{i_{k+1}})$ sont de signes contraires et par le théorème des valeurs intermédiaires, $f_s$ admet une racine dans $\left]x_{i_k}, x_{i_{k+1}}\right[$. Enfin, comme $f_s'$ ne s'annule pas sur cette intervalle, le lemme de Rolle 2.2.11 implique que la racine est unique.

3. Le polynôme $f_s$ admet une racine sur $]-\infty, x_{i_1}[$ (si $M \geq 1$) si et seulement si

$$\text{sign}(f_s'(]-\infty, x_1[))\text{sign}(g_{\Theta(1)}(x_{i_1})) = 1,$$

et dans ce cas, cette racine est unique. En effet, on procède comme ci-dessus : si $f_s'$ est positif sur l'intervalle considéré, et si $f_s$ y admet une racine $c$, alors $0 = f_s(c) < f_s(x_{i_1}) = g_{\Theta(1)}(x_{i_1})$, puisque $f_s$ est strictement croissant sur l'intervalle. Si $f_s'$ est négatif sur l'intervalle, le même raisonnement donne $g_{\Theta(1)}(x_{i_1})) < 0$. Réciproquement, supposons la condition satisfaite et par exemple $f_s'$ positif sur l'intervalle (l'autre cas est similaire). Alors $f_s(x_{i_1}) > 0$ et, sur un intervalle du type $]-\infty, a[$, $f_s$ et $f_s'$ ont le signe de leurs termes de plus haut degré, qui sont de signes contraires, donc $f_s(x)$ est négatif pour des valeurs de $x$ suffisamment petites. Le théorème des valeurs intermédiaires fournit l'existence d'une racine pour $f_s$. L'unicité se démontre comme plus haut.

4. Le polynôme $f_s$ admet une racine sur $]x_{i_M}, +\infty[$ (si $M \geq 1$) si et seulement si

$$\text{sign}(f_s'(]x_N, +\infty[))\text{sign}(g_{\Theta(M)}(x_{i_M})) = -1,$$

auquel cas la racine est unique. Cette assertion se démontre comme la précédente, en inversant là où c'est nécessaire les signes d'inégalité, et en notant que pour $x$ suffisamment grand, $f_s(x)$ et $f_s'(x)$ ont le même signe, celui de leurs termes dominants.

5. Enfin, si $M = 0$, $f_s'$ est de signe constant sur $\mathbf{R}$, donc $f_s$ y est strictement monotone. De plus, par les raisonnements ci-dessus, $f_s$ doit changer de signe sur $\mathbf{R}$, puisque $f_s(x)$ a le même signe que $f_s'(x)$ pour $x$ suffisamment grand et le signe opposé pour $x$ suffisamment petit. Donc ce cas, $f_s$ admet une unique racine sur $\mathbf{R}$.

Montrons maintenant que $\Omega$ permet à lui seul de déterminer le tableau de signes associé à $f_1, \ldots, f_s$. Ses $s-1$ premières lignes déterminent les racines de $f_1, \ldots, f_{s-1}$, qui sont parmi $x_{i_1}, \ldots, x_{i_M}$, et nous venons de voir que $\Omega$ permet également de déterminer si $x_{i_1}, \ldots, x_{i_M}$ sont racines de $f_s$, ou si $f_s$ admet une racine dans les intervalles déterminés par ces points $x_{i_1}, \ldots, x_{i_M}$.

Notons maintenant $y_1 < \cdots < y_L$ les racines dans $\mathbf{R}$ de $f_1, \ldots, f_s$ (avec $L \leq sm$) et établissons le tableau de signes associé à $f_1, \ldots, f_s$ à partir de données contenues dans $\Omega$. On pose $y_0 = -\infty$ et $y_{L+1} = +\infty$. Pour tout $j \in \{1, \ldots, s\}$, il s'agit d'établir le signe de $f_j(y_l)$, pour $1 \leq l \leq L$ et le signe de $f_j$ sur l'intervalle $]y_l, y_{l+1}[$, pour $0 \leq l \leq M$. Il faut distinguer selon que $j$ vaut $s$ ou non, et selon le fait que la racine $y_l = x_{i_k}$, pour $1 \leq k \leq M$, ou $y_l \in \left]x_{i_k}, x_{i_{k+1}}\right[$, pour un $k \in \{0, \ldots, M\}$.

1. Déterminons le signe de $f_j(y_l)$ :
   A) On traite le cas $y_l = x_{i_k}$,
      a) si $j \leq s-1$, on a $f_j(y_l) = f_j(x_{i_k})$ et le signe est déterminé par $\Omega$, en considérant la ligne correspondante à $f_j$ et la colonne correspondante à $x_{i_k}$ ;
      b) si $j = s$, par (3.2), on a $f_s(y_l) = g_{\Theta(k)}(x_{i_k})$, dont le signe est déterminé par $\Omega$ ;
   B) Traitons maintenant le cas $y_l \in \left]x_{i_k}, x_{i_{k+1}}\right[$ ;
      a) si $j \leq s-1$, $f_j$ est de signe constant sur $\left]x_{i_k}, x_{i_{k+1}}\right[$ (et ce signe se lit sur $\Omega$), et $y_l$ est dans cet intervalle ;
      b) si $j = s$, comme $y_l$ est une racine de $f_1, \ldots, f_s$, mais n'est pas une racine de $f_1, \ldots, f_{s-1}$ (qui sont parmi $x_{i_1}, \ldots, x_{i_M}$), on a $f_s(y_l) = 0$.
2. Déterminons le signe de $f_j$ sur l'intervalle $]y_l, y_{l+1}[$. La distinction principale se fait sur $j$ :
   a) Si $j \leq s-1$, alors si $y_l = x_{i_k}$ (pour $0 < k \leq M$) ou $y_l \in \left]x_{i_k}, x_{i_{k+1}}\right[$ (pour $0 \leq k \leq M$), $f_j$ est de signe constant sur $\left]x_{i_k}, x_{i_{k+1}}\right[$, et sur $]y_l, y_{l+1}[$. Ces deux intervalles ont une intersection non vide, donc on a
   $$\operatorname{sign}(f_j(]y_l, y_{l+1}[)) = \operatorname{sign}(f_j(\left]x_{i_k}, x_{i_{k+1}}\right[)).$$
   b) Si $j = s$, alors on traite plusieurs cas :
      i) Si $l \neq 0$ et $y_l = x_{i_k}$ pour un $k \in \{1, \ldots, M\}$, deux cas peuvent se produire : soit $f_s(x_{i_k}) \neq 0$ et $f_s$ garde le signe de $f_s(x_{i_k})$ sur un voisinage de $y_l = x_{i_k}$, donc on a
      $$\operatorname{sign}(f_s(]y_l, y_{l+1}[)) = \operatorname{sign}(f_s(x_{i_k})) = \operatorname{sign}(g_{\Theta(k)}(x_{i_k})).$$
      Soit $f_s(x_{i_k}) = 0$, et le signe de $f_s$ sur l'intervalle $]y_l, y_{l+1}[$ est déterminé par la croissance de $f_s$, c'est-à-dire le signe de $f'_s$, que l'on connaît au moins sur $\left]x_{i_k}, x_{i_{k+1}}\right[$. On a donc
      $$\operatorname{sign}(f_s(]y_l, y_{l+1}[)) = \operatorname{sign}(f'_s(\left]x_{i_k}, x_{i_{k+1}}\right[)).$$
      ii) Si $l \neq 0$ et $y_l \in \left]x_{i_k}, x_{i_{k+1}}\right[$ pour un $k \in \{0, \ldots, M\}$, alors $f_s(y_l) = 0$ et le signe de $f_s$ sur $]y_l, y_{l+1}[$ est encore déterminé par la croissance de $f_s$ sur $\left]x_{i_k}, x_{i_{k+1}}\right[$, c'est-à-dire le signe de $f'_s$ sur cet intervalle. On a donc dans ce cas aussi
      $$\operatorname{sign}(f_s(]y_l, y_{l+1}[)) = \operatorname{sign}(f'_s(\left]x_{i_k}, x_{i_{k+1}}\right[)).$$
      iii) Finalement, si $l = 0$, on détermine le signe de $f_s$ sur $]-\infty, y_1[)$ en notant que pour des valeurs de $x$ suffisamment petites, $f_s(x)$ et $f'_s(x)$ sont de signes opposés. On a donc
      $$\operatorname{sign}(f_s(]-\infty, y_1[)) = \operatorname{sign}(f'_s(]-\infty, x_1[)).$$

On a donc montré qu'à partir de la seule information contenue dans le tableau de signe $\Omega$ de $(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s)$, on peut reconstruire le tableau de signes de $(f_1, \ldots, f_s)$ (sans précision de la position exacte des racines), et indépendamment des fonctions considérées. C'est cette correspondance qui définit la fonction $\Phi$. □

On voit ici qu'à partir de $s$ polynômes, on obtient $2s$ polynômes juste pour abaisser le degré d'un des $s$ polynômes initiaux. Le nombre de polynômes à traiter explose de façon exponentielle. Cela peut expliquer pourquoi le Principe de Tarski-Seidenberg n'est pas utilisé en pratique.

Par la suite, on va définir un ordre sur les $n$-uplets d'entiers positifs, ceux-ci étant associés à des degrés des polynômes. Cela permettra d'effectuer une récurrence sur les $n$-uplets de degrés de plusieurs polynômes afin d'appliquer ce lemme.

Comme on s'intéresse aux degrés de polynômes $f_1, \ldots, f_s$ dont l'ordre n'a pas d'importance, on peut formuler les raisonnements qui suivent soit en considérant qu'on ordonne les degrés des polynômes par ordre décroissant, soit que l'on considère comme équivalents les $n$-uplets de degrés qui sont images l'un de l'autre par une permutation.

**Définition 3.2.8.** On note $\mathcal{E}$ l'ensemble $\cup_{n\in\mathbb{N}_0}\mathbb{N}^n = \{\sigma = (\sigma_1, \ldots, \sigma_n) : n \in \mathbb{N}_0, \sigma_1, \ldots, \sigma_n \in \mathbb{N}\}$. Pour $\sigma, \tau \in \mathcal{E}$ on dit que $\sigma$ est équivalent à $\tau$ et on note $\sigma \sim \tau$ si et seulement si $\sigma$ et $\tau$ sont égaux à permutation de leurs éléments près.

**Exemple 3.2.9.** Considérons $\sigma = (1, 0, 0, 2, 3, 1)$ et $\tau = (0, 0, 1, 1, 2, 3)$ alors on a $\sigma \sim \tau$.

Il s'agit d'une relation d'équivalence. La réflexivité est évidente, la transitivité découle du fait que la composition de permutations est une permutation et le caractère symétrique vient du fait que l'inverse d'une permutation est une permutation.

Afin de définir un ordre sur $\mathcal{E}_{/\sim}$, on introduit les fonctions suivantes.

**Définition 3.2.10.** Pour $\sigma \in \mathcal{E}$, on note $\theta_k(\sigma)$ le nombre d'occurrences de $k \in \mathbb{N}$ dans la suite de naturels $\sigma$.

Bien sûr $\theta_k$ est une fonction définie sur $\mathcal{E}$ et constante sur les classes d'équivalence. Elle passe donc au quotient en une fonction que nous notons encore $\theta_k$. De même, la fonction maximum $\max : \mathcal{E} \to \mathbb{N} : \sigma \mapsto \max(\sigma_1, \ldots, \sigma_n)$ passe au quotient en une fonction qu'on note également max. On peut maintenant introduire l'ordre sur $\mathcal{E}_{/\sim}$.

**Définition 3.2.11.** Soient $\sigma, \tau \in \mathcal{E}_{/\sim}$, on définit l'ordre $\prec$ via

$$\sigma \prec \tau,$$

s'il existe $p \in \mathbb{N}$ tel que pour tout $q > p$,

$$\theta_q(\sigma) = \theta_q(\tau),$$

et

$$\theta_p(\sigma) < \theta_p(\tau).$$

On a $\sigma \preceq \tau$ si $\sigma \prec \tau$ ou si $\sigma = \tau$.

**Exemple 3.2.12.** Considérons $\sigma = [(3,0,2,4,0,1,1,3)]$ et $\tau = [(4,1,2,0)]$. Alors il est clair que

$$\theta_q(\sigma) = \theta_q(\tau) = 0,$$

pour tout $q > 4$. On a de plus que

$$\theta_4(\sigma) = \theta_4(\tau) = 1,$$

et également que

$$\theta_3(\sigma) = 2 > 0 = \theta_3(\tau).$$

On en déduit alors que $\tau \prec \sigma$.

On constate que si $\max(\tau) < \max(\sigma)$, alors $\theta_q(\tau) = \theta_q(\sigma) = 0$ pour $q > p = \max(\sigma)$, et $\theta_p(\sigma) \neq 0$, $\theta_p(\tau) = 0$, donc $\tau \prec \sigma$. Si $\max(\tau) = \max(\sigma)$, alors si on note $k$ ce nombre, on a $\theta_q(\tau) = \theta_q(\sigma) = 0$ pour $q > k$, et on a alors par définition

$$\tau \prec \sigma \Leftrightarrow (\theta_k(\tau), \dots, \theta_0(\tau)) <_{\text{lex}} (\theta_k(\sigma), \dots, \theta_0(\sigma)), \tag{3.3}$$

où $<_{\text{lex}}$ est l'ordre lexicographique sur $\mathbb{N}^{k+1}$. Réciproquement, si $\sigma \prec \tau$, comme $\theta_q(\sigma) = \theta_q(\tau) = 0$ si $q$ est supérieur à $\max(\tau)$ et à $\max(\sigma)$, on doit avoir $\max(\sigma) \leq \max(\tau)$, et aussi l'équivalence (3.3), s'ils sont égaux.

**Proposition 3.2.13.** *La relation $\preceq$ est un bon ordre sur $\mathcal{E}_{/\sim}$.*

*Démonstration.* On commence par montrer que $\preceq$ est un ordre sur $\mathcal{E}_{/\sim}$.

1) Par définition, pour tout $\sigma \in \mathcal{E}_{/\sim}$, on a $\sigma \preceq \sigma$ et la relation est donc réflexive.
2) Soit $\sigma, \tau, \alpha \in \mathcal{E}_{/\sim}$ tels que $\sigma \preceq \tau$ et $\tau \preceq \alpha$ et montrons $\sigma \preceq \alpha$. On a $\max(\sigma) \leq \max(\tau)$ et $\max(\tau) \leq \max(\alpha)$. Si une des inégalités est stricte, on obtient $\max(\sigma) < \max(\alpha)$, puis $\sigma \prec \alpha$. Dans le cas contraire, si on note $k$ le nombre $\max(\sigma) = \max(\alpha) = \max(\tau)$, on a
$$(\theta_k(\sigma), \dots, \theta_0(\sigma)) \leq_{\text{lex}} (\theta_k(\tau), \dots, \theta_0(\tau)) \leq_{\text{lex}} (\alpha_k(\tau), \dots, \alpha_0(\tau)),$$
et on conclut par transitivité de l'ordre lexicographique sur $\mathbb{N}^{k+1}$.
3) Soient $\sigma, \tau \in \mathcal{E}_{/\sim}$ tels que $\sigma \preceq \tau$ et $\tau \preceq \sigma$. On a alors $\max(\sigma) \leq \max(\tau)$ et $\max(\tau) \leq \max(\sigma)$. Donc $\max(\tau) = \max(\sigma)$, et si on note $k$ ce nombre, on a
$$(\theta_k(\sigma), \dots, \theta_0(\sigma)) = (\theta_k(\tau), \dots, \theta_0(\tau))$$
vu l'antisymétrie de l'ordre lexicographique sur $\mathbb{N}^{k+1}$. Enfin, cette condition implique que $\sigma$ et $\tau$ contiennent les mêmes entiers avec les mêmes multiplicités, donc ils sont égaux.
4) Montrons désormais que toute partie $\mathcal{P}$ non vide de $\mathcal{E}_{/\sim}$ possède un élément minimum pour l'ordre $\preceq$. L'ensemble $\max(\mathcal{P}) = \{\max(\sigma) : \sigma \in \mathcal{P}\}$ est non vide et inclus dans $\mathbb{N}$. Il admet un minimum $k$. Par définition l'ensemble $\mathcal{P}_k = \{\sigma \in P : \max(\sigma) = k\}$ est non vide et sur cet ensemble $\preceq$ est équivalent à l'ordre lexicographique, qui est un bon ordre sur $\mathbb{N}^{k+1}$, donc $\mathcal{P}_k$ admet un minimum, qui est également un minimum de $\mathcal{P}$.

□

**Proposition 3.2.14.** *Soient $f_i(X,Y) \in (\mathbb{Z}[Y])[X]$ pour $i \in \{1,\dots,s\}$, de la forme 3.1, avec $Y = (Y_1,\dots,Y_n)$ et soit*

$$m = \max\{m_i : i \in \{1,\dots,s\}\}.$$

*Soit $W' \subseteq W_{s,m}$, il existe une combinaison booléenne $\mathcal{B}(Y)$ d'équations et inéquations polynomiales avec des polynômes de $\mathbb{Z}[Y]$ telle que pour tout champ réel clos $\mathbf{R}$ et pour tout $y \in \mathbf{R}^n$, on a*

$$\mathrm{SIGN}_{\mathbf{R}}(f_1(X,y),\dots,f_s(X,y)) \in W',$$

*si et seulement si $\mathcal{B}(y)$ est satisfait dans $\mathbf{R}$.*

*Démonstration.* Sans perte de généralités, on peut supposer que $f_1,\dots,f_s$ sont non identiquement nuls et que les $h_{1,m_1}(Y),\dots,h_{s,m_s}(Y)$ non plus. A $(f_1,\dots,f_s)$ on associe $[(m_1,\dots,m_s)]_\sim$ la classe de leur suite de degrés en $X$. Comme $\preceq$ est un bon ordre, on peut procéder par récurrence, en commençant par le minimum, qui correspond au cas $m = 0$, si $m = \max\{m_1,\dots,m_s\}$. Si $m = 0$, alors les polynômes $f_1,\dots,f_s$ sont indépendants de $X$, et appartiennent à $\mathbb{Z}[Y]$. Dès lors,

$$\mathrm{SIGN}_{\mathbf{R}}(f_1(X,y),\dots,f_s(X,y)) = (\mathrm{sign}(h_{1,0}(y)),\dots,\mathrm{sign}(h_{s,0}(y))).$$

En se servant des tableaux de signe des polynômes $h_{i,m_i}$ on peut alors trouver une combinaison booléenne $\mathcal{B}$ qui satisfait l'énoncé. Supposons désormais que $m \geq 1$ (et que $m = m_s$). Considérons l'ensemble $W'' \subseteq W_{2s,m}$ défini par

$$W'' = \Phi^{-1}(W'),$$

où $\Phi$ est définie dans le lemme 3.2.7. Par ce même lemme, pour tout champ réel clos $\mathbf{R}$ et pour tout $y \in \mathbf{R}^n$ tel que $h_{i,m_i}(y) \neq 0$ pour tout $i \in \{1,\dots,s\}$. On a

$$\mathrm{SIGN}_{\mathbf{R}}(f_1(X,y),\dots,f_s(X,y)) \in W',$$

si et seulement si

$$\mathrm{SIGN}_{\mathbf{R}}(f_1(X,y),\dots,f_{s-1}(X,y),f'_s(X,y),g_1(X,y),\dots,g_s(X,y)) \in W'',$$

où $f'_s = \frac{\partial f_s}{\partial X}$ et $g_i$ le reste de la division euclidienne par rapport à $X$ de $f_s$ par $f_i$ pour tout $i \in \{1,\dots,s-1\}$ et par $f'_s$ si $i = s$, qu'on a respectivement multiplié par une puissance paire appropriée de $h_{i,m_i}$ afin de faire disparaître les dénominateurs apparaissant dans les restes issus des divisions euclidiennes. Dès lors,

$$[(m_1,\dots,m_{s-1},m_s-1,n_1,\dots,n_s)]_\sim \prec [(m_1,\dots,m_s)]_\sim.$$

où $n_i$ est le degré de $X$ dans $g_i$ pour $i \in \{1,\dots,s\}$, étant donné que $g_i$ est le reste d'une division euclidienne de $f_s$, on a $n_i < m_s$ pour tout $i \in \{1,\dots,s\}$ car $m = m_s$. On applique alors l'hypothèse de récurrence. Si l'un des $h_{i,m_i}(y) = 0$ alors on tronque le polynôme correspondant afin d'avoir un polynôme dont le terme de plus haut degré soit non nul. □

*Démonstration du Théorème de Tarski-Seidenberg.* Par la proposition 3.2.14 et le lemme 3.2.5, on a démontré le théorème 3.2.2, c'est à dire le Principe de Tarski-Seidenberg. □

## 3.3 Élimination des quantificateurs

Le résultat qu'on a obtenu fonctionne pour les polynômes à coefficients dans $\mathbb{Z}$. Nous allons montrer qu'on peut l'étendre à n'importe quel champ réel, et donc qu'on peut effectuer une élimination des quantificateurs dans le langage des champs réels à coefficients dans un champ réel clos $\mathbf{R}$.

**Corollaire 3.3.1.** *Soient* $\mathbf{F}$ *un champ réel et*

$$f_1(X,Y),\dots,f_s(X,Y)\in\mathbf{F}[X,Y]$$

*avec* $Y=(Y_1,\dots,Y_n)$. *Soit également une fonction*

$$\varphi:\{1,\dots,s\}\to\{-1,0,1\}.$$

*Alors il existe une combinaison booléenne* $\mathcal{B}(Y)$ *d'égalités et inégalités polynomiales de polynômes de* $\mathbf{F}[Y]$ *tel que pour tout champ réel clos* $\mathbf{R}$ *contenant* $\mathbf{F}$ *et pour tout* $y\in\mathbf{R}^n$ *le système*

$$\begin{cases} \operatorname{sign}(f_1(X,y))) & =\varphi(1)\\ & \vdots\\ \operatorname{sign}(f_s(X,y)) & =\varphi(s)\end{cases}$$

*admet une solution* $x\in\mathbf{R}$ *si et seulement si* $\mathcal{B}(y)$ *est vrai dans* $\mathbf{R}$.

*Démonstration.* Pour tout $i\in\{1,\dots,s\}$, on considère

$$g_i(X,Y,a)=f_i(X,Y)$$

où $a$ est la suite de coefficient des $f_i$ et $g_i\in\mathbb{Z}[X,Y,T]$ ($a\in\mathbf{R}^m$ pour un certain $m$). On applique alors le Principe de Tarski-Seidenberg aux polynômes $g_i$ en ayant remplacé $y\in\mathbf{R}^n$ par $(y,a)\in\mathbf{R}^{n+m}$ dans l'énoncé du théorème 3.2.2. □

**Exemple 3.3.2.** Si on a $\alpha,\beta,\gamma\in\mathbf{F}$ et le polynôme

$$f(X,Y_1,Y_2)=5\alpha X^2+4\alpha XY_2-3\beta\gamma Y_1Y_2\in\mathbf{F}[X,Y_1,Y_2]$$

Alors on considère le polynôme

$$g(X,Y_1,Y_2,\alpha,\beta,\gamma)=5(\alpha X^2)+4(\alpha XY_2)-3(\beta\gamma Y_1Y_2)\in\mathbb{Z}[X,Y_1,Y_2,\alpha,\beta,\gamma].$$

Dès lors, pour toute formule $\Psi$ dans le langage des champs ordonnés, il existe une formule sans quantificateur $\Phi$ telle que $\mathrm{Reali}(\Psi)=\mathrm{Reali}(\Phi)$.

# Chapitre 4

# Ensembles et fonctions semi-algébriques

Dans ce chapitre, nous allons introduire les ensembles et les fonctions semi-algébriques ainsi que démontrer le théorème des fonctions implicites dans ce cadre. Nous allons montrer que les ensembles semi-algébriques sont exactement les ensembles de réalisation d'une formule dans le langage des champs ordonnés. Les fonctions semi-algébriques ainsi que le théorème des fonctions implicites nous serviront dans le chapitre 6. Les résultats présents dans ce chapitre sont tirés de [1, chap. 3] et [2, chap. 2].

## 4.1 Ensembles semi-algébriques

Les ensembles semi-algébriques sont une généralisation des ensembles algébriques. Commençons par rappeler ce que sont les ensembles algébriques.

**Définition 4.1.1.** Soit $\mathbf{R}$ un champ réel clos. Les sous-ensembles algébriques de $\mathbf{R}^n$ sont les ensembles décrits comme étant de la forme

$$\{x \in \mathbf{R}^n : \bigwedge_{P \in \mathcal{P}} P(x) = 0\},$$

où $\mathcal{P}$ est un sous-ensemble fini de $\mathbf{R}[X_1, \ldots, X_n]$.

**Exemple 4.1.2.** L'ensemble $\mathbf{R}^n$ est algébrique car si on considère $\mathcal{P} = \{0\}$ alors

$$\{x \in \mathbf{R}^n : \bigwedge_{P \in \mathcal{P}} P(x) = 0\} = \mathbf{R}^n .$$

**Définition 4.1.3.** L'ensemble des ensembles semi-algébriques de $\mathbf{R}^n$ est le plus petit ensemble de sous-ensembles de $\mathbf{R}^n$ qui :

1) contient tous les ensembles de la forme $\{x \in \mathbf{R}^n : P(x) > 0\}$ où $P \in \mathbf{R}[X_1, \ldots, X_n]$,

2) est stable par union finie, intersection finie et par passage au complémentaire.

La définition posée ci-dessus n'est raisonnable que si on prouve l'existence et l'unicité de l'ensemble dont il y est question.

**Proposition 4.1.4.** *Il existe un ensemble* $\mathrm{S} \subset \mathcal{P}(\mathbf{R}^n)$ *qui satisfait les conditions suivantes :*
*1) il contient tous les ensembles de la forme* $\{x \in \mathbf{R}^n : P(x) > 0\}$ *où* $P \in \mathbf{R}[X_1, \ldots, X_n]$,
*2) il est stable par union finie, intersection finie et complémentaire.*
*De plus,* S *est inclus dans tout ensemble satisfaisant ces conditions, et cet ensemble est unique.*

*Démonstration.* Considérons

$$\mathcal{F} = \{s \subset \mathcal{P}(\mathbf{R}^n) : s \text{ satisfait 1) et 2)}\}.$$

On a $\mathcal{F} \neq \emptyset$ car $s = \mathcal{P}(\mathbf{R}^n) \in \mathcal{F}$. On considère alors l'ensemble

$$S = \bigcap_{s \in \mathcal{F}} s.$$

Il est clair que cet ensemble satisfait les deux conditions de l'énoncé. Par construction, il est aussi inclus dans tout ensemble satisfaisant ces conditions. Enfin, il est unique par minimalité. □

**Remarque 4.1.5.** Soit $P \in \mathbf{R}[X_1, \ldots, X_n]$, on a

$$\{x \in \mathbf{R}^n : P(x) = 0\} = \big(\{x \in \mathbf{R}^n : P(x) > 0\} \cup \{x \in \mathbf{R}^n : -P(x) > 0\}\big)^{\mathrm{c}}.$$

La stabilité par intersection assure donc que les ensembles algébriques sont des ensembles semi-algébriques. Il en découle qu'un ensemble est semi-algébrique si et seulement si c'est la réalisation d'une formule sans quantificateur.

**Lemme 4.1.6.** *Tout ensemble semi-algébrique de* $\mathbf{R}^n$ *peut s'écrire comme une union finie d'ensembles de la forme*

$$\{x \in \mathbf{R}^n : f_1(x) = \cdots = f_l(x) = 0, g_1(x) > 0, \ldots, g_m(x) > 0,$$

*où* $f_1, \ldots, f_l, g_1, \ldots, g_m \in \mathbf{R}[X_1, \ldots, X_n]$.

*Démonstration.* Ces unions finies d'ensembles sont clairement semi-algébriques. De plus, la famille des unions finies de ces ensembles est clairement close par union finie, intersection finie et par passage au complémentaire. □

**Remarque 4.1.7.** Il découle du lemme 4.1.6 que les ensembles semi-algébriques de $\mathbf{R}$ sont exactement les unions finies de points et d'intervalles ouverts (bornés ou non).

**Exemple 4.1.8.** Au vu de la remarque 4.1.7, on sait que $\mathbb{Z}$ n'est pas un ensemble semi-algébrique de $\mathbb{R}$.

Le théorème suivant est une conséquence géométrique du Principe de Tarski-Seidenberg. Ce résultat est parfois appelé théorème de Tarski-Seidenberg.

**Théorème 4.1.9.** *Soit $S$ un ensemble semi-algébrique de $\mathbf{R}^{n+1}$ et soit la projection*

$$\pi : \mathbf{R}^{n+1} \to \mathbf{R}^n : (x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n).$$

*Alors l'ensemble $\pi(S)$ est un ensemble semi-algébrique de $\mathbf{R}^n$.*

*Démonstration.* Par le lemme 4.1.6, on peut supposer que

$$S = \{(y, x) \in \mathbf{R}^n \times \mathbf{R} : f_1(y, x) = \ldots = f_l(y, x) = 0, g_1(y, x) > 0, \ldots, g_m(y, x) > 0\}.$$

Montrons alors que l'ensemble

$$\pi(S) = \{y \in \mathbf{R}^n : \exists x \in \mathbf{R} : (y, x) \in S\},$$

est semi-algébrique. Par le corollaire 3.3.1, on sait qu'il existe une combinaison booléenne $\mathcal{B}(Y)$ d'égalités et d'inégalités polynomiales de polynômes de $\mathbf{R}[Y]$ telle que

$$\forall y \in \mathbf{R}^n, \exists x \in \mathbf{R} : (y, x) \in S \Leftrightarrow \mathcal{B}(y) \text{ est satisfait dans } \mathbf{R}^n.$$

Donc $\pi(S) = \{y \in \mathbf{R}^n : \mathcal{B}(y)\}$. On en déduit que $\pi(S)$ est semi-algébrique. □

**Proposition 4.1.10.** *Soit $\Phi(X)$ une formule dans le langage des champs ordonnés. Alors l'ensemble* $\text{Reali}(\Phi) = \{x \in R^n : \Phi(x)\}$ *est un ensemble semi-algébrique.*

*Démonstration.* Étant donné la remarque 4.1.5. Il suffit de le vérifier pour les formules avec quantificateurs. Si $\Phi(X)$ est de la forme $\exists Y : \Theta(X, Y)$ où l'ensemble

$$\text{Reali}(\Theta) = \{(x, y) \in \mathbf{R}^{n+1} : \Theta(x, y)\}$$

est un ensemble semi-algébrique alors l'ensemble $\text{Reali}(\Phi) = \{x \in \mathbf{R}^n : \Phi(x)\}$ est la projection de $\text{Reali}(\Theta)$ et est donc semi-algébrique par le théorème 4.1.9. Pour le cas des $(\forall Y)\Theta$, on les transforme en $\neg((\exists Y)(\neg\Theta))$. □

On en déduit donc que les ensembles semi-algébriques sont exactement les ensembles de la forme $\text{Reali}(\Phi)$ où $\Phi$ est une formule dans le langage des champs ordonnés.

## 4.2 Fonctions semi-algébriques

A partir des ensembles semi-algébriques, on définit la notion de fonction semi-algébrique. Rappelons que $\mathbf{R}^n$ est muni de la topologie euclidienne définie en 2.2.8, ce qui nous apporte une notion de continuité.

**Définition 4.2.1.** Soient $A \subset \mathbf{R}^n$ et $B \subset \mathbf{R}^m$ deux ensembles semi-algébriques, une fonction $f : A \to B$ est semi-algébrique si son graphe

$$\mathcal{G}(f) = \{(x, y) \in A \times B : y = f(x)\}$$

est un ensemble semi-algébrique de $\mathbf{R}^n \times \mathbf{R}^m$.

**Exemple 4.2.2.** Considérons la fonction

$$f : \mathbf{R} \to \mathbf{R} : \begin{cases} x^2 & \text{si } x \leq 1 \\ 2x+1 & \text{si } x > 1. \end{cases}$$

Cette fonction est semi-algébrique car son graphe est l'ensemble semi-algébrique

$$\mathcal{G}(f) = \{(x,y) \in \mathbf{R}^2 : x-1 \leq 0 \wedge y - x^2 = 0\} \cup \{(x,y) \in \mathbf{R}^2 : x-1 > 0 \wedge y - 2x - 1 = 0\}.$$

**Exemple 4.2.3.** Considérons la fonction

$$\sin : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x).$$

Cette fonction n'est pas semi-algébrique. En effet, le graphe de cette fonction est l'ensemble

$$\mathcal{G} = \{(x, \sin(x)) : x \in \mathbb{R}\}.$$

Or cet ensemble n'est pas semi-algébrique. En effet, considérons l'ensemble semi-algébrique

$$A = \{(x,y) \in \mathbb{R}^2 : y = 0\}.$$

Donc si $\mathcal{G}$ était semi-algébrique, l'ensemble

$$\mathcal{G} \cap A = \{(x, \sin(x)) \in \mathbb{R}^2 : \sin(x) = 0\} = \{(\pi z, 0) : z \in \mathbb{Z}\}$$

serait également semi-algébrique, or cet ensemble n'est pas semi-algébrique étant donné la remarque 4.1.7.

**Proposition 4.2.4.** *Soient $A, B, C$ des ensembles semi-algébriques, si $f : A \to B$ et $g : B \to C$ sont des fonctions semi-algébriques (continues) alors la fonction composée $g \circ f : A \to C$ est une fonction semi-algébrique (continue).*

*Démonstration.* Notons $\mathcal{G}(f) \subset \mathbf{R}^{m+n}$ et $\mathcal{G}(g) \subset \mathbf{R}^{n+p}$ les graphes de $f$ et de $g$. Le graphe de $g \circ f$ est la projection de $(\mathcal{G}(f) \times \mathbf{R}^p) \cap (\mathbf{R}^m \times \mathcal{G}(g))$ sur $\mathbf{R}^{m+p}$ et est donc semi-algébrique par la proposition 4.1.9. □

On en tire que l'ensemble des fonctions semi-algébriques définies sur un ensemble semi-algébrique $S$ forme un anneau.

**Corollaire 4.2.5.** *Soient $S$ un ensemble semi-algébrique et $f, g : S \to \mathbf{R}$ deux fonctions semi-algébriques. Alors $f + g$ et $fg$ sont deux fonctions semi-algébriques.*

*Démonstration.* Les applications $(f,g) : S \to \mathbf{R}^2$, $+ : \mathbf{R}^2 \to \mathbf{R}$ et $\cdot : \mathbf{R}^2 \to \mathbf{R}$ sont semi-algébriques car leurs graphes

$$\begin{aligned} \mathcal{G}((f,g)) &= \{(x,y,z) \in S \times \mathbf{R}^2 : (x,y) \in \mathcal{G}(f) \wedge (x,z) \in \mathcal{G}(g)\}, \\ \mathcal{G}(+) &= \{(x,y,z) \in \mathbf{R}^3 : z = x + y\}, \\ \mathcal{G}(\cdot) &= \{(x,y,z) \in \mathbf{R}^3 : z = xy\}, \end{aligned}$$

sont semi-algébriques. La proposition 4.2.4 permet de conclure. □

**Définition 4.2.6.** Si $S$ et $T$ sont des ensembles semi-algébriques, un homéomorphisme semi-algébrique $f : S \to T$ est une bijection semi-algébrique, continue et d'inverse continue. Si un tel homéomorphisme existe, on dit que $S$ et $T$ sont des ensembles semi-algébriquement homéomorphes.

**Proposition 4.2.7.** *Soit $f : S \to T$ une fonction semi-algébrique. Soient $S' \subseteq S$ et $T' \subseteq T$ des ensembles semi-algébriques, alors $f(S')$ et $f^{-1}(T')$ sont semi-algébriques.*

*Démonstration.* L'ensemble $f(S')$ est l'image de $(S' \times T) \cap \mathcal{G}(f)$ selon la projection de $S \times T \to T$. De même, l'ensemble $f^{-1}(T')$ est l'image de $(S \times T') \cap \mathcal{G}(f)$ selon la projection $S \times T \to S$. Le théorème 4.1.9 permet de conclure. □

## 4.3 Connexité semi-algébrique

**Définition 4.3.1.** Un ensemble semi-algébrique $S \subset \mathbf{R}^n$ est semi-algébriquement connexe si $S$ n'est pas l'union disjointe de deux ensembles semi-algébriques non vides qui sont ouverts dans $S$.

**Remarque 4.3.2.** Il est clair qu'un ensemble semi-algébrique qui est connexe (topologiquement) est également semi-algébriquement connexe. On peut cependant préciser que dans $\mathbb{R}^n$, les deux notions coïncident dans le cadre des ensembles semi-algébriques (voir [2, p. 35]).

Les deux résultats qui suivent nous seront utiles dans le chapitre 6. Nous les utiliserons pour montrer que les cellules d'une décomposition cylindrique algébrique sont semi-algébriquement connexes.

**Proposition 4.3.3.** *Soit $f : S \to \mathbf{R}^m$ une fonction semi-algébrique continue telle que $S$ est semi-algébriquement connexe. Alors $f(S)$ est semi-algébriquement connexe. De plus, le graphe de $f$ est également semi-algébriquement connexe.*

*Démonstration.* Par la proposition 4.2.7, on sait que $f(S)$ est semi-algébrique. Montrons désormais le caractère semi-algébriquement connexe. Pour ce faire, on procède par l'absurde. Supposons qu'il existe $A, B$ des ensembles semi-algébriques ouverts dans $f(S)$ non vides tels que $f(S) = A \cup B$ et $A \cap B = \emptyset$. Dès lors, $S = f^{-1}(A) \cup f^{-1}(B)$ et $f^{-1}(A) \cap f^{-1}(B) = \emptyset$. Or $f$ étant une application semi-algébrique continue, on en tire, par la proposition 4.2.7, que $f^{-1}(A)$ et $f^{-1}(B)$ sont des ensembles ouverts semi-algébriques et non vides. On en déduit que $S$ n'est pas semi-algébriquement connexe, une absurdité. Enfin, le graphe de $f$ est semi-algébriquement connexe car c'est l'image de l'application semi-algébrique continue $S \to S \times \mathbf{R}^m : x \mapsto (x, f(x))$. □

**Proposition 4.3.4.** *Soient $S$ un ensemble semi-algébriquement connexe et $f, g : S \to \mathbf{R}$ deux fonctions semi-algébriques continues telles que $f(x) < g(x)$ pour tout $x \in S$. Alors, l'ensemble*

$$C = \{(x, y) \in S \times \mathbf{R} : x \in S, f(x) < y < g(x)\},$$

*est semi-algébriquement connexe.*

*Démonstration.* L'ensemble $C$ est l'image de l'application semi-algébrique continue

$$h : S\times]0,1[\to \mathbf{R}^2 : (x,\lambda) \mapsto (x,(1-\lambda)f(x)+\lambda g(x)).$$

On peut montrer que $S\times]0,1[$ est semi-algébriquement connexe donc l'ensemble $C$ est semi-algébriquement connexe au vu de la proposition 4.3.3.

□

Le résultat suivant sera utile dans la démonstration de la proposition 6.2.6. On rappelle qu'une fonction $f : S \to R$ est localement constante si pour tout pour $x \in S$, il existe un ouvert $U \subset S$ tel que pour tout $y \in U$, $f(y) = f(x)$.

**Proposition 4.3.5.** *Si $S$ est un semi-algébriquement connexe et $f : S \to R$ est une fonction semi-algébrique localement constante, alors $f$ est constante.*

*Démonstration.* Soit $d \in f(S)$. Comme $f$ est localement constante, $f^{-1}(\{d\})$ est un ouvert. Si $f$ n'est pas constante, $f(S)\backslash\{d\}$ est non vide et $f^{-1}(f(S)\backslash\{d\})$ est également ouvert. On a $S = f^{-1}(\{d\}) \cup f^{-1}(f(S)\backslash\{d\})$. Ceci contredit le fait que $S$ est semi-algébriquement connexe car $f^{-1}(\{d\})$ et $f^{-1}(f(S)\backslash\{d\})$ sont non vides, ouverts dans $S$ et sont des ensembles semi-algébriques par la proposition 4.2.7. □

## 4.4 Théorème des fonctions implicites

On connaît bien le théorème des fonctions implicites dans $\mathbb{R}^n$. Ce théorème est également vérifié pour les fonctions semi-algébriques dans $\mathbf{R}^n$. Ce résultat est nécessaire dans le chapitre concernant la décomposition cylindrique algébrique dans la démonstration du lemme 6.2.4.

Remarquons cependant que la topologie dans les champs réels clos quelconques n'a pas les mêmes propriétés que la topologie euclidienne de $\mathbb{R}$. Par exemple, le théorème de Heine-Borel qui dit qu'un ensemble est fermé et borné dans $\mathbb{R}^n$ si et seulement s'il est compact n'est pas vrai en général.

**Exemple 4.4.1.** Considérons l'ensemble $[0,1]$ dans $\mathbb{R}_{alg}$ et les ensembles

$$\{[0,r[\,\cup\,]s,1] : 0 < r < \frac{\pi}{4} < s < 1\},$$

où $r, s \in \mathbb{R}_{alg}$. Ces ensembles définissent bien un recouvrement ouvert de $[0,1]$ dans $\mathbb{R}_{alg}$ étant donné que $\frac{\pi}{4} \notin \mathbb{R}_{alg}$. On ne peut pourtant pas en extraire de recouvrement fini. Donc $[0,1]$ est borné et fermé dans $\mathbb{R}_{alg}$, mais il n'est pas compact.

Cependant, on peut quand même prouver que toute fonction semi-algébrique continue sur un ensemble borné et fermé atteint un maximum et un minimum sur cet ensemble. C'est l'objet du théorème suivant, que nous allons admettre (voir [1, p. 93]).

**Théorème 4.4.2.** *Soit $S \subset \mathbf{R}^n$ un ensemble semi-algébrique fermé et borné et $g : S \to \mathbf{R}^m$ une fonction semi-algébrique continue définie sur $S$. Alors $g(S)$ est fermé et borné.*

Afin d'énoncer le théorème des fonctions implicites, il est nécessaire de définir les notions de limite, de continuité, de dérivation etc. Cependant, les notions de limite, de continuité et de dérivabilité sont les mêmes que dans $\mathbb{R}$. Il en va de même pour les notions de dérivées partielles, de différentielle, de matrice jacobienne et de jacobien pour les fonctions semi-algébriques multivariées. On récupère également les formules de dérivation classiques telles que la dérivation d'un produit ou d'une composée.

**Proposition 4.4.3.** *Soit $f : U \to \mathbf{R}$ une fonction semi-algébrique dérivable sur l'ensemble semi-algébrique ouvert $U \subseteq \mathbf{R}$ alors sa dérivée $f'$ est une fonction semi-algébrique définie sur $U$.*

*Démonstration.* La graphe de $f'$ est l'ensemble

$$\mathcal{G}(f') = \left\{ (x, y) \in U \times \mathbf{R} : \forall \epsilon > 0, \exists \delta > 0, \forall t \in \,]-\delta, \delta[\,, \left| y - \frac{f(x+t) - f(x)}{t} \right| < \epsilon \right\}.$$

Cet ensemble est bien semi-algébrique par la proposition 4.1.10. □

**Définition 4.4.4.** Soit $U \subset \mathbf{R}^n$ un ensemble semi-algébrique ouvert et $V \subset \mathbf{R}^m$ un ensemble semi-algébrique. L'ensemble des fonctions semi-algébriques de $U$ dans $V$ pour lesquelles toutes les dérivées partielles, jusqu'à l'ordre $l$, existent et sont continues est noté $\mathcal{S}^l(U, V)$.

Afin de démontrer le théorème des fonctions implicites, on utilise le théorème de la fonction inverse. Pour ce faire, nous avons besoin du résultat suivant, ainsi que de la définition qui suit.

**Définition 4.4.5.** Soit $F : \mathbf{R}^n \to \mathbf{R}^m$ une application linéaire. On définit sa norme par

$$\|F\| = \sup\{|F(x)| : |x| = 1\}.$$

Cette définition est bien posée au vu du théorème 4.4.2, et puisqu'une application linéaire est semi-algébrique, car son graphe est défini par des équations polynomiales (linéaires).

**Proposition 4.4.6.** *Soient $x, y \in \mathbf{R}^n$, $U$ un ouvert semi-algébrique contenant le segment $[x, y]$ et $f \in \mathcal{S}^1(U, \mathbf{R}^l)$. Alors*

$$|f(x) - f(y)| \leq M|x - y|$$

*où $M = \max\{\|d_z f\| : z \in [x, y]\}$.*

*Démonstration.* Remarquons tout d'abord que le nombre $M$ de l'énoncé est bien défini par le théorème 4.4.2. Définissons

$$g : [0, 1] \subset \mathbf{R} \to \mathbf{R}^l : t \mapsto f((1-t)x + ty).$$

Dès lors, on a $g'(t) = d_z f(y-x)$ avec $z = ((1-t)x + ty)$ et donc

$$|g'(t)| \leq M|y-x|.$$

Pour tout $c > 0$, l'ensemble

$$A_c = \{t \in [0,1] : |g(t) - g(0)| \leq M|x-y|t + ct\}$$

est semi-algébrique et contient 0. Soit $c > 0$ et $[0, t_0]$ un intervalle maximal inclus dans $A_c$. Supposons que $t_0 < 1$. On a d'une part, puisque $t_0$ est dans $A_c$ :

$$|g(t_0) - g(0)| \leq M|x-y|t_0 + ct_0.$$

D'autre part, comme $|g'(t_0)| \leq M|x-y|$, par définition de $g'(t_0)$, il existe $r > 0$ tel que si $t_0 < t < t_0 + r$ on a

$$|g(t) - g(t_0)| \leq M|x-y|(t-t_0) + c(t-t_0).$$

En sommant ces deux inégalités, et par inégalité triangulaire, on trouve que

$$|g(t) - g(0)| \leq M|x-y|t + ct,$$

pour $t_0 < t < t_0 + r$, ce qui contredit le fait que $t_0$ est maximal. On en déduit que $t_0 = 1$, et ce pour tout $c > 0$. Dès lors, $1 \in A_c$ pour tout $c > 0$. Donc

$$|f(y) - f(x)| = |g(1) - g(0)| \leq M|x-y| + c,$$

pour tout $c > 0$, et finalement $|f(y) - f(x)| \leq M|x-y|$. □

**Théorème 4.4.7.** *(Théorème de la fonction inverse) Soit $U'$ un voisinage semi-algébrique ouvert de $0 \in \mathbf{R}^n$ et $f \in \mathcal{S}^l(U', \mathbf{R}^n)$, $l \geq 1$ tel que $f(0) = 0$ et $d_0 f : \mathbf{R}^n \to \mathbf{R}^n$ est inversible. Alors il existe des voisinages ouverts semi-algébriques $U, V$ de 0 dans $\mathbf{R}^n$ tels que $U \subset U'$ et $f_{|U}$ est un homéomorphisme sur $V$ et $(f_{|U})^{-1} \in \mathcal{S}^l(V, U)$.*

Dans la preuve qui suit, nous n'allons pas démontrer le caractère $\mathcal{S}^l$ de la fonction. La preuve complète peut être trouvée dans [3, p. 207].

*Démonstration.* Quitte à composer $f$ avec $(d_0 f)^{-1}$, on peut supposer que $d_0 f = \mathrm{Id}$ de $\mathbf{R}^n$. Posons

$$g = f - \mathrm{Id}.$$

Dès lors, $d_0 g = 0$ donc il existe $r_1 \in \mathbf{R}$ tel que $\|d_x g\| \leq \frac{1}{2}$ si $x \in B_n(0, r_1)$, la boule ouverte de $\mathbf{R}^n$ de centre 0 et de rayon $r_1$. On peut bien sûr supposer que cette boule est incluse dans $U'$. Par la proposition 4.4.6, si $x, y \in B_n(0, r_1)$ alors on a

$$|g(x) - g(y)| \leq \frac{1}{2}|x-y|$$

et donc

$$|f(x) - f(y) - (x - y)| \leq \frac{1}{2}|x - y|.$$

Par l'inégalité triangulaire on obtient alors

$$\frac{1}{2}|x - y| \leq |f(x) - f(y)| \leq \frac{3}{2}|x - y|. \tag{4.1}$$

On en déduit que $f$ est injectif sur $B_n(0, r_1)$ : si $x, y$ sont dans cette boule et $f(x) = f(y)$, la première inégalité donne $x = y$.

De plus, comme $f \in \mathcal{S}^l$, et puisque $d_0 f$ est inversible, il existe $r_2 < r_1$ tel que $d_x f$ est inversible pour tout $x \in B_n(0, r_2)$.

On montre alors que l'image de $f(B_n(0, r_2))$ contient $B_n(0, \frac{r_2}{4})$. Considérons en effet $y_0 \in B_n(0, \frac{r_2}{4})$, et définissons

$$h : U' \to \mathbf{R} : x \mapsto |f(x) - y_0|^2.$$

Par le théorème 4.4.2, cette fonction atteint un minimum sur $\overline{B_n(0, r_2)}$. Or si $|x| = r_2$ on a $|f(x)| \geq \frac{r_2}{2}$ donc

$$h(x) > (\frac{r_2}{4})^2 > h(0).$$

On en déduit que ce minimum n'est pas atteint sur la frontière de la boule. Dès lors, il existe $x_0 \in B_n(0, r_2)$ qui minimise $h$. Donc, pour tout $i \in \{1, \ldots, n\}$ on a $\frac{\partial h}{\partial x_i}(x_0) = 0$, autrement dit, on a

$$\sum_{j=1}^{n} (f_j(x_0) - (y_0)_j) \frac{\partial f_j}{\partial x_i}(x_0) = 0,$$

or comme $d_x f$ est inversible, on a $f(x_0) = y_0$. On définit alors

$$V = B_n(0, \frac{r_2}{4}) \text{ et } U = f^{-1}(V) \cap B_n(0, r_2).$$

Alors la fonction $f$ est injective sur $U$ car $U \subset B_n(0, r_1)$ et $f|_U : U \to V$ est surjective par les développements précédents. La fonction $f^{-1}$ est continue car par (4.1)

$$|f^{-1}(x) - f^{-1}(y)| \leq 2|x - y|$$

pour tout $x, y \in V$. On peut alors montrer que $f^{-1}$ est de classe $\mathcal{S}^l$. □

Nous pouvons désormais démontrer le résultat qui nous intéresse. A savoir le théorème des fonctions implicites.

**Théorème 4.4.8.** *(Théorème des fonctions implicites) Soit $(x_0, y_0) \in \mathbf{R}^n \times \mathbf{R}^m$ et soient $f_1, \ldots, f_m$ des fonctions semi-algébriques de classe $\mathcal{S}^l$ sur un voisinage ouvert de $(x_0, y_0)$ tel que $f_j(x_0, y_0) = 0$ pour tout $j \in \{1, \ldots, m\}$ et tel que la matrice jacobienne de $f = (f_1, \ldots, f_m)$ en $(x_0, y_0)$ par rapport aux variables $y_1, \ldots, y_m$ est inversible. Alors il existe un voisinage ouvert semi-algébrique $U$ (resp. $V$) de $x_0$ (resp. $y_0$) dans $\mathbf{R}^n$ (resp. $\mathbf{R}^m$) et une fonction $\varphi \in \mathcal{S}^l(U, V)$ tel que $\varphi(x_0) = y_0$ et pour tout $(x, y) \in U \times V$, on a*

$$f_1(x, y) = \ldots = f_m(x, y) = 0 \Leftrightarrow y = \varphi(x).$$

*Démonstration.* Considérons l'application

$$\Phi : \mathbf{R}^n \times \mathbf{R}^m \to \mathbf{R}^n \times \mathbf{R}^m : (x, y) \mapsto (x, f(x, y)).$$

Quitte à définir $\tilde{f}(x, y) = f(x + x_0, y + y_0)$, on peut appliquer le théorème de la fonction inverse 4.4.7 à $\Phi$ et donc il existe des voisinages semi-algébriques ouverts $U', V' \subset \mathbf{R}^{n+m}$ de 0 et une application $\Psi : U' \to V'$ de classe $\mathcal{S}^l$ telle que

$$\Phi \circ \Psi = \mathrm{Id}_{U'} \text{ et } \Psi \circ \Phi = \mathrm{Id}_{V'}.$$

Cela implique que $\Psi$ prend la forme

$$\Psi : U' \to V' : (x, z) \mapsto (x, g(x, z)),$$

où $g$ est de classe $\mathcal{S}^l$. Considérons l'ensemble semi-algébrique ouvert $W = \{x \in \mathbf{R}^n : (x, 0) \in U'\}$ et définissons l'application de classe $\mathcal{S}^l$

$$\varphi : W \to \mathbf{R}^m : x \mapsto g(x, 0).$$

Soit $x \in W$, on a

$$(x, 0) = \Phi(\Psi(x, 0)) = \Phi(x, g(x, 0)) = \Phi(x, \varphi(x)) = (x, f(x, \varphi(x))),$$

on en déduit que $f(x, \varphi(x)) = 0$ pour tout $x \in W$. Réciproquement, si $f(x, y) = 0$ avec $(x, y) \in V'$, on a alors

$$(x, f(x, y)) = (x, 0),$$

et donc $(x, y) = \Psi(\Phi(x, y)) = \Psi(x, 0) = (x, g(x, 0)) = (x, \varphi(x))$. On en tire que $y = \varphi(x)$. □

# Chapitre 5

# Résultant et discriminant

Ce chapitre a pour but de continuer à donner des résultats préliminaires à la construction de la décomposition cylindrique algébrique. En effet, afin d'effectuer une décomposition cylindrique algébrique, nous avons besoin de conditions sur les degrés des pgcd des polynômes.

Nous allons commencer par définir le discriminant d'un polynôme de degré quelconque. Nous allons ensuite définir le résultant de deux polynômes, cette notion peut généraliser celle de discriminant. Ensuite, nous définissons les sous-résultants, qui généralisent à leur tour la notion de résultant. Ces différentes notions vont nous permettre d'obtenir des résultats concernant les polynômes et leurs pgcd.

Les résultats présents dans ce chapitre sont inspirés de [1, chap. 4]. Historiquement, la théorie du discriminant et des résultants a principalement été développée au 18$^{\text{e}}$ siècle et au 19$^{\text{e}}$ siècle, par de célèbres mathématiciens tels que le Leonhard Euler, Étienne Bézout et James Joseph Sylvester [1, p. 157].

Nous considérons $\mathbf{D}$ un anneau intègre et nous notons $\mathbf{K}$ son corps des fractions et $\mathbf{C}$ un champ algébriquement clos contenant $\mathbf{K}$. De plus, si $\mathbf{D}$ est ordonné alors on considère également un champ réel clos $\mathbf{R}$ tel que $\mathbf{D} \subset \mathbf{K} \subset \mathbf{R} \subset \mathbf{C}$.

## 5.1 Discriminant

Le discriminant est bien connu pour les équations algébriques de degré deux. Il s'exprime en fonction des coefficients du polynôme définissant l'équation et permet par exemple de déterminer si une telle équation admet une racine double. Il se généralise à tout degré, comme nous allons le voir. Nous suivons la définition utilisée dans [1].

**Définition 5.1.1.** Soit $P \in \mathbf{R}[X]$ un polynôme monique de degré $p$,

$$P = X^p + a_{p-1}X^{p-1} + \ldots + a_1X + a_0,$$

et soient $x_1, \ldots, x_p$ les racines, comptées autant de fois que leur multiplicité, de $P$ dans $\mathbf{C}$. Le discriminant de $P$ est

$$\text{Disc}(P) = \prod_{1 \leq i < j \leq p} (x_i - x_j)^2.$$

On peut étendre la définition aux polynômes non moniques en multipliant le résultat par $a_p^{2p-2}$, ou $a_p$ est le coefficient du terme de plus haut degré $(p)$ de $P$.

Notons que nous définissons le discriminant pour les polynômes à coefficients dans un champ réel clos $\mathbf{R}$. Cependant, si on considère un polynôme $P \in \mathbf{D}[X_1, \ldots, X_n]$ où $\mathbf{D}$ est un anneau intègre ordonné alors, au vu de l'exemple 2.1.4, $D' = D[X_1, \ldots, X_{n-1}]$ est également un anneau intègre ordonné. On peut alors considérer son corps des fractions $\mathbf{K}'$ qui est un champ réel (généraliser l'exemple 2.1.5). Au vu du théorème 2.2.6, on peut alors le plonger dans sa clôture réelle $\mathbf{R}'$. Finalement, tout polynôme de $\mathbf{D}[X_1, \ldots, X_n]$ peut être vu en un élément de $\mathbf{R}'[X_n]$ où $\mathbf{R}'$ est un champ réel clos.

**Remarque 5.1.2.** Au vu de la proposition 1.3.14, on tire que $\mathrm{Disc}(P) \in \mathbf{R}$ pour tout $P \in \mathbf{R}[X]$.

**Proposition 5.1.3.** *Le discriminant de $P$ est nul si et seulement si* $\deg(\mathrm{pgcd}(P, P')) > 0$ *où $P'$ est la dérivée de $P$.*

*Démonstration.* Par définition de $\mathrm{Disc}(P)$, il est clair que $\mathrm{Disc}(P) = 0$ si et seulement si $P$ a une racine multiple dans $\mathbf{C}$. Autrement dit, que $\deg(\mathrm{pgcd}(P, P')) > 0$. □

**Remarque 5.1.4.** Considérons le polynôme du second degré

$$P = aX^2 + bX + c,\ a \neq 0.$$

Les racines de $P$ sont alors

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Donc

$$\mathrm{Disc}(P) = a^2(x_1 - x_2)^2 = b^2 - 4ac.$$

On retombe alors sur la formule bien connue du discriminant $\Delta = b^2 - 4ac$.

**Exemple 5.1.5.** Considérons le polynôme $P$ de $\mathbb{R}[X]$ défini par

$$P = 2X^3 - X^2 + 2X - 1 = 2(X - i)(X + i)(X - \frac{1}{2}).$$

On a alors $\mathrm{Disc}(P) = 2^4(i - (-i))^2(i - \frac{1}{2})^2(-i - \frac{1}{2})^2 = -100$.

**Exemple 5.1.6.** Considérons le polynôme de $\mathbb{R}[Y]$ où $x \in \mathbb{R}$,

$$P_1 = Y^2 + x^2 - 3.$$

Les racines de ce polynôme sont $\pm\sqrt{3 - x^2}$. On en déduit que $\mathrm{Disc}(P_1) = (-\sqrt{3 - x^2} - \sqrt{3 - x^2})^2 = -4(x^2 - 3)$. Dès lors, $x^2 - 3 = 0$ si et seulement si $\deg(\mathrm{pgcd}(P_1, P_1')) > 0$, ce qui est bien le cas étant donné que $P_1' = 2Y$ s'annule uniquement en $y = 0$.

## 5.2 Résultant

Nous allons maintenant introduire la notion de résultant de deux polynômes. Cette notion est liée à celle de discriminant car nous allons voir le résultant de $P$ et de $P'$ est proportionnel à $\mathrm{Disc}(P)$, lorsque $P$ est un polynôme à coefficients dans un champ. En particulier $\mathrm{Res}(P, P') = 0 \Leftrightarrow \mathrm{Disc}(P) = 0$.

**Définition 5.2.1.** Soient $P, Q$ deux polynômes de $\mathbf{D}[X]$ de degrés respectifs $p$ et $q$. On définit l'application

$$f_{(P,Q)} : \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X] \to \mathbf{K}_{p+q-1}[X] : (U, V) \mapsto UP + VQ, \tag{5.1}$$

où $\mathbf{K}$ est le corps des fractions de $\mathbf{D}$.

**Proposition 5.2.2.** *L'application $f_{(P,Q)}$ est linéaire. De plus, si*

$$P = a_p X^p + \ldots + a_0 \text{ et } Q = b_q X^q + \ldots + b_0.$$

*Alors dans les bases*

$$((X^{q-1}, 0), \ldots, (1, 0), (0, X^{p-1}), \ldots, (0, 1)),$$

*de $\mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$, et*

$$(X^{q+p-1}, \ldots, X, 1),$$

*de $\mathbf{K}_{p+q-1}[X]$, cette application se représente par la matrice*

$$\begin{pmatrix}
a_p & 0 & \ldots & 0 & b_q & 0 & \ldots & 0 \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\
\vdots & & & a_p & \vdots & & & b_q \\
a_0 & & & \vdots & b_0 & & & \vdots \\
0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & \ldots & 0 & a_0 & 0 & \ldots & 0 & b_0
\end{pmatrix}.$$

*Démonstration.* Montrons la linéarité, soient $(U, V), (U', V') \in \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$ et soient $\lambda, \mu \in \mathbf{K}$. On a

$$\begin{aligned}
f_{(P,Q)}(\lambda(U, V) + \mu(U', V')) &= f_{(P,Q)}((\lambda U + \mu U', \lambda V + \mu V')) \\
&= (\lambda U + \mu U')P + (\lambda V + \mu V')Q \\
&= \lambda(UP + VQ) + \mu(U'P + V'Q) \\
&= \lambda f_{(P,Q)}((U, V)) + \mu f_{(P,Q)}((U', V')).
\end{aligned}$$

Pour trouver sa représentation matricielle, on calcule l'image des éléments de la base de $\mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$ et on en prend les composantes dans la base de $\mathbf{K}_{p+q-1}[X]$. On a alors

$$\begin{aligned} f_{(P,Q)}((X^{q-1},0)) &= PX^{q-1} = (a_p,\dots,a_0,0,\dots,0),\\ &\vdots\\ f_{(P,Q)}((1,0)) &= P = (0,\dots,0,a_p,\dots,a_0),\\ f_{(P,Q)}((0,X^{p-1})) &= X^{p-1}Q = (b_q,\dots,q_0,0,\dots,0),\\ &\vdots\\ f_{(P,Q)}((0,1)) &= Q = (0,\dots,0,b_q,\dots,q_0). \end{aligned}$$

Ces vecteurs de composantes sont les colonnes de la matrice qui représente l'application linéaire dans ces bases. □

**Définition 5.2.3.** Soient $P, Q$ deux polynômes de $\mathbf{D}[X]$ de degrés respectifs $p$ et $q$. La matrice de Sylvester associée à $P$ et $Q$ est la matrice carrée de dimension $(p+q)\times(p+q)$ suivante :

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a_p & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & 0\\ 0 & \ddots & & & & & \ddots & \ddots & \vdots\\ \vdots & \ddots & \ddots & & & & & \ddots & 0\\ 0 & \dots & 0 & a_p & \dots & \dots & \dots & \dots & a_0\\ b_q & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & 0\\ 0 & \ddots & & & & \ddots & \ddots & & \vdots\\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots\\ \vdots & & \ddots & \ddots & & & & \ddots & 0\\ 0 & \dots & \dots & 0 & b_q & \dots & \dots & \dots & b_0 \end{pmatrix}.$$

Cette matrice est définie comme étant la transposée de la matrice qui représente l'application $f_{(P,Q)}$ (5.1) définie ci-dessus. Le résultant de $P$ et $Q$, noté $\mathrm{Res}(P,Q)$ est le déterminant de $\mathrm{Syl}(P,Q)$.

**Exemple 5.2.4.** Reprenons le polynôme de l'exemple 5.1.6 et considérons un autre polynôme $P_2$. On a

$$P_1 = Y^2 + x^2 - 3 \text{ et } P_2 = xY - 1,$$

avec $x \in \mathbb{R}_0$. Dès lors,

$$\mathrm{Syl}(P_1,P_2) = \begin{pmatrix} 1 & 0 & x^2-3\\ x & -1 & 0\\ 0 & x & -1 \end{pmatrix}.$$

On obtient alors

$$\mathrm{Res}(P_1,P_2) = \det(\mathrm{Syl}(P_1,P_2)) = x^4 - 3x^2 + 1.$$

**Lemme 5.2.5.** *Soient* $\mathbf{D}$ *un anneau intègre et* $P, Q \in \mathbf{D}[X]$ *des polynômes de degrés respectifs* $p$ *et* $q$*. On a* $\mathrm{Res}(P,Q) = 0$ *si et seulement si il existe deux polynômes non nuls* $U \in \mathbf{K}[X]$ *et* $V \in \mathbf{K}[X]$ *avec* $\deg(U) < q$ *et* $\deg(V) < p$ *tels que* $UP + VQ = 0$*.*

*Démonstration.* Il existe de tels $U, V$ si et seulement si l'application $f_{(P,Q)}$, ou de manière équivalente la matrice qui la représente, n'est pas inversible. Cela arrive exactement quand son déterminant est nul. Cette matrice étant la transposée de la matrice de Sylvester, c'est enfin équivalent à $\mathrm{Res}(P,Q) = 0$. □

**Proposition 5.2.6.** *Soient* $\mathbf{D}$ *est un anneau intègre et* $P, Q \in \mathbf{D}[X]$ *des polynômes de degrés respectifs* $p$ *et* $q$*. Alors* $\mathrm{Res}(P,Q) = 0$ *si et seulement si* $P$ *et* $Q$ *ont un facteur commun dans* $\mathbf{K}[X]$*.*

*Démonstration.* Par le lemme précédent, $\mathrm{Res}(P,Q) = 0$ si et seulement si il existe $U, V \in \mathbf{K}[X]$ des polynômes tels que $\deg(U) < q$, $\deg(V) < p$ et $UP + VQ = 0$. Dès lors, on a $UP = -VQ$. Si la décomposition en facteurs premiers de $Q$ dans $\mathbf{K}[X]$ est donnée par

$$Q = q_1 \dots q_n,$$

alors on a

$$UP = -V q_1 \dots q_n.$$

Or $\deg(U) < q$, donc il existe $i \leq n$ tel que $q_i$ divise $P$ et $q_i$ est donc également un facteur premier de $P$.
Réciproquement, si il existe $q \in \mathbf{K}[X]$ tel que $\deg(q) \geq 1$ et $P = qP_0$ et $Q = qQ_0$ alors on considère

$$U = Q_0 \text{ et } V = -P_0.$$

On a alors $\deg(U) < q$ et $\deg(V) < p$ et $UP + VQ = qQ_0P_0 - qP_0Q_0 = 0$. □

**Exemple 5.2.7.** Considérons les polynômes de $\mathbb{Z}[X]$

$$Q = X^2 + 1 \text{ et } P = X^3 - X^2 + X - 1 = (X-1)Q.$$

On a

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} 1 & -1 & 1 & -1 & 0 \\ 0 & 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix},$$

on trouve alors

$$\mathrm{Res}(P,Q) = 0.$$

Dans cet exemple, le facteur en commun est $(X^2 + 1)$.

**Exemple 5.2.8.** Au vu de l'exemple 5.2.4, on en déduit que les polynômes

$$P = Y^2 + x^2 - 3 \text{ et } Q = xY - 1,$$

ont une racine commune si et seulement si $x^4 - 3x^2 + 1 = 0$.

**Remarque 5.2.9.** Si $Q$ est un polynôme constant $b$ et $P$ un polynôme de degré $p$, on a $\mathrm{Res}(P,Q) = b^p$ car

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} b & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & b \end{pmatrix}.$$

**Lemme 5.2.10.** *Soient $P, Q \in \mathbf{D}[X]$ deux polynômes qui se décomposent dans $\mathbf{C}[X]$ en*

$$P = a_p \prod_{i=1}^{p} (X - x_i) \text{ et } Q = b_q \prod_{j=1}^{q} (X - y_j),$$

*avec $p > q$ et $x_1, \dots, x_p, y_1, \dots, y_q \in \mathbf{C}$ les racines (comptées avec leur multiplicité) de $P$ et de $Q$. Si on pose*

$$\Theta(P,Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (x_i - y_j),$$

*alors on a*

$$\Theta(P,Q) = (-1)^{pq} b_q^{p-r} \Theta(Q,R),$$
$$\mathrm{Res}(P,Q) = (-1)^{pq} b_q^{p-r} \mathrm{Res}(Q,R).$$

*où $R$ est le reste de la division euclidienne de $P$ par $Q$ avec* $\deg(R) = r$.

*Démonstration.* En effectuant la division euclidienne de $P$ par $Q$, on obtient un polynôme $S \in \mathbf{K}[X]$ de degré $p - q$ tel que $P = QS + R$. Notons

$$R = \sum_{i=0}^{r} c_i X^i,$$

et

$$S = \sum_{i=0}^{p-q} s_i X^i.$$

On a alors

$$R = P - \sum_{i=0}^{p-q} s_i X^i Q.$$

Considérons la matrice $\mathrm{Syl}(Q,R)$ de dimension $(q+r) \times (q+r)$ dont les rangées sont les composantes de

$$X^{r-1}Q, \dots, Q, X^{q-1}R, \dots, R,$$

dans la base $\{X^{q+r-1}, \dots, X, 1\}$, et étendons la de sorte à avoir une matrice de dimension $(p+q) \times (p+q)$ telle que les rangées soient les composantes de

$$X^{p-1}Q, \dots, X^{r-1}Q, \dots, Q, X^{q-1}R, \dots, R,$$

dans la base $\{X^{p+q-1}, \dots, X, 1\}$ et appelons cette matrice $N$. C'est alors la matrice suivante :

$$N = \begin{pmatrix} b_q & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_q & \dots & \dots & \dots & b_0 \\ 0 & \dots & 0 & c_r & \dots & c_0 & 0 & \dots & 0 \\ \vdots & & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & c_r & \dots & c_0 \end{pmatrix}.$$

Dès lors, en calculant le déterminant de cette matrice, via la règle des mineurs sur les $p-r$ premières colonnes, on obtient

$$\det(N) = b_q^{p-r} \mathrm{Res}(Q, R).$$

Or la matrice $N$ est la matrice $\mathrm{Syl}(P, Q)$ où on a permuté les rangées contenant les coefficients du polynôme $Q$ avec celles contenant ceux de $P$ et où on a ensuite remplacé les rangées $X^{q-1}P, \dots, P$ par $X^{q-1}R, \dots, R$. On a alors

$$\det(N) = (-1)^{pq} \mathrm{Res}(P, Q).$$

En effet, le facteur $(-1)^{pq}$ étant issu des permutations de rangées, et le $\mathrm{Res}(P, Q)$ est issu du fait que le déterminant d'une matrice reste inchangé lorsqu'on ajoute à la matrice des combinaisons linéaires de ses rangées. Dès lors, on obtient que

$$\mathrm{Res}(P, Q) = (-1)^{pq} b_q^{p-r} \mathrm{Res}(Q, R).$$

Ensuite pour toute racine $y_j$ de $Q$, étant donné que $Q(y_j) = 0$, on a

$$P(y_j) = R(y_j).$$

De plus, par définition de $\Theta$, on a

$$\Theta(P, Q) = a_p^q \prod_{i=1}^{p} Q(x_i) = (-1)^{pq} b_q^p \prod_{j=1}^{q} P(y_j),$$

donc

$$\begin{aligned} \Theta(P, Q) &= (-1)^{pq} b_q^p \prod_{j=1}^{q} P(y_j) \\ &= (-1)^{pq} b_q^p \prod_{j=1}^{q} R(y_j) \\ &= (-1)^{pq} b_q^{p-r} \Theta(Q, R), \end{aligned}$$

toujours en utilisant la définition de $\Theta$. Finalement, on trouve donc que

$$\Theta(P,Q) = (-1)^{pq} b_q^{p-r} \Theta(Q,R),$$
$$\mathrm{Res}(P,Q) = (-1)^{pq} b_q^{p-r} \mathrm{Res}(Q,R).$$

□

**Théorème 5.2.11.** *Soient $P, Q \in \mathbf{D}[X]$ tels qu'on a*

$$P = a_p \prod_{i=1}^{p} (X - x_i) \text{ et } Q = b_q \prod_{j=1}^{q} (X - y_j),$$

*où $p > q$ et $x_1, \ldots, x_p, y_1, \ldots, y_q \in \mathbf{C}$ sont les racines (comptées avec leur multiplicité) de $P$ et de $Q$. On a alors*

$$\mathrm{Res}(P,Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (x_i - y_j).$$

*Démonstration.* Montrons que $\Theta(P,Q) = \mathrm{Res}(P,Q)$. Il est clair que si $P$ et $Q$ ont une racine en commun dans $\mathbf{C}$, on a

$$\mathrm{Res}(P,Q) = \Theta(P,Q) = 0.$$

Supposons alors que $P$ et $Q$ sont premiers entre eux et que la longueur de la suite de restes de $P$ et $Q$ est $n$. On a alors (en considérant $R_{-1} = P$ et $R_0 = Q$),

$$\begin{aligned} P &= D_1 Q + R_1, \\ Q &= D_2 R_1 + R_2, \\ R_1 &= D_3 R_2 + R_3, \\ &\vdots \\ R_{n-2} &= D_n R_{n-1} + R_n, \\ R_{n-1} &= D_{n+1} R_n. \end{aligned}$$

En appliquant $n$ fois le lemme 5.2.10, on voit qu'il suffit de vérifier que

$$\mathrm{Res}(R_{n-1}, R_n) = \Theta(R_{n-1}, R_n).$$

Or, $R_n = \mathrm{pgcd}(P,Q)$ et donc $\deg(R_n) = 0$. Si on a $R_n = k \in \mathbf{K}_0$, alors

$$\mathrm{Res}(R_{n-1}, R_n) = k^{\deg(R_{n-1})} = \Theta(R_{n-1}, R_n).$$

□

**Corollaire 5.2.12.** *Soit $P \in \mathbf{R}[X]$ tel que*

$$P = a_p X^p + \ldots + a_1 X + a_0,$$

*avec $p > 1$ et $a_p \neq 0$. On a alors*

$$\mathrm{Res}(P, P') = (-1)^{\frac{p(p-1)}{2}} a_p \mathrm{Disc}(P).$$

*En particulier,* $\mathrm{Res}(P, P') = 0$ *si et seulement si* $\mathrm{Disc}(P) = 0$.

*Démonstration.* Notons $x_1, \ldots, x_p$ (resp. $y_1, \ldots, y_{p-1}$) les racines de $P$ (resp. $P'$) dans $\mathbf{C}$ comptées avec leur multiplicité. Par le théorème 5.2.11, on a

$$\mathrm{Res}(P, P') = a_p^{p-1}(pa_p)^p \prod_{i=1}^{p} \prod_{j=1}^{p-1} (x_i - y_j) = a_p^{p-1} \prod_{i=1}^{p} P'(x_i),$$

car pour tout $i \in \{1, \ldots, p\}$, on a

$$P'(x_i) = pa_p \prod_{j=1}^{p-1} (x_i - y_j).$$

De plus, au vu de la formule de Leibniz, on a

$$P' = a_p \sum_{i=1}^{p} \prod_{\substack{1 \leq j \leq p \\ j \neq i}} (X - x_j).$$

Dès lors, en évaluant $P'$ en $x_i$ pour $i \in \{1, \ldots, p\}$, on a

$$P'(x_i) = a_p \prod_{\substack{1 \leq j \leq p \\ j \neq i}} (x_i - x_j).$$

Donc on a

$$\prod_{i=1}^{p} P'(x_i) = \prod_{i=1}^{p} a_p \prod_{\substack{1 \leq j \leq p \\ j \neq i}} (x_i - x_j) = (-1)^{\frac{p(p-1)}{2}} a_p^p \prod_{1 \leq i < j \leq p} (x_i - x_j)^2.$$

Au vu de la définition 5.1.1, on en déduit alors que

$$\mathrm{Res}(P, P') = (-1)^{\frac{p(p-1)}{2}} a_p \mathrm{Disc}(P).$$

□

Cette relation peut être utilisée afin de définir le discriminant d'un polynôme à partir du résultant. C'est d'ailleurs une définition assez courante. En effet, en pratique, on peut toujours calculer le résultant de deux polynômes, alors que pour calculer le discriminant d'un polynôme, au vu de sa définition, il faut connaître toutes ses racines. Pour calculer le discriminant d'un polynôme donné on peut alors calculer le résultant de ce polynôme avec sa dérivée et utiliser le corollaire 5.2.12. Ce résultat suggère comment étendre la définition du discriminant pour des polynômes à coefficients dans un anneau intègre $\mathbf{D}$.

**Exemple 5.2.13.** On peut déterminer le discriminant d'un polynôme de la forme

$$P = aX^3 + bX^2 + cX + d.$$

En effet, on a

$$P' = 3aX^2 + 2bX + c,$$

et donc la matrice de Sylvester associée est la matrice

$$\mathrm{Syl}(P, P') = \begin{pmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{pmatrix}.$$

Après un calcul de déterminant qu'on ne détaille pas ici, on trouve que

$$\mathrm{Res}(P, P') = a(-18abcd + a(27ad^2 + 4c^3) + 4b^3d - b^2c^2.$$

La formule du corollaire 5.2.12 nous dit que

$$\mathrm{Res}(P, P') = -a\mathrm{Disc}(P),$$

on en déduit que la formule pour calculer le discriminant d'un polynôme de degré 3 est

$$\mathrm{Disc}(P) = 18abcd - a(27ad^2 + 4c^3) - 4b^3d + b^2c^2.$$

Notons qu'en général, une équation du troisième degré peut se ramener à $X^3 + pX + q = 0$. Dans ce cas, le discriminant du polynôme en question vaut $-27q^2 - 4p^3$.

Nous allons montrer qu'on peut obtenir le résultant de deux polynômes au moyen d'une combinaison de ces polynômes. Regardons cela dans l'exemple qui suit.

**Exemple 5.2.14.** Considérons les polynômes $P, Q \in \mathbf{D}[X]$

$$P = aX^2 + bX + c \text{ et } Q = dX + e,$$

avec $a, b, c, d, e \in \mathbf{D}$. Notons $\mathrm{Syl}(P,Q)^*$ la matrice de Sylvester de $P$ et $Q$ où on a remplacé les éléments de la dernière colonne par les polynômes $P, XQ$ et $Q$ respectivement. On a alors

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a & b & c \\ d & e & 0 \\ 0 & d & e \end{pmatrix}, \mathrm{Syl}(P,Q)^* = \begin{pmatrix} a & b & aX^2+bX+c \\ d & e & dX^2+eX \\ 0 & d & dX+e \end{pmatrix}.$$

D'une part, par linéarité du déterminant, on a

$$\det(\mathrm{Syl}(P,Q)^*) = \begin{vmatrix} a & b & c \\ d & e & 0 \\ 0 & d & e \end{vmatrix} + \begin{vmatrix} a & b & b \\ d & e & e \\ 0 & d & d \end{vmatrix} X + \begin{vmatrix} a & b & a \\ d & e & d \\ 0 & d & 0 \end{vmatrix} X^2.$$

Comme les deux derniers déterminants sont nuls, on remarque alors que

$$\det(\mathrm{Syl}(P,Q)^*) = \det(\mathrm{Syl}(P,Q)) = \mathrm{Res}(P,Q).$$

D'autre part, on a

$$\det(\mathrm{Syl}(P,Q)^*) = (aX^2+bX+c)d^2 - (dX^2+eX)(ad) + (dX+e)(ae-bd).$$

On en déduit que

$$\mathrm{Res}(P,Q) = d^2P + (-adX + ae - bd)Q.$$

En développant, on trouve que $\mathrm{Res}(P,Q) = d^2c + ae^2 - bde$.

Ce résultat se généralise à n'importe quels polynômes $P$ et $Q$. C'est ce que nous dit la proposition suivante.

**Proposition 5.2.15.** *Soient $P, Q \in \mathbf{D}[X]$, il existe $U, V \in \mathbf{D}[X]$ tel que $\deg(U) < q$, $\deg(V) < p$ et $\mathrm{Res}(P,Q) = UP + VQ$.*

*Démonstration.* Notons $\mathrm{Syl}(P,Q)^*$ la matrice $\mathrm{Syl}(P,Q)$ où on a remplacé la dernière colonne par les polynômes $X^{q-1}P, \ldots, P, X^{p-1}Q, \ldots, Q$. Dès lors, par linéarité du déterminant sur la dernière colonne, on a

$$\det(\mathrm{Syl}(P,Q)^*) = \det(\mathrm{Syl}(P,Q)) + \sum_{j=1}^{p+q-1} d_j X^j,$$

où $d_j$ est le déterminant de $\mathrm{Syl}(P,Q)$ où on a remplacé la dernière colonne de la matrice par sa j-ième colonne. On en déduit donc que $d_j = 0$ pour tout $j \in \{1, \ldots, p+q-1\}$. Et donc,

$$\det(\mathrm{Syl}(P,Q)^*) = \det(\mathrm{Syl}(P,Q)) = \mathrm{Res}(P,Q).$$

Or en développant le déterminant de $\mathrm{Syl}(P,Q)^*$ via sa dernière colonne, on obtient les polynômes $U$ et $V$ recherchés. □

Terminons cette section sur les résultants par un résultat qui lie la matrice de Sylvester et son déterminant, le résultant, à la matrice jacobienne et au jacobien d'une application naturelle. Nous avons défini un polynôme comme une suite de coefficients, mais on peut le voir comme une application particulière. Si on le voit de telle façon, à un polynôme monique de degré $n$, on associe une suite de $n+1$ coefficients débutant par 1. Si on s'en tient strictement à la définition, cette application est l'identité. On remarque ensuite que le coefficient 1 n'apporte aucune information. On introduit une notation pour clarifier ces points de vue.

**Définition 5.2.16.** Pour tout $n \in \mathbb{N}_0$, on définit l'application suivante :

$$\mathrm{poly}_n : \mathbf{C}^n \to \mathbf{C}_n[X] : (a_{n-1}, \ldots, a_0) \mapsto P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0.$$

Cette application définit une bijection entre les polynômes moniques de degré $n \geq 1$ à coefficients dans $\mathbf{C}$ et les éléments de $\mathbf{C}^n$.

**Définition 5.2.17.** Pour tout $n \in \mathbb{N}$ et $p_1, \ldots, p_n \in \mathbb{N}_0$, on définit l'application suivante :

$$m : \mathbf{C}^{p_1} \times \ldots \times \mathbf{C}^{p_n} \to \mathbf{C}^{p_1+\ldots+p_n} : (u_1, \ldots, u_n) \mapsto \mathrm{poly}^{-1}_{p_1+\ldots+p_n}(\mathrm{poly}_{p_1}(u_1) \ldots \mathrm{poly}_{p_n}(u_n)).$$

L'application $m$ est la multiplication de polynômes vue en coordonnées.

**Exemple 5.2.18.** Considérons l'exemple où $(0, -2, 3) \in \mathbb{C}^3$ et $(-1) \in \mathbb{C}$. On a

$$\mathrm{poly}_3((0, -2, 3)) = X^3 - 2X + 3 \text{ et } \mathrm{poly}_1((-1)) = X - 1.$$

Le produit de ces deux polynômes est le polynôme

$$R = X^4 - X^3 - 2X^2 + 5X - 3 \in \mathbb{C}_4[X],$$

et on a $\mathrm{poly}_4^{-1}(R) = (-1, -2, 5, -3)$. Dès lors,

$$m((0, -2, 3), (-1)) = (-1, -2, 5, -3).$$

**Proposition 5.2.19.** *La matrice jacobienne de $m$ en $(P, Q)$ est la transposée de la matrice de Sylvester de $P$ et $Q$ et le jacobien de $m$ en $(P, Q)$ est leur résultant de $P$ et de $Q$.*

*Démonstration.* Avec

$$P = X^p + a_{p-1}X^{p-1} + \ldots + a_1X + a_0 = \mathrm{poly}_p(a_{p-1}, \ldots, a_0),$$

et

$$Q = X^q + b_{q-1}X^{q-1} + \ldots + b_1X + b_0 = \mathrm{poly}_q(b_{q-1}, \ldots, b_0).$$

On a

$$m((b_{q-1}, \ldots, b_0), (a_{p-1}, \ldots, a_0)) = (m_{p+q-1}, \ldots, m_0),$$

avec

$$m_j = \sum_{q-i+p-k=j} b_{q-i}a_{p-k},$$

pour tout $j \in \{0, \ldots, p+q-1\}$. Donc la matrice jacobienne de $m$ est

$$J_m = \begin{pmatrix} \frac{\partial m_{p+q-1}}{\partial b_{q-1}} & \cdots & \frac{\partial m_{p+q-1}}{\partial a_0} \\ \vdots & \ddots & \vdots \\ \frac{\partial m_0}{\partial b_{q-1}} & \cdots & \frac{\partial m_0}{\partial a_0} \end{pmatrix}.$$

Ce qui nous donne la transposée de la matrice de Sylvester. □

## 5.3 Sous-résultants

Nous allons généraliser la notion de résultant en définissant les sous-résultants. Commençons par la généralisation de la définition 5.2.1.

**Définition 5.3.1.** Soient $P, Q$ deux polynômes de $\mathbf{D}[X]$ de degrés $p$ et $q$ tel que $p > q$. Pour tout $0 \leq j \leq q$, on considère l'application

$$f_{j(P,Q)} : \mathbf{K}_{q-j-1}[X] \times \mathbf{K}_{p-j-1}[X] \to \mathbf{K}_{p+q-j-1}[X] : (U, V) \mapsto UP + VQ.$$

Remarquons que si $j = q$ on considère $\mathbf{K}_{q-j-1}[X] = \mathbf{K}_{-1}[X] = \{0\}$.

De plus, pour $j = 0$, l'application $f_{0(P,Q)}$ est égale à l'application $f_{(P,Q)}$ de la définition 5.2.1, au détail près qu'ici on suppose que $p > q$, cette hypothèse est utile dans la démonstration 5.3.9. La proposition suivante est analogue à la proposition 5.2.2.

**Proposition 5.3.2.** *L'application $f_{j(P,Q)}$ est une application linéaire. De plus, si*

$$P = a_pX^p + \ldots + a_1X + a_0,$$

*et*

$$Q = b_qX^q + \ldots + b_1X + b_0,$$

*alors son expression dans la base*

$$((X^{q-j-1}, 0), \ldots, (1, 0), (0, X^{p-j-1}), \ldots, (0, 1)),$$

*de $\mathbf{K}_{q-j-1}[X] \times \mathbf{K}_{p-j-1}[X]$ et dans la base*

$$(X^{p+q-j-1}, \ldots, X, 1),$$

*de* $\mathbf{K}_{p+q-j-1}[X]$*, est la matrice*

$$\begin{pmatrix} a_p & 0 & \dots & 0 & b_q & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & & & a_p & \vdots & & & b_q \\ a_0 & & & \vdots & b_0 & & & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_0 & 0 & \dots & 0 & b_0 \end{pmatrix}.$$

*Démonstration.* Soit $0 \leq j \leq q$, l'application $f_{j(P,Q)}$ est bien une application linéaire. En effet, soient $\lambda, \mu \in \mathbf{K}$ et soient $(U, V), (U', V') \in \mathbf{K}_{q-j-1}[X] \times \mathbf{K}_{p-j-1}[X]$.On a

$$\begin{aligned} f_{j(P,Q)}(\lambda(U,V) + \mu(U',V')) &= f_{j(P,Q)}((\lambda U + \mu U', \lambda V + \mu V')) \\ &= (\lambda U + \mu U')P + (\lambda V + \mu V')Q \\ &= \lambda(UP + VQ) + \mu(U'P + V'Q) \\ &= \lambda f_{j(P,Q)}((U,V)) + \mu f_{j(P,Q)}((U',V')). \end{aligned}$$

De plus, pour connaître la matrice qui représente l'application, on regarde les images des vecteurs de la base qui sont

$$\begin{aligned} f_{j(P,Q)}((X^{q-j-1}, 0)) &= X^{q-j-1}P, \\ &\vdots \\ f_j((1,0)) &= P, \\ f_j((0, X^{p-j-1})) &= X^{p-j-1}Q, \\ &\vdots \\ f_j((0,1)) &= Q. \end{aligned}$$

Les représentations de ces polynômes dans la base considérée sont alors les colonnes de la matrice, et sont

$$\begin{gathered} (a_p, \dots, a_0, 0, \dots, 0), \\ \vdots \\ (0, \dots, 0, a_p, \dots, a_0), \\ (b_q, \dots, b_0, 0, \dots, 0), \\ \vdots \\ (0, \dots, 0, b_q, \dots, b_0). \end{gathered}$$

□

**Définition 5.3.3.** Soit $0 \leq j \leq q$. La transposée de la matrice qui représente l'application $f_{j(P,Q)}$ est la $j$-ième matrice de Sylvester-Habicht de $P$ et $Q$ notée $\mathrm{SyHa}_j(P,Q)$. Cette matrice a $p+q-j$ colonnes et $p+q-2j$ rangées.

**Définition 5.3.4.** Le $j$-ième coefficient sous-résultant , noté $\mathrm{sRes}_j(P,Q)$, est le déterminant de la matrice carrée $\mathrm{SyHa}_{j,j}(P,Q)$ obtenue en prenant les $p+q-2j$ premières colonnes de $\mathrm{SyHa}_j(P,Q)$. Par convention, on étend ces définitions pour $q < j \leq p$ par

$$\mathrm{sRes}_p(P,Q) = \mathrm{sign}(a_p),$$

et

$$\mathrm{sRes}_j(P,Q) = 0.$$

Cette définition des sous-résultants n'est pas la définition standard. En effet, dans la définition standard, on considère l'application $f_j$ exprimée dans la base

$$((X^{q-j-1},0),\ldots,(1,0),(0,1),\ldots,(0,X^{p-j-1})),$$

ce qui conduit à une permutation des rangées de la matrice. Les sous-résultants définis ici sont donc les sous-résultants standards à un potentiel facteur multiplicatif $-1$ près. Cependant, dans ce mémoire on ne va s'intéresser qu'aux lieux d'annulation des sous-résultants c'est pourquoi on se permet une telle modification de la définition (car la base utilisée ici semble plus naturelle que la standard).

**Remarque 5.3.5.** Dès lors, si $p > q$, $\mathrm{SyHa}_0(P,Q) = \mathrm{Syl}(P,Q)$ et donc $\mathrm{sRes}_0(P,Q) = \mathrm{Res}(P,Q)$. Le résultant est un cas particulier de sous-résultant et la matrice de Sylvester un cas particulier de la matrice de Sylvester-Habicht.

**Exemple 5.3.6.** Considérons les polynômes suivants :

$$P = X^4 + 2X^3 - X^2 - 3 \text{ et } Q = X^2 + 2,$$

et calculons leurs sous-résultants.
Premier coefficient, $j = 0$ : la matrice est de dimension $p+q-j \times p+q-2j = 6 \times 6$. De plus, on a $q-j-1 = 1$ et $p-j-1 = 3$ donc les rangées de la matrice correspondent alors aux coefficients des polynômes $XP, P, X^3Q, X^2Q, XQ, Q$, on a donc

$$\mathrm{SyHa}_0(P,Q) = \begin{pmatrix} 1 & 2 & -1 & 0 & -3 & 0 \\ 0 & 1 & 2 & -1 & 0 & -3 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{pmatrix},$$

et on obtient alors

$$\mathrm{sRes}_0(P,Q) = \det(\mathrm{SyHa}_0(P,Q)) = 41.$$

Second coefficient, $j = 1$ : la matrice est de dimension $p + q - j \times p + q - 2j = 5 \times 4$. De plus, on a $q - j - 1 = 0$ et $p - j - 1 = 2$ donc les rangées de la matrice correspondent alors aux coefficients de $P, X^2Q, XQ, Q$, on a donc

$$\mathrm{SyHa}_1(P,Q) = \begin{pmatrix} 1 & 2 & -1 & 0 & -3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix},$$

et on obtient alors

$$\mathrm{sRes}_1(P,Q) = \det \begin{pmatrix} 1 & 2 & -1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 4.$$

Troisième coefficient, $j = 2$ : la matrice est de dimension $p + q - j \times p + q - 2j = 4 \times 2$. De plus, on a $q - j - 1 = -1$ et $p - j - 1 = 1$ et les rangées de la matrice correspondent donc aux coefficients de $XQ, Q$, on a donc

$$\mathrm{SyHa}_2(P,Q) = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix},$$

et on obtient alors

$$\mathrm{sRes}_2(P,Q) = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Quatrième coefficient, $j = 3$ : on a $j = 3 > 2 = q$ et donc

$$\mathrm{sRes}_3(P,Q) = 0.$$

Et le cinquième coefficient, $j = 4$ : on a $j = 4 = p$ donc

$$\mathrm{sRes}_4(P,Q) = \mathrm{sign}(1) = 1.$$

Les coefficients sous-résultants de $P$ et $Q$ sont donc $(41, 4, 1, 0, 1)$

**Exemple 5.3.7.** Reprenons à nouveau l'exemple 5.2.4 avec

$$P = X^2 + Y^2 - 3 \text{ et } Q = XY - 1.$$

On trouve que

$$\begin{aligned} \mathrm{SyHa}_0(P,Q) &= \mathrm{SyHa}(P,Q), \\ \mathrm{SyHa}_1(P,Q) &= \begin{pmatrix} X & -1 \end{pmatrix}. \end{aligned}$$

On obtient alors que

$$\begin{aligned} \mathrm{sRes}_0(P,Q) &= X^4 - 3X^2 + 1, \\ \mathrm{sRes}_1(P,Q) &= X, \\ \mathrm{sRes}_2(P,Q) &= 1. \end{aligned}$$

**Lemme 5.3.8.** *Soit* $\mathbf{D}$ *un anneau intègre et* $0 \leq j \leq \min(p,q)$ *si* $p \neq q$ *(resp.* $0 \leq j \leq p-1$ *si* $p = q$*). Alors* $\mathrm{sRes}_j(P,Q) = 0$ *si et seulement si il existe des polynômes non-nuls* $U \in \mathbf{K}_{q-j-1}[x]$ *et* $V \in \mathbf{K}_{p-j-1}[X]$ *tels que* $\deg(UP+VQ) < j$.

*Démonstration.* On a $\mathrm{sRes}_j(P,Q) = 0$ lorsque $\det(\mathrm{SyHa}_{j,j}(P,Q)) = 0$. Or c'est le cas si et seulement si sa transposée est de déterminant nul. Cependant, la transposée de $\mathrm{SyHa}_{j,j}(P,Q)$ est la matrice qui permet de trouver les $p+q-2j$ premières composantes de $f_j((U,V))$. Donc son déterminant est nul si et seulement il existe un couple $(U,V)$ non nul tel que $f_j((U,V))$ est nul sur ses $p+q-2j$ premières composantes. Donc si et seulement si $\deg(f_j((U,V))) \leq (p+q-j-1)-(p+q-2j) = j-1$ (car $f_j(P,Q) \in \mathbf{K}_{p+q-j-1}[X]$). □

**Proposition 5.3.9.** *Soit* $\mathbf{D}$ *un anneau intègre et* $0 \leq j \leq \min(p,q)$ *si* $p \neq q$ *(resp.* $0 \leq j \leq p-1$ *si* $p = q$*). Alors* $\deg(\mathrm{pgcd}(P,Q)) \geq j$ *si et seulement si*

$$\mathrm{sRes}_0(P,Q) = \ldots = \mathrm{sRes}_{j-1}(P,Q) = 0.$$

*Démonstration.* Supposons que $\deg(\mathrm{pgcd}(P,Q)) \geq j$. Alors le plus petit commun multiple de $P$ et $Q$,

$$\mathrm{ppcm}(P,Q) = \frac{PQ}{\mathrm{pgcd}(P,Q)},$$

est de degré $\leq p+q-j$. Ce qui est équivalent à l'existence d'un couple de polynômes $(U,V) \in \mathbf{K}_{q-j-1}[X] \times \mathbf{K}_{p-j-1}[X]$ tels que

$$UP = -VQ = \mathrm{ppcm}(P,Q).$$

Donc tels que $UP+VQ = 0$. Par le lemme 5.3.8, cela implique que

$$\mathrm{sRes}_0(P,Q) = \ldots = \mathrm{sRes}_{j-1}(P,Q) = 0.$$

La réciproque se montre par récurrence sur $j$.
Si $j = 0$ : il n'y a rien a montrer car $\mathrm{pgcd}(P,Q)$ est un polynôme non nul (éventuellement constant).
Si $j = 1$ : $\mathrm{sRes}_0(P,Q) = 0$ implique, par le lemme 5.3.8, qu'il existe un couple $(U,V) \in \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X]$ qui satisfait

$$UP + VQ = 0,$$

et donc

$$UP = -VQ.$$

Or comme $\deg(P) \neq \deg(Q)$ et que $\deg(U) < q, \deg(V) < p$, on a $\deg(\mathrm{pgcd}(P,Q)) \geq 1$. Supposons que $\mathrm{sRes}_0(P,Q) = \ldots = \mathrm{sRes}_{j-2}(P,Q) = 0$ implique que $\deg(\mathrm{pgcd}(P,Q)) \geq j-1$. De plus, si $\mathrm{sRes}_{j-1}(P,Q) = 0$, alors par le lemme 5.3.8, il existe un couple $(U,V) \in \mathbf{K}_{q-j-1}[X] \times \mathbf{K}_{p-j-1}[X]$ tels que $\deg(UP+VQ) < j-1$. Comme $\mathrm{pgcd}(P,Q)$ divise $UP+VQ$ et est de degré $\geq j-1$, on a $UP+VQ = 0$. Donc

$$UP = -VQ,$$

ce qui implique que

$$\deg(\text{ppcm}(P,Q)) \geq p+q-j,$$

et donc

$$\deg(\text{pgcd}(P,Q)) \geq j.$$

□

On en déduit directement le résultat suivant qui est celui qui nous intéresse.

**Proposition 5.3.10.** *Dans les mêmes conditions que pour l'énoncé précédent, on a* $\deg(\text{pgcd}(P,Q)) = j$ *si et seulement si*

$$\text{sRes}_0(P,Q) = \ldots = \text{sRes}_{j-1}(P,Q) = 0, \text{sRes}_j(P,Q) \neq 0.$$

# Chapitre 6

# Décomposition cylindrique algébrique

La décomposition cylindrique algébrique (abrégée CAD pour Cylindrical Algebraic Decomposition) est une méthode introduite dans les années 1970 par Georges Edwin Collins [6]. Considérons un champ réel clos $\mathbf{R}$ et notons $\mathbf{C}$ une extension algébriquement close de $\mathbf{R}$ . Cette méthode permet, à un ensemble fini de polynômes multivariés donné $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ d'obtenir une décomposition de $\mathbf{R}^n$ en des ensembles semi-algébriquement connexes telle que chaque polynôme de $\mathcal{P}$ est de signe constant sur chacune des cellules de la décomposition.

Dans la première section nous définissons la CAD et donnons un exemple, ensuite, dans la seconde section, nous démontrons le théorème 6.2.1, résultat central de ce mémoire, qui est le théorème d'existence. Dans la troisième section nous montrons comment obtenir une description explicite des cellules. Pour finir, dans la quatrième section, nous expliquons comment effectuer une élimination des quantificateurs en se servant de la CAD et illustrons cela au moyen d'un exemple.

## 6.1 Définition et exemples

Afin de manipuler aisément les cellules d'une CAD, nous utilisons la convention suivante. Si on identifie $I = (i_1, \ldots, i_k)$ avec le mot $i_1 \ldots i_k$ et où pour $j \in \mathbb{N}$ on a $I : j = (i_1, \ldots, i_k, j)$. De plus, on dit que $I = (i_1, \ldots, i_k)$ est pair (resp. impair) si $i_k$ est pair (resp. impair).

**Définition 6.1.1.** Une décomposition algébrique cylindrique (CAD) de $\mathbf{R}^n (n \geq 1)$ est une suite $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_n)$ telle que pour tout $k \in \{1, \ldots, n\}$, l'ensemble

$$\mathcal{C}_k = \{C_{i_1 \ldots i_k} : \forall j \in \{1, \ldots, k\}, i_j \in \{1, \ldots, 2u_{i_1 \ldots i_{j-1}} + 1\}\}$$

est une partition finie de $\mathbf{R}^k$ par des ensembles semi-algébriques définie récursivement comme suit :

- Il existe $u_\epsilon \in \mathbb{N}$ et des nombres réels algébriques $\alpha_2 < \alpha_4 < \ldots < \alpha_{2u_\epsilon}$ définissant les cellules de $\mathcal{C}_1$ par

$$C_{2j} = \{\alpha_{2j}\}, (1 \leq j \leq u_\epsilon),$$

$$C_{2j+1} = \left]\alpha_{2j}, \alpha_{2(j+1)}\right[, (0 \leq j \leq u_\epsilon)$$

avec les conventions $\alpha_0 = -\infty$ et $\alpha_{2u_\epsilon+2} = +\infty$.

- Alors pour chaque cellule $C_I \in \mathcal{C}_k$ $(k < n)$, il existe $n \in \mathbb{N}$ et des fonctions semi-algébriques continues $\alpha_{I:2} < \alpha_{I:4} < \ldots < \alpha_{I:2u_I} : C_I \mapsto \mathbf{R}$ qui définissent les cellules de $\mathcal{C}_{k+1}$ par

$$C_{I:2j} = \{(a, b) \in C_I \times \mathbf{R} \mid b = \alpha_{I:2j}(a)\}, (1 \leq j \leq u_I)$$

$$C_{I:2j+1} = \{(a, b) \in C_I \times \mathbf{R} \mid \alpha_{I:2j}(a) < b < \alpha_{I:2(j+1)}(a)\}, (0 \leq j \leq u_I)$$

avec les conventions $\alpha_{I:0} = -\infty$ et $\alpha_{I:2u_\epsilon+2} = +\infty$

On dit qu'un élément $C_I$ de $\mathcal{C}_k$ est une cellule d'indice $I$. Si $I$ est pair (resp. impair), on dit que la cellule est un secteur (resp. une section). Quand le contexte est clair, on identifie $\mathcal{C}$ avec $\mathcal{C}_n$.

**Définition 6.1.2.** Soit $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ un ensemble fini de polynômes. Un sous-ensemble $S \subset \mathbf{R}^n$ est $\mathcal{P}$-invariant si chaque polynôme $P \in \mathcal{P}$ est de signe constant sur $S$. Une CAD $\mathcal{C}$ de $\mathbf{R}^n$ est adaptée à $\mathcal{P}$ si chaque cellule de $\mathcal{C}$ est $\mathcal{P}$-invariante.

**Exemple 6.1.3.** Considérons l'exemple classique d'un cercle (prenons le ici de rayon $\sqrt{3}$). C'est à dire que

$$\mathcal{P} = \{X^2 + Y^2 - 3\}.$$

On commence par donner une décomposition de $\mathbb{R}$, la suivante :

$$\mathcal{C}_1 = \left\{C_1 = \left]-\infty, -\sqrt{3}\right[, C_2 = \{-\sqrt{3}\}, C_3 = \left]-\sqrt{3}, \sqrt{3}\right[, C_4 = \{\sqrt{3}\}, C_5 = \left]\sqrt{3}, +\infty\right[\right\}.$$

Puis on trouve une décomposition de $\mathbb{R}^2$, la suivante :

$$\begin{aligned}
C_{11} &= C_1 \times \mathbb{R} = \left]-\infty, -\sqrt{3}\right[ \times \mathbb{R} \\
C_{21} &= \{-\sqrt{3}\} \times ]-\infty, 0[, \\
C_{22} &= \{-\sqrt{3}\} \times \{0\} = (-\sqrt{3}, 0), \\
C_{23} &= \{-\sqrt{3}\} \times ]0, +\infty[ \\
C_{31} &= \{(x, y) \in \left]-\sqrt{3}, \sqrt{3}\right[ \times \mathbb{R} : y \in \left]-\infty, -\sqrt{x^2-3}\right[\} \\
C_{32} &= \{(x, -\sqrt{x^2-3}) : x \in \left]-\sqrt{3}, \sqrt{3}\right[\} \\
C_{33} &= \{(x, y) \in \left]-\sqrt{3}, \sqrt{3}\right[ \times \mathbb{R} : y \in \left]-\sqrt{x^2-3}, \sqrt{x^2-3}\right[\} \\
C_{34} &= \{(x, \sqrt{x^2-3}) : x \in \left]-\sqrt{3}, \sqrt{3}\right[\} \\
C_{35} &= \{(x, y) : y \in \left]\sqrt{x^2-3}, +\infty\right[\} \\
C_{41} &= \{\sqrt{3}\} \times ]-\infty, -0[, C_{42} = (\sqrt{3}, 0), C_{43} = \{\sqrt{3}\} \times ]0, +\infty[ \\
C_{51} &= C_5 \times \mathbb{R} = \left]\sqrt{3}, +\infty\right[ \times \mathbb{R}.
\end{aligned}$$

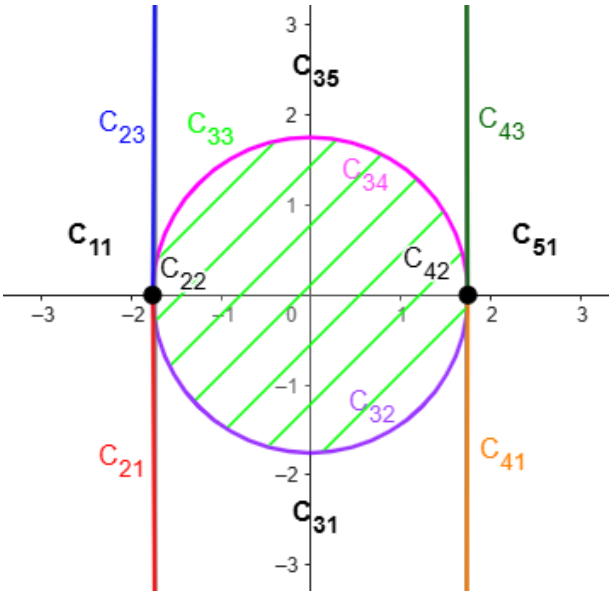


FIGURE 6.1 – CAD adaptée à $X^2 + Y^2 - 3$.

Dès lors, l'ensemble

$$\mathcal{C}_2 = \{C_{11}, C_{21}, C_{22}, C_{23}, C_{31}, C_{32}, C_{33}, C_{34}, C_{35}, C_{41}, C_{42}, C_{43}, C_{51}\}$$

forme une décomposition cylindrique algébrique de $\mathbb{R}^2$ adaptée à $\mathcal{P}$. La figure 6.1 est une représentation graphique de cette décomposition.

Une telle décomposition peut permettre d'effectuer une élimination de quantificateur. Considérons, par exemple, la formule

$$\exists Y \in \mathbb{R} : X^2 + Y^2 - 3 < 0.$$

Étant donné que le signe du polynôme est constant sur chacune des cellules de la CAD, on peut, en évaluant le polynôme en un point de chacune des cellules, connaître les régions de $\mathbb{R}$ où cette condition est vérifiée et ainsi éliminer le quantificateur "$\exists Y \in \mathbb{R}$". La seule cellule où la condition est vérifiée est la cellule $C_{33}$ et on va, dans ce cas-ci, trouver la formule sans quantificateur équivalente qui est

$$X^2 - 3 < 0.$$

De manière générale, lorsqu'on a une combinaison booléenne d'inéquations polynomiales, on effectue une CAD adaptée aux polynômes et en évaluant ceux-ci dans chacune des cellules obtenues, on peut déterminer les régions de l'espace où la combinaison est vérifiée. On peut alors éliminer les quantificateurs en projetant.

Complexifions un peu cet exemple en rajoutant le polynôme $XY - 1$ dans $\mathcal{P}$ (l'ensemble d'annulation de ce polynôme est une hyperbole d'équation $y = \frac{1}{x}$). On peut calculer une

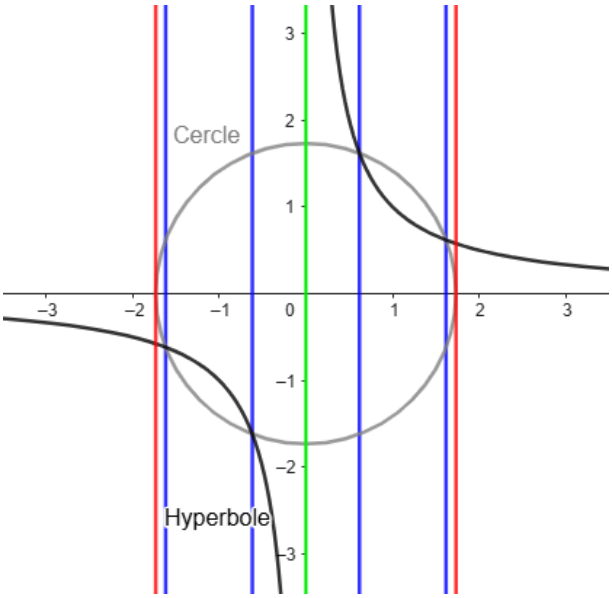


FIGURE 6.2 – CAD adaptée à $X^2 + Y^2 - 3$ et $XY - 1$.

CAD adaptée. On obtient par exemple la CAD présentée à la figure 6.2, qui est un raffinement de la précédente et qui contient 83 cellules.

Nous allons éviter de détailler ces 83 cellules, cependant nous allons expliquer intuitivement leur nature. Afin de découper $\mathbb{R}$, on compte le nombre de racines distinctes des polynômes $P(x, Y) \in \mathbb{R}[Y]$ avec $P \in \mathcal{P}$ pour tout $x \in \mathbb{R}$ et lorsque ce nombre varie, on "découpe" $\mathbb{R}$ en ce point $x$. En effet, le nombre de racines varie soit lorsque deux racines deviennent une seule (ou inversement), ce qui se produit lorsque l'ensemble d'annulation du polynôme admet une tangente verticale (en rouge sur 6.2 ). Ce nombre varie également lorsque l'ensemble d'annulation admet une asymptote verticale, ce qui peut arriver lorsque le coefficient dominant du polynôme s'annule (en vert sur 6.2). Enfin, ce nombre varie lorsque deux ensembles d'annulations de polynômes s'intersectent (en bleu sur 6.2). On va dans la suite donner un algorithme qui permet de déterminer le découpage de $\mathbb{R}$ en tenant compte de toutes les variations possibles de l'ensemble des racines.

## 6.2 Théorème d'existence

Le but de cette section va être de prouver que pour tout ensemble fini de polynômes à coefficients dans un champ réel clos, on peut construire algorithmiquement une décomposition cylindrique algébrique adaptée.

**Théorème 6.2.1.** *Pour chaque ensemble fini $\mathcal{P}$ de polynômes de $\mathbf{R}[X_1, \ldots, X_n]$ il existe une décomposition cylindrique algébrique de $\mathbf{R}^n$ adaptée à $\mathcal{P}$.*

Cependant, ce résultat nécessite plusieurs résultats préliminaires avant d'être prouvé. Dans la sous-section qui suit, nous allons démontrer le théorème de continuité des racines

(théorème 6.2.5) et les résultats qui en découlent. Dans la sous-section suivante nous définissons l'opérateur de projection de Collins, comme présenté dans [1], qui nous permet d'effectuer une récurrence sur la dimension de l'espace qu'on veut décomposer. Cet opérateur sera défini afin de pouvoir se combiner aux résultats sur la continuité des racines ce qui nous permettra alors de démontrer le théorème d'existence (théorème 6.2.1).

### 6.2.1 Théorème de continuité des racines et conséquences

Afin de démontrer le théorème 6.2.5, nous avons besoin des lemmes 6.2.3 et 6.2.4. Commençons par démontrer la proposition 6.2.2 qui fixe une borne sur les racines d'un polynôme. Ce résultat est utilisé dans la démonstration du lemme 6.2.3.

**Proposition 6.2.2.** *Soit $P = a_pX^p + \ldots + a_1X + a_0 \in \mathbf{C}[X]$ avec $a_p \neq 0$. Si $x \in \mathbf{C}$ est une racine de $P$, alors*

$$| x | \leq \max_{j=1,\ldots,p} \left( p \left| \frac{a_{p-j}}{a_p} \right| \right)^{\frac{1}{j}} = M_P$$

*Démonstration.* Si $z \in \mathbf{C}$ est tel que $|z| > M_P$, alors pour tout $i \in \{1, \ldots, p\}$ on a

$$|a_{p-i}| < \frac{|a_p|}{p}|z|^i.$$

Dès lors,

$$|P(z) - a_pz^p| = |a_{p-1}z^{p-1} + \ldots + a_0| \leq |a_{p-1}||z|^{p-1} + \ldots + |a_0| < |a_pz^p|,$$

et donc $P(z) \neq 0$. □

Dans ce qui suit, nous allons utiliser les applications poly et $m$. Pour rappel, celles-ci sont définies en 5.2.16 et en 5.2.17.

**Lemme 6.2.3.** *Soit $r > 0$, il existe $U$ un voisinage ouvert de $\mathrm{poly}_n^{-1}((X-c)^n)$ dans $\mathbf{C}^n$ tel que tout polynôme (monique) de $\mathrm{poly}_n(U)$ a ses racines dans $D(c,r) = \{z \in \mathbf{C} : |z-c| < r\}$.*

*Démonstration.* Sans perte de généralité, on peut supposer que $c = 0$. On cherche alors un voisinage de $0 \in \mathbf{C}^n$. On considère alors l'ensemble

$$U = \{v \in \mathbf{C}^n : M_Q < r \text{ où } Q = \mathrm{poly}_n(v)\}$$

où $M_Q$ est la constante définie dans la proposition 6.2.2. Soit $v \in U$, on définit $P = \mathrm{poly}_n(v)$. Si $z \in \mathbf{C}$ est tel que $P(z) = 0$ alors $|z| \leq M_P < r$ donc $z \in D(0,r)$. Montrons désormais que $U$ est un ouvert. Soit $v = (a_{n-1}, \ldots, a_0) \in U$ et notons $P = \mathrm{poly}_n(v)$. Par définition de $M_P$ on a,

$$|a_{n-j}| < \frac{r^j}{n},$$

pour tout $j \in \{1, \ldots, n\}$. Donc, il existe $\varepsilon > 0$ tel que pour tout $j \in \{1, \ldots, n\}$, on a

$$|a_{n-j}| < \frac{r^j}{n} - \varepsilon.$$

Par inégalité triangulaire, on vérifie que $B(v, \varepsilon) \subset U$. □

**Lemme 6.2.4.** *Soit $P_0 \in \mathbf{C}^{q+r}$ tel que $P_0 = m(Q_0, R_0)$ où $Q_0 \in \mathbf{C}^q$, $R_0 \in \mathbf{C}^r$ sont tels que* $\mathrm{poly}_q(Q_0)$ *et* $\mathrm{poly}_r(R_0)$ *sont premiers entre eux. Alors il existe des voisinages ouverts $U$ de $P_0$ dans $\mathbf{C}^{q+r}$, $U_1$ de $Q_0$ dans $\mathbf{C}^q$ et $U_2$ de $R_0$ dans $\mathbf{C}^r$ tels que pour tout $P \in U$ il existe un unique $Q \in U_1$ et un unique $R \in U_2$ tels que $P = m(Q, R)$.*

*Démonstration.* Au vu de la proposition 5.2.19, le jacobien de $m$ est égal au résultant de $Q_0$ et $R_0$. Ce dernier est non nul au vu de la proposition 5.2.6. On conclut alors via le théorème des fonctions implicites (théorème 4.4.8). □

On peut bien évidemment généraliser le résultat précédent avec un produit de $n > 2$ polynômes. Nous allons utiliser ces deux lemmes afin de démontrer le résultat principal de cette section qui est le théorème de continuité des racines.

**Théorème 6.2.5.** *(Continuité des racines) Soit $P \in \mathbf{R}[X_1, \ldots, X_n]$ et soit $S$ un ensemble semi-algébrique de $\mathbf{R}^{n-1}$. Supposons que* $\deg(P(x', X_n))$ *est le même pour tout $x' \in S$ et que pour un certain $a \in S$, $c_1, \ldots, c_j$ sont les racines distinctes de $P(a, X_n)$ dans $\mathbf{C}$, de multiplicités respectives $\mu_1, \ldots, \mu_j$. Si les disques ouverts $D(c_i, r) \subset \mathbf{C}$ sont disjoints alors il existe un voisinage ouvert $V$ de $a$ tel que pour tout $x' \in V \cap S$, le polynôme $P(x', X_n)$ a exactement $\mu_i$ racines, comptées avec leurs multiplicités, dans le disque $D(c_i, r)$, pour tout $i \in \{1, \ldots, j\}$.*

*Démonstration.* Pour tout $x' \in S$, on peut supposer que $P(x', X_n)$ est monique (quitte à le diviser par son coefficient (non nul) correspondant à $\deg(P(x', X_n))$). Notons

$$P_0 = \mathrm{poly}^{-1}_{\mu_1+\ldots+\mu_j}(P(a, X_n)) = \mathrm{poly}^{-1}_{\mu_1+\ldots+\mu_j}((X_n - c_1)^{\mu_1} \ldots (X_n - c_j)^{\mu_j}).$$

Par le lemme 6.2.4, il existe des voisinages ouverts $U$ de $P_0$ dans $\mathbf{C}^{\mu_1+\ldots+\mu_j}$, $U_1$ de $\mathrm{poly}^{-1}_{\mu_1}((X_n - c_1)^{\mu_1})$ dans $\mathbf{C}^{\mu_1}$, …, $U_j$ de $\mathrm{poly}^{-1}_{\mu_j}((X_n - c_j)^{\mu_j})$ dans $\mathbf{C}^{\mu_j}$ tels que tout $Q \in U$ peut être factorisé [1] de manière unique comme $Q = m(Q_1, \ldots, Q_j)$ où $Q_i \in U_i$ pour tout $i \in \{1, \ldots, j\}$. Étant donné que les coefficients de $P(x', X_n)$ sont des polynômes en $x'$, si $x'$ est suffisamment proche de $a$ alors on peut supposer que $\mathrm{poly}^{-1}_{\mu_1+\ldots+\mu_j}(P(x', X_n)) \in U$. Donc par le lemme 6.2.3, il existe un voisinage $V$ de $a$ dans $S$ tel que pour tout $x' \in V$, le polynôme $P(x', X_n)$ possède exactement $\mu_i$ racines comptées avec leur multiplicité dans $D(c_i, r)$, pour $i \in \{1, \ldots, j\}$.

□

Maintenant qu'on a obtenu le théorème de continuité des racines, on va pouvoir énoncer et démontrer les résultats qui vont nous servir à démontrer le théorème 6.2.1.

1. On identifie $Q$ à $\mathrm{poly}_n(Q)$.

**Proposition 6.2.6.** *Soient $P, Q \in \mathbf{R}[X_1, \ldots, X_n]$ et $S$ un ensemble semi-algébriquement connexe de $\mathbf{R}^{n-1}$. Supposons que $P$ et $Q$ ne soient pas identiquement nuls sur $S$ et que $\deg(P(x', X_n))$, $\deg(Q(x', X_n))$, $\deg(\mathrm{pgcd}(P(x', X_n), Q(x', X_n)))$, le nombre de racines distinctes de $P(x', X_n)$ dans $\mathbf{C}$ et le nombre de racines distinctes de $Q(x', X_n)$ dans $\mathbf{C}$ sont indépendants de $x' \in S$. Alors il existe $l$ fonctions semi-algébriques continues $\sigma_1 < \ldots < \sigma_l : S \to \mathbf{R}$ telles que pour tout $x' \in S$, l'ensemble de racines réelles de $(PQ)(x', X_n)$ est exactement $\{\sigma_1(x'), \ldots, \sigma_l(x')\}$.*

*De plus, pour $i \in \{1, \ldots, l\}$ la multiplicité de la racine $\sigma_i(x')$ de $P(x', X_n)$ (resp. $Q(x', X_n)$) est la même pour tout $x' \in S$ (la multiplicité est 0 si ce n'est pas une racine).*

*Démonstration.* Soit $a \in S$ et soient $c_1, \ldots c_j$ les racines distinctes de $(PQ)(a, X_n)$ dans $\mathbf{C}$. Soit $\mu_i$ (resp. $\nu_i$) la multiplicité de $c_i$ comme racine de $P(a, X_n)$ (resp. $Q(a, X_n)$). Le degré de $\mathrm{pgcd}(P(a, X_n), Q(a, X_n))$ est $\sum_{i=1}^{j} \min(\mu_i, \nu_i)$ et chaque $c_i$ est de multiplicité $\min(\mu_i, \nu_i)$ en tant que racine de ce pgcd.

Soit $r > 0$ tel que tous les disques $D(c_i, r)$ soient disjoints.

Par le théorème 6.2.5, au vu du fait que le nombre de racines distinctes dans $\mathbf{C}$ est le même pour tout $x' \in S$, on déduit qu'il existe un voisinage $V$ de $a$ dans $S$ tel que pour tout $x' \in V$, chaque disque $D(c_i, r)$ contient une racine de multiplicité $\mu_i$ de $P(x', X_n)$ et une racine de multiplicité $\nu_i$ de $Q(x', X_n)$. En effet, par 6.2.5, chaque disque contient $\mu_i$ (resp. $\nu_i$) racines de $P(x', X_n)$ (resp. $Q(x', X_n)$) comptées avec leur multiplicité. Or, par hypothèse le nombre de racines distinctes de $P(x', X_n)$ (resp. $Q(x', X_n)$) dans $\mathbf{C}$ est le même pour tout $x' \in S$. Par l'absurde, si un disque $D(c_i, r)$ contenait une deuxième racine de $P(x', X_n)$, alors un autre disque $D(c_k, r)$ (tel que $P(a, c_k) = 0$) devrait ne plus en contenir aucune (idem pour $Q(x', X_n)$). Ce qui contredit le théorème 6.2.5. On en déduit que pour tout $i \in \{1, \ldots, j\}$, il existe une unique racine de $P(x', X_n)$ (resp. $Q(x', X_n)$) dans $D(c_i, r)$ de multiplicité $\mu_i$ (resp. $\nu_i$).

Étant donné que le degré de $\mathrm{pgcd}(P(x', X_n), Q(x', X_n))$ vaut $\sum_{i=1}^{j} \min(\mu_i, \nu_i)$, le pgcd doit avoir exactement une racine $\lambda_i$, de multiplicité $\min(\mu_i, \nu_i)$ dans chaque disque $D(c_i, r)$ pour lequel $\min(\mu_i, \nu_i) > 0$. Donc pour tout $x' \in V$ et pour tout $i \in \{1, \ldots, j\}$, il y a exactement une racine $\lambda_i$ de $(PQ)(x', X_n)$ dans $D(c_i, r)$ qui est une racine de $P(x', X_n)$ de multiplicité $\mu_i$ et une racine de $Q(x', X_n)$ de multiplicité $\nu_i$.

De plus, le nombre de racines réelles de $(PQ)(x', X_n)$ ne change pas, en effet, procédons deux fois par l'absurde :

- si $c_i \in \mathbf{R} : \lambda_i \in \mathbf{R}$ sinon, $\overline{\lambda_i}$ serait une autre racine de $P(x', X_n)$ dans $D(c_i, r)$,
- si $c_i \notin \mathbf{R} : \lambda_i \notin \mathbf{R}$ car alors $\overline{c_i}$ est également une racine et donc $D(c_i, r)$ doit être disjoint de $D(\overline{c_i}, r)$ or si $\lambda_i \in \mathbf{R}$, il appartiendra aux deux disques.

Donc si $x' \in V$, le polynôme $(PQ)(x', X_n)$ a le même nombre de racines réelles distinctes que $(PQ)(a, X_n)$. Comme $S$ est un ensemble semi-algébriquement connexe, le nombre de racines réelles distinctes de $(PQ)(x', X_n)$ est constant pour $x' \in S$ au vu de la proposition 4.3.5. Soit $l$ ce nombre de racines. Pour $i \in \{1, \ldots, l\}$, on note par $\sigma_i : S \to \mathbf{R}$ la fonction qui envoie $x' \in S$ à la i-ème racine réelle (dans l'ordre croissant) de $(PQ)(x', X_n)$. L'argument précédent, en prenant $r$ arbitrairement petit, prouve également la continuité des fonctions $\sigma_i$. Comme $S$ est un ensemble semi-algébriquement connexe, chaque $\sigma_i(x')$ a une

multiplicité constante en tant que racine de $P(x', X_n)$ et en tant que racine de $Q(x', X_n)$ par la proposition 4.3.5. Si $S$ est décrit par la formule $\Theta(X')$ alors le graphe de $\sigma_i$ est l'ensemble de réalisation de la formule suivante :

$$\Theta(X') \wedge \left( \exists Y_1 < ... < Y_l \ \left[ \forall Y \left( (PQ)(X', Y) = 0 \Leftrightarrow \bigvee_{i=1}^{l} (Y = Y_i) \right) \wedge X_n = Y_i \right] \right)$$

Cette formule nous dit que pour tout $x' \in S$, il existe $l$ racines de $(PQ)(x', X_n)$ ordonnées dans $\mathbf{R}$ telles que ce sont exactement les racines de ce polynôme et que $X_n = Y_i$. Cela décrit donc l'ensemble des éléments de $\mathbf{R}^n$ de la forme $(x', y_i)$ où $y_i$ est la i-ème racine de $(PQ)(x', X_n)$, il s'agit donc bien du graphe de la fonction $\sigma_i$. Par la proposition 4.1.10, on en déduit que $\sigma_i$ est une fonction semi-algébrique pour tout $i \in \{1, \ldots, l\}$. □

On peut alors directement en déduire le résultat suivant.

**Proposition 6.2.7.** *Soient $\mathcal{P}$ un sous-ensemble fini de $\mathbf{R}[X_1, \ldots, X_n]$ et $S$ un ensemble semi-algébriquement connexe de $\mathbf{R}^{n-1}$. Supposons que, pour tout $P \in \mathcal{P}$, $\deg(P(x', X_n))$ et le nombre de racines réelles distinctes de $P$ sont les mêmes pour tout $x' \in S$ et que, pour tout $P, Q \in \mathcal{P}$, $\deg(\mathrm{pgcd}(P(x', X_n), Q(x', X_n)))$ soit également le même pour tout $x' \in S$. Alors il existe $l$ fonctions semi-algébriques continues $\sigma_1 < \ldots < \sigma_l : S \to \mathbf{R}$ tel que, pour tout $x' \in S$, l'ensemble des racines réelles de $\prod_{P \in \mathcal{P}'} P(x', X_n)$ où $\mathcal{P}'$ est le sous-ensemble de $\mathcal{P}$ composé des polynômes non identiquement nuls sur $S$, est exactement $\{\sigma_1(x'), \ldots, \sigma_l(x')\}$. De plus, pour $i \in \{1, \ldots, l\}$ et pour pour tout $P \in \mathcal{P}'$, la multiplicité de la racine $\sigma_i(x')$ de $P(x', X_n)$ est constante pour $x' \in S$.*

### 6.2.2 Opérateur de projection de Collins

Dans cette section, nous définissons $\mathrm{Elim}_{X_n}$, l'opérateur de projection de Collins. A partir d'un ensemble fini $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$, cet opérateur nous rend l'ensemble fini $\mathrm{Elim}_{X_n}(\mathcal{P}) \subset \mathbf{R}[X_1, \ldots, X_{n-1}]$ tel qu'une CAD de $\mathbf{R}^n$ adaptée à $\mathcal{P}$ peut être construite à partir d'une CAD de $\mathbf{R}^{n-1}$ qui est adaptée à $\mathrm{Elim}_{X_n}(\mathcal{P})$. Si on veut par exemple obtenir une CAD de $\mathbf{R}^3$ adaptée à $\mathcal{P} \subset \mathbf{R}[X_1, X_2, X_3]$, on calcule les ensembles

$$\mathcal{P}_1 = \mathrm{Elim}_{X_3}(\mathcal{P}) \subset \mathbf{R}[X_1, X_2]$$
$$\mathcal{P}_2 = \mathrm{Elim}_{X_2}(\mathcal{P}_1) \subset \mathbf{R}[X_1].$$

On peut alors trouver une CAD de $\mathbf{R}$ adaptée à $\mathcal{P}_2$ (on découpe $\mathbf{R}$ en fonction des racines dans $\mathbf{R}$ des polynômes). Cette étape peut être réalisée grâce aux résultats obtenus dans la sous-section 2.2.4. Nous allons, via les résultats de la sous-section suivante, pouvoir construire une CAD de $\mathbf{R}^2$ qui est adaptée à $\mathcal{P}_1$ et à partir de celle-ci, construire une CAD de $\mathbf{R}^3$ qui est adaptée à $\mathcal{P}$.

Cet opérateur est défini afin qu'un ensemble semi-algébrique $S$ qui est $\mathrm{Elim}_{X_n}$-invariant satisfera les conditions imposées dans l'énoncé de la proposition 6.2.7.

Avant de définir l'opérateur, introduisons la notion de troncature d'un polynôme. Cette notion est définie car on s'en sert pour définir l'opérateur $\mathrm{Elim}_{X_n}$.

**Définition 6.2.8.** Soient un anneau intègre $\mathbf{D}$ et un polynôme $P = a_pX^p + \ldots + a_0 \in \mathbf{D}[X]$. On définit, pour tout $0 \leq i \leq p$ la troncature de $P$ en $i$ par

$$\mathrm{Tru}_i(P) = a_iX^i + \ldots + a_0.$$

L'ensemble des troncatures d'un polynôme non nul $P \in \mathbf{D}[X_1, \ldots, X_n]$ est le sous-ensemble fini de $\mathbf{D}[X_1, \ldots, X_n]$ défini par

$$\mathrm{Tru}(P) = \begin{cases} \{P\} & \text{si } \mathrm{lcof}_{X_n}(P) \in \mathbf{D} \text{ ou si } \deg_{X_n}(P) = 0. \\ \{P\} \cup \mathrm{Tru}(\mathrm{Tru}_{\deg_{X_n}(P)-1}(P)) & \text{sinon.} \end{cases} \tag{6.1}$$

**Exemple 6.2.9.** Considérons le polynôme

$$P = (2X_1)X_2^2 + (3 - 4X_1)X_2 - X_1 + 2 \in \mathbb{Z}[X_1, X_2].$$

Calculons l'ensemble de ses troncatures. Étant donné que $\deg_{X_2}(P) = 2$ et $\mathrm{lcof}_{X_2}(P) = 2X_1 \notin \mathbb{Z}$, nous nous trouvons dans le second cas. On a alors

$$\mathrm{Tru}(P) = \{P\} \cup \mathrm{Tru}(\mathrm{Tru}_{\deg_{X_2}(P)-1}(P)).$$

Cependant, on a

$$\mathrm{Tru}_{\deg_{X_2}(P)-1}(P) = X_2(3 - 4X_1) - X_1 + 2.$$

Notons ce polynôme $P_1$. On a alors $\mathrm{Tru}(P) = \{P\} \cup \mathrm{Tru}(P_1)$. Comme $\deg_{X_2}(P_1) = 1$ et $\mathrm{lcof}_{X_2}(P_1) = 3 - 4X_1 \notin \mathbb{Z}$, on a

$$\mathrm{Tru}(P_1) = \{P_1\} \cup \mathrm{Tru}(\mathrm{Tru}_0(P_1)).$$

On a $\mathrm{Tru}_0(P_1) = -X_1 + 2$, notons ce polynôme $P_2$. Étant donné que $\deg_{X_2}(P_2) = 0$, on a $\mathrm{Tru}(P_2) = \{P_2\}$. Au final, obtient alors que

$$\mathrm{Tru}(P) = \{P, P_1, P_2\} = \{(2X_1)X_2^2 + X_2(3-4X_1) - X_1 + 2, X_2(3-4X_1) - X_1 + 2, -X_1 + 2\}.$$

Nous allons désormais définir l'ensemble des troncatures d'un ensemble fini de polynômes et l'opérateur de projection, $\mathrm{Elim}_{X_n}$.

**Définition 6.2.10.** Soit $\mathcal{P}$ un sous-ensemble fini de $\mathbf{R}[X_1, \ldots, X_n]$, on considère

$$\mathrm{Tru}(\mathcal{P}) = \bigcup_{P \in \mathcal{P}} \mathrm{Tru}(P)$$

On définit $\mathrm{Elim}_{X_n}(\mathcal{P})$ le sous-ensemble de polynômes de $\mathbf{R}[X_1, \ldots, X_{n-1}]$ comme suit :

- Si $Q \in \mathrm{Tru}(\mathcal{P})$ et $\deg_{X_n}(Q) \geq 2$ :
  $\mathrm{Elim}_{X_n}(\mathcal{P})$ contient tous les $\mathrm{sRes}_j(Q, \frac{\partial Q}{\partial X_n}) \notin \mathbf{R}$, pour tout $j \in \{0, \ldots, \deg_{X_n}(Q)-2\}$.
- Si $Q, S \in \mathrm{Tru}(\mathcal{P})$ :
  - si $\deg_{X_n}(Q) > \deg_{X_n}(S) \geq 1$ : $\mathrm{Elim}_{X_n}(\mathcal{P})$ contient tous les $\mathrm{sRes}_j(Q, S) \notin \mathbf{R}$, pour tout $j \in \{0, \ldots, \deg_{X_n}(S) - 1\}$

- si $\deg_{X_n}(Q) = \deg_{X_n}(S) \geq 2$ : $\mathrm{Elim}_{X_n}(\mathcal{P})$ contient tous les $\mathrm{sRes}_j(S, \overline{Q}) \notin \mathbf{R}$ avec $\overline{Q} = \mathrm{lcof}_{X_n}(S)Q - \mathrm{lcof}_{X_n}(Q)S$, pour tout $j \in \{0, \ldots, \deg_{X_n}(\overline{Q}) - 1\}$.

- Si $Q \in \mathrm{Tru}(\mathcal{P})$ et $\mathrm{lcof}_{X_n}(Q) \notin R$ alors $\mathrm{Elim}_{X_n}(\mathcal{P})$ contient $\mathrm{lcof}_{X_n}(Q)$.

La définition de l'opérateur $\mathrm{Elim}_{X_n}$ peut sembler peu claire à première vue. On prend les polynômes dont on a besoin pour vérifier qu'un ensemble semi-algébrique $S$ qui est $\mathrm{Elim}_{X_n}(\mathcal{P})$-invariant satisfasse les conditions de la proposition 6.2.7 (voir démonstration du théorème 6.2.13). On précise cependant que si $P$ et $Q$ sont de même degré alors on ne peut pas calculer leurs sous-résultants. Pour contourner ce problème, on définit $\overline{P}$ ou $\overline{Q}$. En effet si on a une racine commune à $P$ et $Q$ alors ce sera également une racine de $\overline{P}$ et de $\overline{Q}$. Dès lors leur pgcd est identique, on peut alors utiliser les $\mathrm{sRes}_j(P, \overline{Q})$ pour étudier $\deg(\mathrm{pgcd}(P, Q))$.

Nous allons désormais montrer deux exemples. Le premier est simplement une mise en oeuvre de la définition tandis que le second continue l'exemple 6.1.3.

**Exemple 6.2.11.** Considérons les polynômes de $\mathbb{R}[X, Y]$

$$P_1 = 2XY + 3Y - X \text{ et } P_2 = Y^2 - 2.$$

On a alors

$$\mathrm{Tru}(P_1) = \{2XY + 3Y - X, -X\} \text{ et } \mathrm{Tru}(P_2) = \{Y^2 - 2\}.$$

On peut alors démarrer l'algorithme permettant de calculer $\mathrm{Elim}_Y(\mathcal{P})$.

- Cas où $Q \in \mathrm{Tru}(\mathcal{P})$ tel que $\deg_Y(Q) \geq 2$. On a $Q = Y^2 - 2$. Comme $\deg_Y(Q) - 2 = 0$, on doit seulement calculer $\mathrm{sRes}_0(Q, \frac{\partial Q}{\partial Y}) = \mathrm{sRes}_0(Y^2 - 2, 2Y)$. On a

$$\mathrm{SyHa}_0(Y^2 - 2, 2Y) = \begin{pmatrix} 1 & 0 & -2 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

  On trouve alors $\mathrm{sRes}_0(Y^2 - 2, 2Y) = -8$, or $-8 \in \mathbb{R}$ donc $\mathrm{sRes}_0(Q, \frac{\partial Q}{\partial Y}) \notin \mathrm{Elim}_Y(\mathcal{P})$.

- Cas où $Q, S \in \mathrm{Tru}(\mathcal{P})$. Il y a donc 3 cas à considérer. Cependant lorsqu'on prend $S = -X$, on a $\deg_Y(S) - 1 = -1 < 0$ et donc on ne considère aucun sous-résultant. Il n'y a donc en réalité, qu'un seul cas à considérer : $Q = Y^2 - 2$ et $S = 2XY + 3Y - X$. On a $\deg_Y(S) - 1 = 0$, on doit alors calculer

$$\begin{aligned} \mathrm{sRes}_0(Q, S) &= \mathrm{sRes}_0(Y^2 - 2, 2XY + 3Y - X) \\ &= \det \begin{pmatrix} 1 & 0 & -2 \\ 2X + 3 & -X & 0 \\ 0 & 2X + 3 & -X \end{pmatrix} \\ &= -(7X^2 + 24X + 18) \notin \mathbb{R} \end{aligned}$$

  Donc $\mathrm{sRes}_0(Q, S) = -(7X^2 + 24X + 18) \in \mathrm{Elim}_Y(\mathcal{P})$.

- Il reste à considérer le cas où $\mathrm{lcof}_Y(Q) \notin \mathbb{R}$, c'est le cas de $2XY + 3Y - X$ et donc $2X + 3 \in \mathrm{Elim}_Y(\mathcal{P})$.

On obtient donc finalement que

$$\mathrm{Elim}_Y(\mathcal{P}) = \{-(7X^2 + 24X + 18), 2X + 3\}.$$

**Exemple 6.2.12.** Prenons les polynômes considérés dans l'exemple 6.1.3, on a

$$P_1 = X^2 + Y^2 - 3 \text{ et } P_2 = XY - 1$$

dans $\mathbb{R}[X, Y]$. Calculons l'ensemble $\mathrm{Elim}_Y(\{P_1, P_2\})$. On trouve que

$$\mathrm{Tru}(P_1) = \{X^2 + Y^2 - 3\} \text{ et } \mathrm{Tru}(P_2) = \{XY - 1, -1\}$$

Donc $\mathrm{Tru}(\{P_1, P_2\}) = \{X^2 + Y^2 - 3, XY - 1, -1\}$. Déterminons alors l'ensemble $\mathrm{Elim}_Y(\{P_1, P_2\})$.

- Le premier cas concerne les polynômes de degré minimum 2. Dans ce cas, seul $X^2+Y^2-3$ est concerné. On a $\deg_Y(X^2+Y^2-3)-2 = 0$, on doit alors uniquement calculer $\mathrm{sRes}_0(X^2 + Y^2 - 3, 2Y)$. Au vu de l'exemple 5.1.6, du corollaire 5.2.12 et de la remarque 5.3.5. On trouve que $\mathrm{sRes}_0(X^2 + Y^2 - 3, 2Y) = 4X^2 - 12$. Or $4X^2 - 12 \notin \mathbf{R}$. Dès lors, $4X^2 - 12 \in \mathrm{Elim}_Y(\{P_1, P_2\})$.
- Dans le second cas, on considère toutes les paires de polynômes de $\mathrm{Tru}(\{P_1, P_2\})$, cependant le polynôme $-1$ n'est pas à prendre en compte car il est de degré nul. On doit seulement considérer le cas

  $$Q = X^2 + Y^2 - 3 \text{ et } S = XY - 1$$

  on a $\deg_Y(S) - 1 = 0$, il faut donc calculer $\mathrm{sRes}_0(Q, S)$. On a montré dans l'exemple 5.3.7 que ce sous-résultant vaut $X^4 - 3X^2 + 1 \notin \mathbf{R}$ donc $X^4 - 3X^2 + 1 \in \mathrm{Elim}_Y(\{P_1, P_2\})$.
- Pour le troisième et dernier cas, on considère les polynômes n'ayant pas un coefficient dominant réel. C'est le cas de $XY - 1$, en effet $\mathrm{lcof}_Y(XY - 1) = X$ et donc $X \in \mathrm{Elim}_Y(\{P_1, P_2\})$.

Au total, on a trouvé que

$$\mathrm{Elim}_Y(\{P_1, P_2\}) = \{X^4 - 3X^2 + 1, 4X^2 - 12, X\}.$$

De plus, notons $A, B, C, D$ et $E$ les ensembles d'annulation respectifs des polynômes $P_1, P_2, X^4 - 3X^2 + 1, 4X^2 - 12$ et $X$ et représentons les à la figure 6.3.

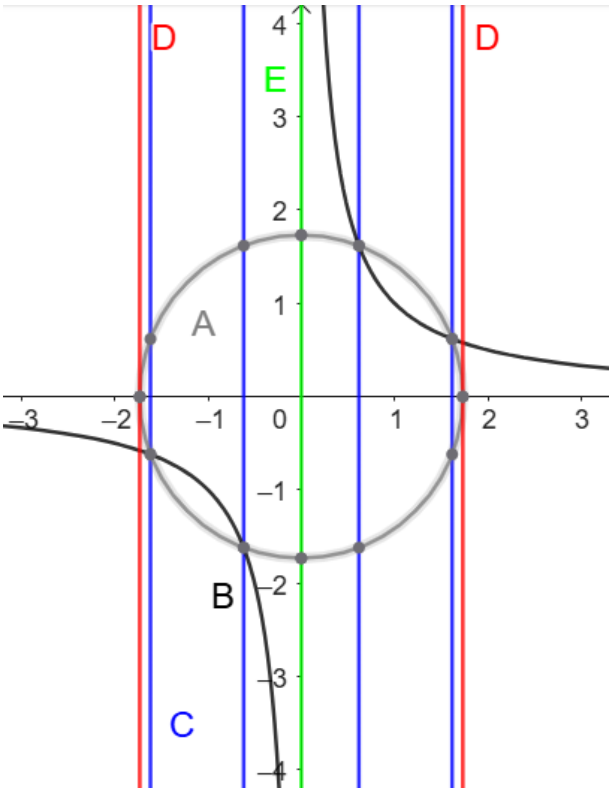


FIGURE 6.3 – Représentation des ensembles A,B,C,D et E.

On remarque qu'il s'agit de la CAD adaptée à $X^2+Y^2-3$ et $XY-1$ dont on parlait dans l'exemple 6.1.3.

**Théorème 6.2.13.** *Soit $\mathcal{P}$ un ensemble fini de polynômes de $\mathbf{R}[X_1,\ldots,X_n]$ et soit $S$ un ensemble semi-algébriquement connexe de $\mathbf{R}^{n-1}$ qui est $\mathrm{Elim}_{X_n}(\mathcal{P})$-invariant. Alors, il existe des fonctions semi-algébriques continues $\sigma_1 < \ldots < \sigma_l : S \to \mathbf{R}$ telles que pour tout $x' \in S$, l'ensemble $\{\sigma_1(x'),\ldots,\sigma_l(x')\}$ est l'ensemble de toutes les racines réelles de tous les polynômes non-nuls $P(x',X_n)$, $P \in \mathcal{P}$. Le graphe de chaque $\sigma_i$ (resp. chaque secteur du cylindre $S \times \mathbf{R}$ bordé par ces graphes est un ensemble semi-algébriquement connexe et est $\mathcal{P}$-invariant.*

*Démonstration.* Il suffit de vérifier que l'ensemble $S$ satisfait les conditions de la proposition 6.2.7. Soient $P \in \mathcal{P}$ et $Q \in \mathrm{Tru}(P)$. On considère l'ensemble semi-algébrique $A \subset \mathbf{R}^{n-1}$ défini par

$$A = \{x' \in \mathbf{R}^{n-1} : \mathrm{lcof}(Q(x',X_n)) \neq 0 \wedge \deg(P(x',X_n)) = \deg(Q(x',X_n))\}$$

Par la proposition 5.3.9, pour tout $x' \in A$, l'annulation ou non des $\mathrm{sRes}_j(Q, \frac{\partial Q}{\partial X_n})(x')$ détermine le nombre de racines distinctes de $P(x',X_n)$ dans $\mathbf{C}$, qui est

$$\deg(Q(x',X_n)) - \deg(\mathrm{pgcd}(Q(x',X_n), \frac{\partial Q}{\partial X_n}(x',X_n))).$$

De même, soient $P_1, P_2 \in \mathcal{P}$, $Q_1 \in \mathrm{Tru}(P_1)$ et $Q_2 \in \mathrm{Tru}(P_2)$. On considère l'ensemble semi-algébrique $B$ défini par

$$B = \Big\{x' \in \mathbf{R}^{n-1} : \bigwedge_{i=1}^{2} \big(\mathrm{lcof}(Q_i(x', X_n)) \neq 0 \wedge \deg(P_i(x', X_n)) = \deg(Q_i(x', X_n))\big)\Big\}.$$

Pour tout $x' \in B$, les $\mathrm{sRes}_j(Q_1, Q_2)(x')$ (resp. $\mathrm{sRes}_j(Q_2, Q_1)(x')$, $\mathrm{sRes}_j(Q_2, \overline{Q_1})(x')$, voir définition 6.2.10) qui s'annulent déterminent, par la proposition 5.3.9, le degré de $(\mathrm{pgcd}(P_1(x', X_n), P_2(x', X_n)))$. Ainsi, l'hypothèse qu'un ensemble semi-algébriquement connexe de $\mathbf{R}^{n-1}$ est $\mathrm{Elim}_{X_n}(\mathcal{P})$-invariant implique que les hypothèses de la proposition 6.2.7 sont vérifiées. La connexité semi-algébrique des graphes des $\sigma_i$ découle de la proposition 4.3.3 tandis que la connexité semi-algébrique des cellules délimitées par ces graphes découle de la proposition 4.3.4, ou d'une adaptation directe dans le cadre d'un secteur non borné. □

On a désormais tout ce qu'il faut pour démontrer le Théorème 6.2.1.

*Démonstration du Théorème 6.2.1.* Cette preuve s'effectue par récurrence sur la dimension de l'espace.

- Soit $\mathcal{P} \subset \mathbf{R}[X_1]$ un sous-ensemble fini. Les racines réelles des polynômes de $\mathcal{P}$ donnent un découpage de $\mathbf{R}$ en un nombre fini de points et d'intervalles ouverts de $\mathbf{R}$ qui constituent les cellules d'une décomposition cylindrique algébrique de $\mathbf{R}$ adaptée à $\mathcal{P}$. En effet, au vu de la proposition 2.2.9, chaque polynôme $P \in \mathcal{P}$ est de signe constant sur chacune des cellules.
- Soit $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ un sous-ensemble fini. En partant d'une décomposition cylindrique algébrique de $\mathbf{R}^{n-1}$ adaptée à $\mathrm{Elim}_{X_n}(\mathcal{P})$, on applique aux cellules de cette décomposition le théorème 6.2.13, on obtient une décomposition cylindrique algébrique de $\mathbf{R}^n$ adaptée à $\mathcal{P}$ dont les cellules sont délimitées par les graphes fonctions $\sigma_1 < \ldots < \sigma_l$ évoquées précédemment.

□

Lorsque Collins introduit la décomposition cylindrique algébrique dans [6], il ne parle pas encore d'ensembles et fonctions semi-algébriques.

Dans son raisonnement il ne semble pas faire appel au Principe de Tarski-Seidenberg, contrairement à ce qu'on a fait dans la proposition 6.2.6. En effet, Collins fournit une preuve totalement constructive. Comme nous allons le voir dans la section 6.4, la CAD permet d'effectuer une élimination des quantificateurs dans le langage des champs ordonnés. Dès lors, la décomposition cylindrique algébrique telle que Collins l'a introduite démontre donc l'élimination des quantificateurs dans le langage des champs ordonnés dans le contexte des champs réels clos.

## 6.3 Description semi-algébrique des cellules

On a prouvé l'existence d'une décomposition cylindrique algébrique adaptée à $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$, mais on n'a pas de description de ces cellules au moyen d'une formule sans quantificateur du langage des champs ordonnés. En effet, pour rappel, au vu de la remarque 4.1.5 et de de la proposition 4.1.10, on sait que les ensembles semi-algébriques sont exactement les ensembles de la forme Reali($\Phi$) où $\Phi$ est une formule du langage des champs ordonnés. Dans cette section, nous allons montrer comment obtenir une CAD adaptée à $\mathcal{P}$, où les cellules sont des ensembles semi-algébriques dont on connaît les formules qui les définissent.

**Définition 6.3.1.** Soit $\mathbf{R}$ un champ réel clos. Une condition de signe sur $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ est une application

$$\sigma : \mathcal{P} \to \{-1, 0, 1\}.$$

On dit que $\mathcal{P}$ réalise la condition de signe $\sigma$ en $x \in \mathbf{R}^n$ si

$$\bigwedge_{P \in \mathcal{P}} (\text{sign}(P(x)) = \sigma(P)).$$

La réalisation d'une condition de signe $\sigma$ est l'ensemble

$$\text{Reali}(\sigma) = \{x \in \mathbf{R}^n : \bigwedge_{P \in \mathcal{P}} \text{sign}(P(x)) = \sigma(P)\}.$$

La condition de signe $\sigma$ est réalisable si $\text{Reali}(\sigma) \neq \emptyset$.

**Définition 6.3.2.** Sous les mêmes hypothèses, une condition de signe faible est une application

$$\sigma : \mathcal{P} \to \{\{0\}, \{0, 1\}, \{-1, 0\}\}.$$

La réalisation d'une condition de signe faible est l'ensemble

$$\text{Reali}(\sigma) = \{x \in \mathbf{R}^n : \bigwedge_{P \in \mathcal{P}} (\text{sign}(P(x)) \in \sigma(P))\}.$$

De même, cette condition est réalisable si $\text{Reali}(\sigma) \neq \emptyset$.

Il est clair que les ensembles Reali($\sigma$) sont des ensembles semi-algébriques pour toute condition de signe $\sigma$ (faible ou non).

**Définition 6.3.3.** Si $\sigma$ est une condition de signe sur $\mathcal{P}$, on peut définir la condition de signe faible qui lui est associée par

$$\overline{\sigma} : \mathcal{P} \to \{\{0\}, \{0, 1\}, \{-1, 0\}\} : P \mapsto \begin{cases} \{0\} & \text{si } \sigma(P) = 0 \\ \{0, 1\} & \text{si } \sigma(P) = 1 \\ \{-1, 0\} & \text{si } \sigma(P) = -1. \end{cases}$$

**Remarque 6.3.4.** Malgré ce à quoi on pourrait s'attendre, relâcher la condition de signe n'est pas équivalent à prendre l'adhérence de la réalisation. Considérons le polynôme $P = X^3 - X^2$ et la condition de signe $\sigma : P \mapsto 1$, on a alors $\overline{\sigma}(P) = \{0, 1\}$. Cependant on a d'une part

$$\overline{\text{Reali}(\sigma)} = \overline{\{x \in \mathbb{R} : P(x) > 0\}} = \overline{]1, +\infty[} = [1, +\infty[\,,$$

et d'autre part

$$\text{Reali}(\overline{\sigma}) = \{x \in \mathbb{R} : P(x) \geq 0\} = \{0\} \cup [1, +\infty[\,.$$

Nous savons que les polynômes sont de signe constant sur les cellules de la CAD, il est donc évident que pour chaque cellule $C$, il existe une condition de signe $\sigma$ telle que $C \subseteq \text{Reali}(\sigma)$. Cependant, plusieurs cellules peuvent se trouver dans le même ensemble $\text{Reali}(\sigma)$, c'est ce que nous allons illustrer dans l'exemple 6.3.6.

Pour contrer ce problème, nous allons rajouter une étape dans la construction de la CAD afin d'ajouter des polynômes tels que pour chaque cellule $C$ de la CAD obtenue en considérant ces polynômes supplémentaires, il existe une condition de signe $\sigma$ telle que $C = \text{Reali}(\sigma)$.

Ce qui nous amène à la définition suivante.

**Définition 6.3.5.** Soit $S$ un ensemble semi-algébrique de $\mathbf{R}^n$. Une description semi-algébrique de $S$ est un ensemble fini de polynômes $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ ainsi que un ensemble fini de conditions de signe (ou de signe faible) $\sigma_1, \ldots, \sigma_J$ sur $\mathcal{P}$ telles que $S = \bigcup_{j=1}^{J} \text{Reali}(\sigma_j)$.

**Exemple 6.3.6.** Reprenons l'exemple 6.2.12. On voulait effectuer une CAD de $\mathbb{R}^2$ adaptée à

$$\mathcal{P} = \{X^2 + Y^2 - 3, XY - 1\}$$

et on avait obtenu une CAD obtenue par les ensembles d'annulation des polynômes de

$$\{X^2 + Y^2 - 3, XY - 1, X^4 - 3X^2 + 1, X^2 - 3, X\}.$$

Dans ce cas, si on avait par exemple voulu décrire la cellule

$$C = \{(x, y) \in \mathbb{R}^2 : x \in ]0, c[, y \in \left]-\sqrt{3 - x^2}, \sqrt{3 - x^2}\right[\}$$

(où $c$ est une des 4 racines $a < b < c < d$ de $X^4 - 3X^2 + 1$). On ne peut alors pas donner une description de cette cellule avec ces polynômes. En effet, dans cette région on a

$$\begin{cases} X^2 + Y^2 - 3 < 0 \\ XY - 1 < 0 \\ X^4 - 3X^2 + 1 > 0 \\ X^2 - 3 < 0 \\ X > 0. \end{cases}.$$

Donc $C \subset \text{Reali}(\sigma)$ avec $\sigma = (-1, -1, 1, -1, 1)$. Cependant cette inclusion est stricte. En effet, la cellule

$$C' = \{(x, y) \in \mathbb{R}^2 : x \in ]d, \sqrt{3}[, y \in ]-\sqrt{3 - x^2}, \sqrt{3 - x^2}[\}$$

correspond également à cette condition. Il faut donc rajouter des polynômes afin de séparer ces deux cellules.

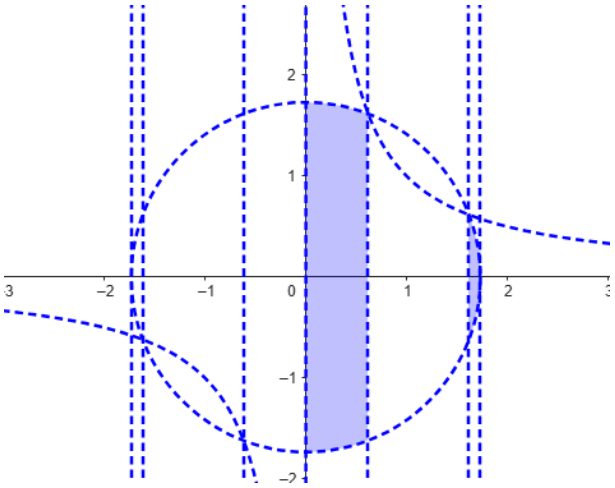


FIGURE 6.4 – Représentation des cellules $C$ (zone bleue au centre du cercle) et $C'$ (zone bleue à l'extrême droite du cercle).

**Définition 6.3.7.** Soit $\mathbf{R}$ un champ réel clos. Un ensemble de polynômes $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ est clos par dérivation selon $X_i$ ($i \in \{1, \ldots, n\}$) si $0 \notin \mathcal{P}$ et si pour tout $P \in \mathcal{P}$ on a $\frac{\partial P}{\partial X_i} \in \mathcal{P}$ ou bien $\frac{\partial P}{\partial X_i} = 0$.

Nous utilisons maintenant cette définition pour des polynômes à une variable.

**Lemme 6.3.8.** *(Lemme de Thom) Soit $\mathcal{P} \subset \mathbf{R}[X]$ un ensemble fini de polynômes clos par dérivation et soit $\sigma$ une condition de signe sur $\mathcal{P}$. Alors*

*(i) l'ensemble* $\mathrm{Reali}(\sigma)$ *est soit vide, soit un point, soit un intervalle ouvert ;*

*(ii) si* $\mathrm{Reali}(\sigma) = \emptyset$ *alors* $\mathrm{Reali}(\overline{\sigma})$ *est soit vide, soit un point ;*

*(iii) si* $\mathrm{Reali}(\sigma) = \{a\}$ *alors* $\mathrm{Reali}(\overline{\sigma}) = \{a\}$ *;*

*(iv) si* $\mathrm{Reali}(\sigma) = ]a, b[$ *alors* $\mathrm{Reali}(\overline{\sigma}) = [a, b]$.

*Démonstration.* Effectuons une récurrence sur le nombre $s$ de polynômes de $\mathcal{P}$.

1. Si $s = 0$, il n'y a rien à faire.
2. Si on considère le cas $s = 1$, la famille $P_1$ n'est stable par dérivation que si $P_1$ est constant. Comme cela nous sera utile par la suite, considérons le cas d'une famille finie $P_1, \ldots, P_s$ de polynômes constants et non nuls, disons $P_i(x) = c_i \neq 0$ pour tout $x \in \mathbf{R}$. Dans ce cas particulier on a

$$\mathrm{Reali}(\sigma) = \begin{cases} \mathbf{R} & \text{si } \sigma(P_i) = \mathrm{sign}(c_i), \quad \forall i \leq s \\ \emptyset & \text{sinon} \end{cases}$$

La condition $(i)$ est alors satisfaite. Pour les conditions suivantes, traitons les deux cas séparément :

a) Si Reali($\sigma$) = $\mathbf{R}$, alors les conditions $(ii)$ et $(iii)$ sont directement satisfaites et pour $(iv)$ on note que Reali($\sigma$) $\subset$ Reali($\overline{\sigma}$).

b) Si Reali($\sigma$) = $\emptyset$, alors $(iii)$ et $(iv)$ sont directement satisfaites et il existe $i \leq s$ tel que $\sigma(P_i) \neq \text{sign}(c_i)$. Comme sign($c_i$) vaut $-1$ ou 1 par hypothèse, on a aussi sign($c_i$) $\notin \overline{\sigma}(P_i)$, et donc Reali($\overline{\sigma}$) = $\emptyset$.

3. Supposons maintenant que le résultat est vérifié pour $s$ ($s \geq 1$) polynômes et supposons que $P$ est un polynôme de degré maximal de l'ensemble $\mathcal{P}$ qui est clos par dérivation et qui contient $s+1$ polynômes. On peut supposer que $P$ n'est pas constant vu le point précédent. Puisque $P$ est de degré maximal dans $\mathcal{P}$, il n'est le dérivé d'aucun élément de $\mathcal{P}$. Dès lors, l'ensemble $\mathcal{P}\backslash\{P\}$ est toujours clos par dérivation et contient $s$ polynômes. Soit $\sigma$ une condition de signe sur $\mathcal{P}$ et notons $\sigma'$ sa restriction à $\mathcal{P}\backslash\{P\}$. On a alors

$$\text{Reali}(\sigma) = \text{Reali}(\sigma') \cap \{x \in \mathbf{R} : \text{sign}(P(x)) = \sigma(P)\}, \tag{6.2}$$

et de même

$$\text{Reali}(\overline{\sigma}) = \text{Reali}(\overline{\sigma'}) \cap \{x \in \mathbf{R} : \text{sign}(P(x)) \in \overline{\sigma}(P)\}, \tag{6.3}$$

Par hypothèse de récurrence, Reali($\sigma'$) et Reali($\overline{\sigma'}$) satisfont les propriétés de l'énoncé. Traitons trois cas distincts selon la nature de Reali($\sigma'$).

a) Si Reali($\sigma'$) = $\emptyset$, alors par $(ii)$, Reali($\overline{\sigma'}$) est soit vide, soit réduit à un point. Alors par (6.2), Reali($\sigma$) est vide et $(i)$ est satisfait. On note alors que $(ii)$ (pour $\sigma$) découle alors de (6.3), et que $(iii)$ et $(iv)$ sont directs.

b) Si Reali($\sigma'$) = $\{a\}$, alors par $(iii)$, Reali($\overline{\sigma'}$) = $\{a\}$. Alors par (6.2), Reali($\sigma$) $\subset$ Reali($\sigma'$) = $\{a\}$ et $(i)$ est vrai : Reali($\sigma$) est vide ou égal à $\{a\}$. Cela implique directement $(iv)$. Les points $(ii)$ et $(iii)$ sont également directs, puisque Reali($\overline{\sigma'}$) = $\{a\}$.

c) Si Reali($\sigma'$) est un intervalle ouvert $]a, b[$, alors par $(iv)$ on a Reali($\overline{\sigma'}$) = $[a, b]$. Alors la dérivée de $P$ appartient à $\mathcal{P}\backslash\{P\}$ a un signe constant non nul sur $]a, b[$ (car $P$ n'est pas constant). Dès lors, $P$ est strictement monotone sur $[a, b]$ = Reali($\overline{\sigma'}$) et ne s'y annule au plus qu'en un seul point. On peut alors construire tous les tableaux de signes possibles pour $P$ sur $]a, b[$ et sur $[a, b]$ et on constate que Reali($\sigma$) est vide, ou réduit à un point ou un intervalle ouvert inclus dans Reali($\sigma'$), et que Reali($\overline{\sigma}$) satisfait les conditions $(ii)$ à $(iv)$ dans tous les cas.

□

En alternant l'application de l'opérateur Elim avec la clôture par dérivation, on obtient un ensemble de polynômes dont les conditions de signe réalisables définissent les cellules d'une décomposition cylindrique algébrique adaptée à $\mathcal{P}$.

**Théorème 6.3.9.** *Soit $\mathcal{P} \subset \mathbf{R}[X_1, \ldots, X_n]$ un ensemble fini de polynômes. Considérons des ensembles finis de polynômes non nuls $\mathcal{P}_1, \ldots, \mathcal{P}_n$ tels que*

- $\mathcal{P} \subseteq \mathcal{P}_n$ ;
- *pour tout* $i \in \{2, \ldots, n\}$, $\mathrm{Elim}_{X_i}(\mathcal{P}_i) \subseteq \mathcal{P}_{i-1}$ ;
- *pour tout* $i \in \{1, \ldots, n\}$, $\mathcal{P}_i \subset \mathbf{R}[X_1, \ldots, X_i]$ *et est clos par dérivation par rapport à* $X_i$.

*Alors la famille* $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_n)$, *où*

$$\mathcal{C}_i = \{\mathrm{Reali}(\sigma) \mid \sigma \text{ est une condition de signe réalisable sur } \cup_{j=1}^{i} \mathcal{P}_j\} \tag{6.4}$$

*pour tout* $i \in \{1, \ldots, n\}$, *est une CAD de* $\mathbf{R}^n$ *adaptée à* $\mathcal{P}_n$.

Remarquons que si $\mathcal{C}$ est adapté à $\mathcal{P}_n$, alors $\mathcal{C}$ est automatiquement adapté à $\mathcal{P}$.

*Idée de la preuve.* Procédons par récurrence sur $n$. Le cas $n = 1$ est traité par le lemme 6.3.8. Supposons que $(\mathcal{C}_1, \ldots, \mathcal{C}_{n-1})$ constitue une CAD de $\mathbf{R}^{n-1}$ adaptée à $\mathcal{P}_{n-1}$ où les $\mathcal{C}_i$ sont donnés par (6.4). Cette CAD étant en particulier adaptée à $\mathrm{Elim}_{X_n}(\mathcal{P}_n)$, en appliquant le théorème 6.2.13, on peut construire une CAD $(\mathcal{C}_1, \ldots, \mathcal{C}_{n-1}, \mathcal{C}_n)$ adaptée à $\mathcal{P}_n$ en utilisant précisément les fonctions données par la proposition 6.2.7. On peut montrer, en utilisant le lemme de Thom et l'hypothèse de récurrence, que $\mathcal{C}_n$ vérifie bien la relation (6.4).

□

**Exemple 6.3.10.** Illustrons le cas où $n = 1$. Prenons par exemple le polynôme $X^2 - 1$. On doit considérer $\mathcal{P} \subset \mathbb{R}[X]$ clos par dérivation donc on prend

$$\mathcal{P} = \{X^2 - 1, 2X, 2\}.$$

Notons $\sigma = (i, j, k)$ (avec $i, j, k \in \{-1, 0, 1\}$) la condition de signe

$$\sigma : \mathcal{P} \to \{-1, 0, 1\} : \begin{cases} X^2 - 1 \\ 2X \\ 2 \end{cases} \mapsto \begin{cases} i \\ j \\ k \end{cases}$$

Alors, on prend $\sigma_1 = (-1, 0, 1)$. On a l'ensemble

$$\mathrm{Reali}(\sigma_1) = \{x \in \mathbb{R} : X^2 - 1 > 0, 2X < 0, 2 > 0\} = ]-\infty, -1[$$

Et avec les conditions de signe

$$\sigma_2 = (0, -1, 1), \sigma_3 = (-1, -1, 1), \sigma_4 = (-1, 0, 1), \sigma_5 = (-1, 1, 1), \sigma_6 = (0, 1, 1), \sigma_7 = (1, 1, 1).$$

(les autres conditions de signe ne sont pas réalisées). On trouve alors

$$\mathrm{Reali}(\sigma_2) = \{-1\},\ \mathrm{Reali}(\sigma_3) = ]-1, 0[\,,\ \mathrm{Reali}(\sigma_4) = \{0\},$$

$$\mathrm{Reali}(\sigma_5) = ]0, 1[\,,\ \mathrm{Reali}(\sigma_6) = \{1\},\ \mathrm{Reali}_7(\sigma_7) = ]1, +\infty[\,.$$

On obtient alors la décomposition cylindrique algébrique

$$\{]-\infty, -1[\,, \{-1\}, ]-1, 0[\,, \{0\}, ]0, 1[\,, \{1\}, ]1, +\infty[\}.$$

Cette décomposition est bien adaptée à $\mathcal{P}$ donc au polynôme $X^2 - 1$.

**Exemple 6.3.11.** Reprenons l'exemple 6.1.3 où on a considéré

$$\mathcal{P} = \{X^2 + Y^2 - 3\}.$$

Appliquons l'algorithme décrit par le théorème 6.3.9. On trouve $\mathcal{P}_1$ en fermant par dérivation $\mathcal{P}$. On a alors

$$\mathcal{P}_1 = \{X^2 + Y^2 - 3, 2Y, 2\}.$$

Le polynôme constant 2 ne nous apportant aucune information, nous pouvons le supprimer de $\mathcal{P}_2$. De plus, on remplace $2Y$ par $Y$. On remarque également que $\mathrm{Tru}_Y(\mathcal{P}_1) = \mathcal{P}_1$. On trouve alors que $\mathrm{Elim}_Y(\mathcal{P}_1) = \{4X^2 - 12\}$. Étant donné que c'est le signe du polynôme qui nous intéresse, on peut légèrement le simplifier et prendre $\mathrm{Elim}_Y(\mathcal{P}_1) = \{X^2 - 3\}$. Pour trouver $\mathcal{P}_2$, on ferme par dérivation $\mathrm{Elim}_Y(\mathcal{P}_1)$. On a alors

$$\mathcal{P}_2 = \{X^2 - 3, 2X, 2\}.$$

Comme précédemment, on peut retirer le polynôme 2 et remplacer $2X$ par $X$. On a alors

$$\mathcal{P}^* = \{X^2 + Y^2 - 3, Y, X^2 - 3, X\}.$$

Cette famille de polynômes peut alors donner une description semi-algébrique des cellules d'une CAD adaptée au polynôme $X^2 + Y^2 - 3$. Les cellules de la CAD sont les $\mathrm{Reali}(\sigma)$ où $\sigma$ est une condition de signe sur $\mathcal{P}^*$. Il y a 4 polynômes dans $\mathcal{P}^*$, donc on a au plus $3^4 = 81$ cellules.

En pratique, on remarque qu'il y en a 33, pour toutes les autres conditions de signe $\sigma$ sur $\mathcal{P}^*$ on a $\mathrm{Reali}(\sigma) = \emptyset$. Ces 33 cellules sont représentées par les zones délimitées sur la figure 6.5 (les points d'intersection et les courbes qui délimitent les zones sont également des cellules). La CAD qu'on obtient ici est un peu plus complexe que celle donnée dans l'exemple 6.1.3, en effet celle-ci était obtenue à partir de $\{X^2+Y^2-3, X^2-3\}$, ici on rajoute donc les polynômes $X$ et $Y$. La CAD obtenue passe alors de 13 à 33 cellules. Cependant les 13 cellules de cette CAD sont des unions de ces 33 nouvelles cellules qui comprennent 5 points, 16 courbes et 12 régions. Afin de ne pas trop alourdir l'exemple nous allons donner la description semi-algébrique de ces 13 cellules, quitte à les voir comme une union des 33 cellules. On note $\sigma = (i, j, k, l)$ avec $i, j, k, l \in \{-1, 0, 1\}$ la condition de signe $\sigma$ définie par

$$\sigma : \mathcal{P}^* \to \{-1, 0, 1\} : \begin{cases} X^2 - 3 \\ Y^2 + X^2 - 3 \\ X \\ Y \end{cases} \mapsto \begin{cases} i \\ j \\ k \\ l \end{cases}.$$

Détaillons le raisonnement avec une cellule. On a vu dans l'exemple 6.1.3 que

$$C_{11} = ]-\infty, -\sqrt{3}[ \times \mathbb{R}.$$

Cette cellule est donc la réalisation dans $\mathbb{R}^2$ de la formule

$$X^2 - 3 > 0 \wedge X < 0,$$

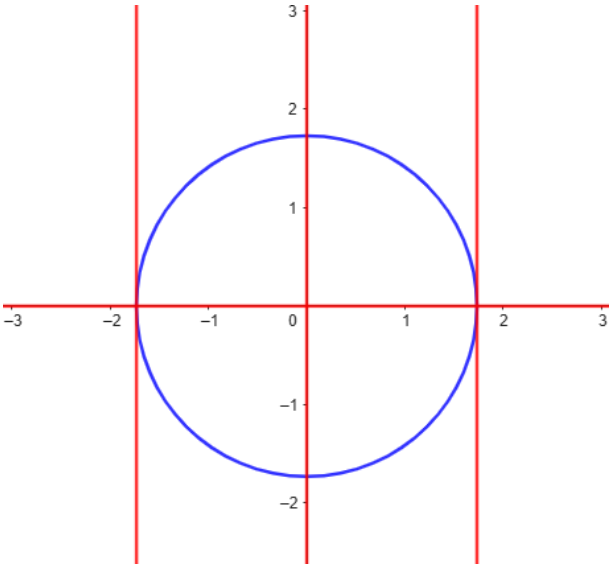


FIGURE 6.5 – CAD adaptée au cercle avec clôture par dérivation.

de plus, $X^2 - 3 > 0$ implique que $Y^2 + X^2 - 3 > 0$. Dès lors,

$$C_{11} = \text{Reali}(1, 1, -1, -1) \cup \text{Reali}(1, 1, -1, 0) \cup \text{Reali}(1, 1, -1, 1).$$

La cellule $C_{11}$ est donc une union de 3 des 33 nouvelles cellules. On procède de la sorte pour chacune des 13 cellules et on trouve alors que

$$\begin{aligned}
C_{11} &= \bigcup_{l\in\{-1,0,1\}} \text{Reali}(1, 1, -1, l), & C_{33} &= \bigcup_{k,l\in\{-1,0,1\}} \text{Reali}(-1, 0, k, l),\\
C_{21} &= \text{Reali}(0, 1, -1, -1), & C_{34} &= \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1, 0, k, 1),\\
C_{22} &= \text{Reali}(0, 0, -1, 0), & C_{35} &= \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1, 1, k, 1),\\
C_{23} &= \text{Reali}(0, 1, -1, 1), & C_{41} &= \text{Reali}(0, 1, 1, -1),\\
C_{31} &= \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1, 1, k, -1), & C_{42} &= \text{Reali}(0, 0, 1, 0),\\
C_{32} &= \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1, 0, k, -1), & C_{43} &= \text{Reali}(0, 1, 1, 1),\\
& & C_{51} &= \bigcup_{l\in\{-1,0,1\}} \text{Reali}(1, 1, 1, l).
\end{aligned}$$

On a donc, au moyen des 33 nouvelles cellules, donné une description semi-algébrique des 13 cellules initiales.

**Exemple 6.3.12.** Reprenons l'exemple 6.3.6. On a

$$\mathcal{P} = \{X^2 + Y^2 - 3, XY - 1\}.$$

En fermant par dérivation, on trouve

$$\mathcal{P}_1 = \{X^2 + Y^2 - 3, 2Y, 2, XY - 1, X\},$$

et comme dans l'exemple précédent, on retire le polynôme 2 et on remplace $2Y$ par $Y$. De plus, on a $\mathrm{Tru}(\mathcal{P}_1) = \mathcal{P}_1 \cup \{-1\}$, on ne garde cependant pas le polynôme $-1$. Comme dans l'exemple 6.2.12, on obtient

$$\mathrm{Elim}_Y(\mathcal{P}_1) = \{X^2 - 3, X^4 - 3X^2 + 1, X\},$$

(dans ce cas-ci, on considère également les polynômes $X$ et $Y$ cependant, $\deg_Y(X) = 0$ donc celui-ci n'apporte rien à l'ensemble $\mathrm{Elim}_Y(\mathcal{P}_1)$ et le seul cas où le polynôme $Y$ intervient est lors du calcul de $\mathrm{sRes}_0(X^2 + Y^2 - 3, Y)$ or on calcule déjà $\mathrm{sRes}_0(X^2 + Y^2 - 3, 2Y)$ donc celui-ci n'apporte rien de nouveau). Afin d'obtenir $\mathcal{P}_2$, on ferme $\mathrm{Elim}_Y(\mathcal{P}_1)$ par dérivation. On a alors

$$\mathcal{P}_2 = \{X^2 - 3, 2X, 2, X^4 - 3X^2 + 1, 4X^3 - 6X, 12X^2 - 6, 24X, 24, X, 1\},$$

avec les simplifications habituelles on obtient

$$\mathcal{P}_2 = \{X^2 - 3, X^4 - 3X^2 + 1, 2X^3 - 3X, 2X^2 - 1, X\}.$$

On considère alors

$$\mathcal{P}^* = \{X^2 + Y^2 - 1, XY - 1, Y, X^2 - 3, X^4 - 3X^2 + 1, 2X^3 - 3X, 2X^2 - 1, X\}.$$

Cet ensemble contient 8 polynômes de $\mathbb{R}[X, Y]$ dont les ensembles d'annulation fournissent une CAD adaptée à $\mathcal{P}$.

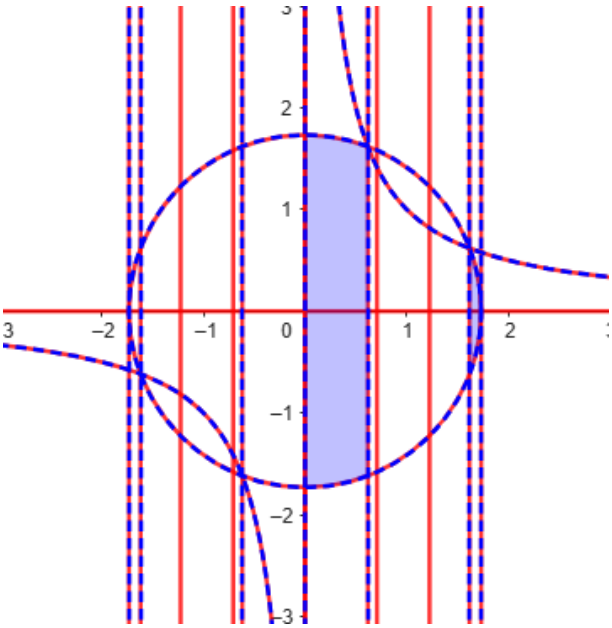


FIGURE 6.6 – CAD adaptée au cercle et à l'hyperbole avec clôture par dérivation.

Dans cette nouvelle CAD, les cellules $C$ et $C'$ considérées dans l'exemple 6.3.6 sont découpées en 3 selon le signe du polynôme $Y$. On trouve alors

$$C = \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1,-1,k,-1,1,-1,-1,1), \tag{6.5}$$

$$C' = \bigcup_{k\in\{-1,0,1\}} \text{Reali}(-1,-1,k,-1,1,1,1,1). \tag{6.6}$$

## 6.4 Élimination des quantificateurs via la CAD

Dans cette section, nous allons expliquer comment effectuer une élimination de quantificateurs en utilisant une décomposition cylindrique algébrique, et nous illustrerons cela par un exemple.

Considérons avoir une formule de la forme

$$\Phi(X_1,\dots,X_n) = \exists Y_1 \in \mathbf{R} \dots \exists Y_m \in \mathbf{R} : \Theta(X_1,\dots,X_n,Y_1,\dots,Y_m).$$

Afin d'effectuer une élimination des quantificateurs, on considère $\mathcal{P}$ l'ensemble des polynômes utilisés dans la formule $\Theta$. On va alors éliminer les variables liées de $\Phi$. Pour ce faire on va appliquer récursivement l'opérateur $\text{Elim}_{Y_k}$ (et la clôture par dérivation, qui est sous-entendue) afin d'obtenir un ensemble de polynômes $\mathcal{P}' \subset \mathbf{R}[X_1,\dots,X_n]$, c'est la phase de projection ou d'élimination.

On effectue alors une CAD de $\mathbf{R}^n$ adaptée à $\mathcal{P}'$. Pour chaque cellule $C$ obtenue, on choisit un point $x \in C \subset \mathbf{R}^n$. On va alors "remonter" la décomposition en ce point $x$. Si on a éliminé (dans l'ordre) la variable $Y_m$ puis $Y_{m-1}$ jusqu'à $Y_1$ alors on considère les polynômes de $\text{Elim}_{Y_2}(\text{Elim}_{Y_3}(\dots(\text{Elim}_{Y_m}(\mathcal{P}))\dots)) \subset \mathbf{R}[X_1,\dots,X_n,Y_1]$ et on les évalue en $x$ afin d'obtenir des polynômes de $\mathbf{R}[Y_1]$. On va alors découper $\{x\}\times\mathbf{R}$ en étudiant les racines des polynômes. De même, pour chaque $x$ précédemment choisi, on prend un point $y_1$ dans chacune des cellules de la décomposition de $\{x\}\times\mathbf{R}$ et on y évalue les polynômes de $\text{Elim}_{Y_3}(\dots(\text{Elim}_{Y_m}(\mathcal{P}))\dots) \subset \mathbf{R}[X_1,\dots,X_n,Y_1,Y_2]$. On répète ainsi l'opération jusqu'à obtenir un point dans chacune des cellules d'une CAD de $\mathbf{R}^{n+m}$ adaptée à $\mathcal{P}$. Toute cette étape de construction est la phase de lifting.

Il reste alors à évaluer chacun des polynômes de $\mathcal{P}$ en chacun des points obtenus dans la phase de lifting (ces points sont de la forme $(x,y_1,\dots,y_m)$). On trouve alors les points $x$ pour lesquels il existe une cellule "au dessus" qui satisfait la formule (phase d'évaluation). Si on a $x^{(1)},\dots,x^{(k)} \in \mathbf{R}^n$ de tels points, on considère les cellules $C_1,\dots,C_k$ de $\mathbf{R}^n$ d'où ces points proviennent. La description de l'union de ces cellules fournit une formule équivalente dans laquelle on retrouve uniquement les variables $X_1,\dots,X_n$.

Illustrons cela au moyen d'un exemple avec $n = m = 1$ en reprenant des polynômes avec lesquels on a déjà travaillé dans ce mémoire.

**Exemple 6.4.1.** Considérons la formule

$$\Phi = \exists Y \in \mathbb{R} : X^2 + Y^2 - 3 < 0 \wedge XY - 1 > 0.$$

L'ensemble de polynômes à considérer est

$$\mathcal{P} = \{X^2 + Y^2 - 3, XY - 1\}.$$

La variable quantifiée de $\Phi$ est $Y$, nous allons l'éliminer. Pour ce faire on applique $\text{Elim}_Y$ et on clôt par dérivation (et on effectue les simplifications habituelles ; on retire les polynômes redondants et on simplifie au maximum ceux qu'on garde). Par l'exemple 6.3.12, on a

$$\mathcal{P}' = \{X^2 - 3, X^4 - 3X^2 + 1, 2X^3 - 3X, 2X^2 - 1, X\}.$$

On note $a < b < c < d$ les racines réelles de $X^4 - 3X^2 + 1$. Les racines des polynômes de $\mathcal{P}'$ sont alors

$$-\sqrt{3} < a < -\sqrt{\frac{3}{2}} < -\sqrt{\frac{1}{2}} < b < 0 < c < \sqrt{\frac{1}{2}} < \sqrt{\frac{3}{2}} < d < \sqrt{3}.$$

Les intervalles déterminés par ces racines fournissent une CAD de $\mathbb{R}$ adaptée à $\text{Elim}_Y(\{X^2 + Y^2 - 3, XY - 1\})$. On va alors, dans chaque cellule de cette décomposition, sélectionner un point $x \in \mathbb{R}$ (les singletons contenant chacune des racines étant des cellules, on doit également les prendre, on a alors 23 points, dont 11 sont les racines des polynômes). Nous allons alors, évaluer nos deux polynômes de départ en chacun de ces points et décomposer $\mathbb{R}$ en fonction de leurs racines. Nous n'allons pas détailler ce qu'il se passe dans chaque cas, mais en donner quelques-uns en exemple. Commençons par regarder ce qu'il se passe dans la cellule $]-\infty, -\sqrt{3}[$. Supposons avoir pris le point $x = -2$. Dès lors, les polynômes de départ deviennent

$$(-2)^2 + Y^2 - 3 = Y^2 + 1 \text{ et } (-2)Y - 1 = -2Y - 1.$$

Le premier polynôme n'admet pas de racine réelle et est toujours positif. On en déduit que la condition ne sera jamais vérifiée, on peut dès lors passer à la cellule, donc au $x$, suivant. Regardons désormais ce qu'il se passe pour la cellule $]\sqrt{\frac{1}{2}}, \sqrt{\frac{3}{2}}[$. Nous y considérons le point $x = 1$, les polynômes deviennent alors

$$1^2 + Y^2 - 3 = Y^2 - 2 \text{ et } 1Y - 1 = Y - 1.$$

On étudie le signe de ces polynômes et on trouve que $Y^2 - 2 < 0$ sur $]-\sqrt{2}, \sqrt{2}[$ et que $Y - 1 > 0$ sur $]1, +\infty[$. On en déduit que la formule de départ est vérifiée lorsque $y \in ]1, \sqrt{2}[$. Dès lors, pour $x \in ]\sqrt{\frac{1}{2}}, \sqrt{\frac{3}{2}}[$, il existe un $y$ tel que la formule est vérifiée.

En procédant de la sorte pour chaque cellule, on trouve que la formule de l'énoncé est vérifiée dans 10 des 23 cellules, qui réunies correspondent à

$$]a, b[ \cup ]c, d[ .$$

Au vu du tableau de signe suivant, on peut obtenir la description semi-algébrique de chacune des cellules. On en déduit alors la description semi-algébrique de l'union de cellules qui nous intéressent, qui est donnée par l'union des descriptions semi-algébriques des cellules.

| $x$ | $-\sqrt{3}$ | $a$ | $-\sqrt{\frac{3}{2}}-\sqrt{\frac{1}{2}}$ | $b$ | $0$ | $c$ | $\sqrt{\frac{1}{2}}$ | $\sqrt{\frac{3}{2}}$ | $d$ | $\sqrt{3}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $X^2-3$ | $+$ | $0$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ |
| $X^4-3X^2+1$ | $+$ | $+$ | $+$ | $0$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ | $0$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ |
| $2X^3-3X$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ | $+$ | $+$ | $0$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ | $+$ | $+$ |
| $2X^2-1$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $0$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ |
| $X$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $-$ | $0$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ |

Après avoir considéré cette union de conditions et supprimé les conditions inutiles (les polynômes $2X^2-1$ et $2X^3-3X$ ne sont pas utiles pour décrire cette union de cellules ; on remarque alors que la clôture par dérivation n'était pas nécessaire dans ce cas très précis), on trouve que $]a,b[\cup]c,d[$ peut être décrit par la formule

$$X^2-3<0\wedge X^4-3X^2+1<0\wedge X\neq 0.$$

Cependant, la condition $X^4-3X^2+1<0$ implique les deux autres. Dès lors, la formule avec quantificateur $\Phi$ est équivalente à la formule sans quantificateur $X^4-3X^2+1<0$, cela s'observe sur la figure 6.8.

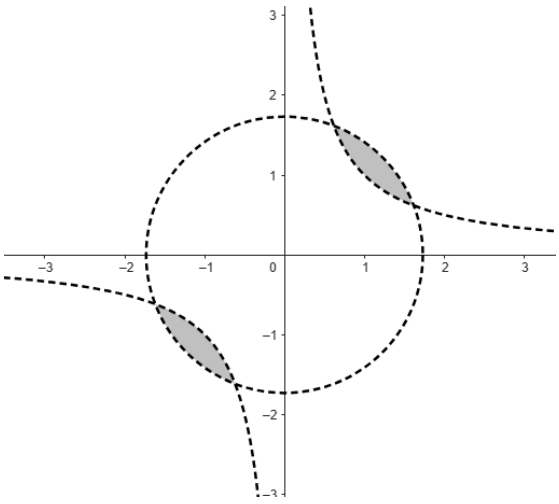


FIGURE 6.7 – Régions vérifiant la formule $X^2+Y^2-3<0\wedge XY-1>0$

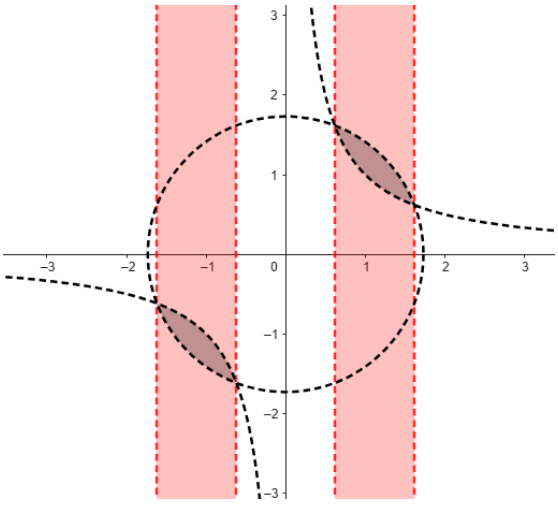


FIGURE 6.8 – Régions vérifiant la formule $X^4-3X^2+1<0$

# Bibliographie


[1] Saugata Basu, Richard Pollack et Marie-Françoise Roy. *Algorithms in real algebraic geometry*. Second. T. 10. Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 2006, p. x+662. ISBN : 978-3-540-33098-1.

[2] Jacek Bochnak, Michel Coste et Marie-Françoise Roy. *Real algebraic geometry*. T. 36. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Translated from the 1987 French original, Revised by the authors. Springer-Verlag, Berlin, 1998, p. x+430. ISBN : 3-540-64663-9. DOI : 10.1007/978-3-662-03718-8. URL : https://doi.org/10.1007/978-3-662-03718-8.

[3] Gregory W. Brumfiel. « Affine semi-algebraic sets ». In : *Partially Ordered Rings and Semi-Algebraic Geometry*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1979, p. 162-267.

[4] B. F. Caviness et J. R. Johnson, éd. *Quantifier elimination and cylindrical algebraic decomposition*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1998, p. xx+431. ISBN : 3-211-82794-3. DOI : 10.1007/978-3-7091-9459-1. URL : https://doi.org/10.1007/978-3-7091-9459-1.

[5] Emilie Charlier. *Théorie de Galois*. Notes de cours, Université de Liège. 2024.

[6] George E. Collins. « Quantifier elimination for real closed fields by cylindrical algebraic decomposition ». In : *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*. T. Vol. 33. Lecture Notes in Comput. Sci. Springer, Berlin-New York, 1975, p. 134-183.

[7] Serge Lang. *Algebra*. third. T. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, p. xvi+914. ISBN : 0-387-95385-X. DOI : 10.1007/978-1-4613-0041-0. URL : https://doi.org/10.1007/978-1-4613-0041-0.

[8] Julien Leroy. *Structure algébrique*. Notes de cours, Université de Liège. 2023.

[9] Pierre Mathonet. *Mathématiques élémentaires*. Notes de cours, Université de Liège. 2019.

[10] Bhubaneswar Mishra. *Algorithmic Algebra*. Monographs in Computer Science. New York : Springer, 1993. ISBN : 978-0-387-94090-8.

[11] Michel Rigo. *Algèbre linéaire*. Notes de cours, Université de Liège. 2009.