Licence Sciences, Technologies, Santé
Parcours de mathématiques
Université Claude Bernard Lyon 1

ALGÈBRE APPLIQUÉE

INTRODUCTION AUX BASES DE GRÖBNER ET À LEURS APPLICATIONS

—

- Notes de cours et de travaux dirigés -

– Printemps 2014 –

PHILIPPE MALBOS

THOMAS BLOSSIER

(version 2)

Table des matières

CHAPITRE
I

Préliminaires algébriques

Sommaire

Ce chapitre contient peu de démonstrations, son rôle est de fixer les notations et de rappeler les structures algébriques fondamentales, ainsi que les principaux résultats algébriques que nous utiliserons dans ce cours. Nous renvoyons le lecteur au cours de première année pour tout approfondissement.

§ 1 Ensembles et applications

I.1.1. Applications.— Soient A et B deux ensembles. Une *application* f de A dans B est un procédé qui à tout élément x de A associe un élément unique de B, noté $f(x)$. On note $f : A \longrightarrow B$, ou $A \xrightarrow{f} B$, ou encore

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longrightarrow f(x). \end{aligned}$$

On note $f(A)$ l'image de l'ensemble A, définie par

$$f(A) = \{y \mid y \in B,\ \exists\, x \in A, \text{ tel que } y = f(x)\}.$$

L'image inverse d'un sous-ensemble $Y \subset B$ est définie par

$$f^{-1}(Y) = \{x \mid x \in A,\ f(x) \in Y\}.$$

Une application $f : A \longrightarrow B$ est dite *injective* si pour tout $x,\ y \in A$, on a $f(x) = f(y)$ implique $x = y$. Elle est dite *surjective* si $f(A) = B$, *i.e.*, pour tout $y \in B$, il existe un $x \in A$ tel que $y = f(x)$. Une application est dite *bijective* si elle est à la fois injective et surjective.

Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont deux applications, on note $g \circ f$, ou encore gf, l'application, dite *composée*, définie par

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ x &\longrightarrow g(f(x)). \end{aligned}$$

La composée des applications est une opération associative, i.e., étant données trois applications $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, on a

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

I.1.2. Ensembles de nombres.— Dans tout ce cours, nous supposons connus les ensembles de nombres suivants et les opérations d'addition, de soustraction, de multiplication et de division sur ces ensembles :

- l'ensemble des entiers naturels, 0, 1, 2, ..., noté $\mathbb{N}$,
- l'ensemble des entiers relatifs, noté $\mathbb{Z}$, formé des entiers naturels et de leurs opposés, -1, -2, ...,
- l'ensemble des rationnels, noté $\mathbb{Q}$, formé des quotients $\frac{p}{q}$, où p et q sont des entiers relatifs, avec q non nul,
- l'ensemble des réels, noté $\mathbb{R}$, qui contient les nombres rationnels et les nombres irrationnels,
- l'ensemble des complexes, noté $\mathbb{C}$, formé des nombres $a + ib$, où a et b sont des réels et i un complexe vérifiant $i^2 = -1$.

Si p et q sont deux entiers relatifs, on notera

$$[\![p, q]\!] = \{a \in \mathbb{Z} \mid p \leq a \leq q\}.$$

§ 2 Les corps

Un *corps* est un objet algébrique constitué d'un ensemble et de deux opérations sur cet ensemble, une addition et une multiplication, qui satisfont à certaines relations. Intuitivement, cette structure est proche de notre intuition de nombres et des opérations que l'on peut leur appliquer. Avant d'énoncer les relations des deux opérations de la structure de corps, rappelons la structure de groupe.

I.2.1. Les groupes.— Un *groupe* est un ensemble G muni d'une opération $\star$, associant à deux éléments a et b de G un troisième élément de G, noté $a \star b$, satisfaisant les assertions suivantes

i) l'opération est *associative*, *i.e.*, pour tous éléments a, b et c de G,

$$a \star (b \star c) = (a \star b) \star c,$$

ii) il existe un élément e dans G, appelé *neutre*, tel que, pour tout élément a de G,

$$a \star e = e \star a = a,$$

iii) pour tout élément a de G, il existe un élément *inverse*, que nous noterons a^{-1}, tel que

$$a \star a^{-1} = e = a^{-1} \star a.$$

Exercice 1. —

1. Montrer qu'un groupe possède un unique élément neutre.
2. Montrer que dans un groupe, l'inverse d'un élément est unique.

I.2.2. Exemples.—

1) Le groupe *trivial* est le groupe à un seul élément, l'élément neutre.

2) L'ensemble des entiers $\mathbb{Z}$ forme un groupe pour l'addition usuelle. Il ne forme pas un groupe pour la multiplication.

3) L'ensemble des nombres rationnels $\mathbb{Q}$ forme un groupe pour l'addition. L'ensemble $\mathbb{Q} - \{0\}$ des nombres rationnels non nul est un groupe pour la multiplication.

4) L'ensemble des complexes non nuls $\mathbb{C} - \{0\}$, muni de la multiplication usuelle des complexes.

5) L'ensemble $\mathbb{R}^n$ des n-uplets ordonnées

$$(x_1, \ldots, x_n)$$

de nombres réels, muni de l'opération

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

forme un groupe.

Exercice 2. — Justifier toutes les propriétés précédentes. Dans le cas de $\mathbb{R}^n$, déterminer l'élément neutre du groupe et l'inverse d'un n-uplet $(x_1, \ldots, x_n)$.

I.2.3. Les groupes abéliens.— Un groupe est dit *abélien*, ou *commutatif*, si tous éléments a et b vérifient

$$a \star b = b \star a.$$

Les groupes des exemples I.2.2 sont abéliens.

Exercice 3. — Soit X un ensemble.

1. Montrer que l'ensemble des permutations de X, i.e. des bijections de X dans lui-même, forment un groupe.
2. Montrer que ce groupe n'est pas commutatif lorsque X possède au moins trois éléments.

I.2.4. Les corps.— Un *corps* (commutatif) est un ensemble $\mathbb{K}$ sur lequel une opération d'addition $(a, b) \to a + b$ et une opération de multiplication $(a, b) \to ab$ sont définies et satisfont aux assertions suivantes :

i) $\mathbb{K}$ est un groupe abélien pour l'addition,

ii) $\mathbb{K} - \{0\}$ est un groupe abélien pour la multiplication,

iii) la multiplication est distributive par rapport à l'addition, i.e., pour tous éléments a, b et c, on a

$$a(b + c) = ab + ac.$$

L'élément neutre pour l'addition, appelé *zero*, est noté 0, l'inverse de a est appelé l'*opposé* de a et noté $-a$, l'élément neutre pour la multiplication est appelé *unité* et noté 1, l'*inverse* de a pour la multiplication est noté a^{-1}.

I.2.5. Exemples.—

1) L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$, munis des opérations d'addition et de multiplication usuelles sont des corps.

2) L'ensemble $\mathbb{Z}$ des entiers relatifs n'est pas un corps.

3) Un exemple de corps fini, i.e., avec un nombre fini d'éléments, est donné par l'ensemble, noté $\mathbb{Z}/p\mathbb{Z}$, des entiers modulo un entier premier p, muni des opérations d'addition et de multiplication induites de celles de $\mathbb{Z}$.

Exercice 4. — Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps.

Exercice 5. — Montrer que dans un corps, l'élément neutre de l'addition joue le rôle d'*annulateur*, i.e., pour tout élément a, on a :

$$a0 = 0.$$

Par définition, un groupe ne peut être vide, il contient au moins un élément. Un corps contient donc au moins deux éléments 0 et 1 qui sont nécessairement distincts.

Exercice 6. — Montrer qu'un corps ne contient pas de diviseur de zero, c'est-à-dire que si a et b sont deux éléments non nul d'un corps $\mathbb{K}$, alors leur produit ab est non nul.

Il n'existe qu'un seul corps à deux éléments (à isomorphisme près), noté $\mathbb{F}_2$.

Exercice 7. — Établir les tables d'addition et de multiplication du corps à deux éléments.

I.2.6. Extension de corps.— Un sous-ensemble $\mathbb{L}$ d'un corps $\mathbb{K}$ est un *sous-corps* de $\mathbb{K}$ si les opérations du corps $\mathbb{K}$ munissent $\mathbb{L}$ d'une structure de corps. On dit alors que $\mathbb{K}$ est une *extension* du corps $\mathbb{L}$. Par exemple, le corps des réels $\mathbb{R}$ est une extension du corps des rationnels $\mathbb{Q}$ et le corps des complexes $\mathbb{C}$ est une extension du corps $\mathbb{R}$.

§ 3 Les anneaux

La structure d'anneau généralise celle de corps. Un ensemble muni d'une opération d'addition et d'une opération de multiplication qui satisfont à tous les axiomes de corps, excepté l'existence d'un élément inverse a^{-1}, pour tout élément a non nul, est appelé un *anneau commutatif*. Pour que notre définition soit complète, on convient, qu'il existe un anneau qui possède un seul élément.

Par exemple, l'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication, n'est pas un corps - les éléments non nuls ne sont pas tous inversibles - mais il forme un anneau commutatif. Nous verrons que l'ensemble $A[x]$ des polynômes à une indéterminée à coefficients dans un anneau ou un corps A forme un anneau ; les principales constructions sur les anneaux de polynômes sont rappelées dans la section suivante.

I.3.1. Les anneaux.— Un *anneau* est un ensemble A muni d'une opération d'*addition* $(a,b) \to a+b$ et d'une opération de *multiplication* $(a,b) \to ab$ qui satisfont aux assertions suivantes

i) A est un groupe abélien pour l'addition,

ii) la multiplication est associative, i.e., pour tous éléments a, b et c de A,

$$(ab)c = a(bc).$$

iii) la multiplication possède un élément neutre dans A, appelé *unité* et noté 1, vérifiant pour tout élément a de A,

$$1a = a1 = a.$$

iv) la multiplication est *distributive* par rapport à l'addition, i.e., pour tous éléments a,b,c de A, on a :

$$a(b+c) = ab+ac, \qquad (b+c)a = ba+ca.$$

Un anneau est dit *commutatif* si sa multiplication est commutative.

Exercice 8. — Montrer que dans un anneau A, on a, pour tous éléments a et b,

1. $0a = a0 = 0$,
2. $(-1)a = -a$,
3. $-(ab) = (-a)b = a(-b)$,
4. $(-a)(-b) = ab$.

I.3.2. Exemples.—

1) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, forme un anneau commutatif.

2) Un corps (commutatif) est un anneau $\mathbb{K}$ non réduit à $\{0\}$, tel que la multiplication muni $\mathbb{K} - \{0\}$ d'une structure de groupe abélien.

3) Si $1 = 0$ dans un anneau A, alors A est réduit à $\{0\}$, car pour tout élément a de A, $a = 1a = 0a = 0$.

I.3.3. Endomorphismes d'un groupe abélien.— Rappelons qu'un *endomorphisme* d'un groupe $(G,\star)$ est un morphisme de groupes de G dans lui-même, c'est-à-dire, une application $f : G \longrightarrow G$ vérifiant, pour tous $a,b \in G$,

$$f(a \star b) = f(a) \star f(b).$$

L'ensemble des endomorphismes d'un groupe abélien $(G,+)$, muni de l'addition induite de celle sur G et de la composition, est un anneau non commutatif en général.

I.3.4. Formule du binôme.— Dans un anneau, si deux éléments a et b commutent, i.e., $ab = ba$, alors on a la formule dite du *binôme de Newton*, pour tout entier naturel n,

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}.$$

Exercice 9. — Démontrer la formule du binôme de Newton.

I.3.5. Caractéristique d'un anneau commutatif.— Soit A un anneau commutatif. La *caractéristique* de A est le plus petit entier naturel non nul q, tel que l'addition de q fois l'unité soit égale à zero :

$$q.1 = \underbrace{1+1+\ldots+1}_{q \text{ fois}} = 0.$$

Si un tel entier n'existe pas, on dit que l'anneau est de caractéristique nulle.

Exercice 10. —

1. Montrer qu'un anneau commutatif fini est de caractéristique non nulle.
2. Montrer que la caractéristique d'un corps fini est un nombre premier.

Exercice 11. — Construire un corps de caractéristique 3.

Exercice 12. — Montrer que dans un anneau commutatif de caractéristique un nombre premier p, alors, pour tous éléments a et b de A, on a

$$(a+b)^p = a^p + b^p.$$

I.3.6. Division euclidienne dans l'anneau $\mathbb{Z}$.— La *division euclidienne* est un résultat fondamental de l'arithmétique élémentaire sur les entiers ou les polynômes. Avant d'identifier les anneaux dans lesquels, un tel algorithme est disponible, rappelons la division euclidienne sur les entiers.

I.1 Théorème (division euclidienne). — Soient $a, b \in \mathbb{Z}$, avec $b > 0$. Il existe un couple unique (q, r) d'entiers dans $\mathbb{Z}$ tel que :

$$a = bq + r, \quad \text{avec } 0 \leq r < b.$$

L'entier q est appelé le *quotient* de la division euclidienne de a par b et l'entier r est appelé le *reste* de la division euclidienne de a par b.

Preuve. Montrons dans un premier temps l'unicité du couple. Supposons que (q, r) et (q', r') soient deux couples vérifiant la condition, alors

$$a = bq + r = bq' + r'.$$

D'où $r' - r = b(q - q')$, par suite b divise $r' - r$. Comme, par hypothèse, $0 \leq r < b$ et $0 \leq r' < b$, on a

$$b|q - q'| = |r' - r| < b.$$

Par suite, $|q - q'| = 0$, d'où $q = q'$ et $r = r'$.

Montrons l'existence du couple. Considérons l'ensemble $A = \{k \in \mathbb{Z} \mid bk \leq a\}$. C'est une partie non vide et majorée de $\mathbb{Z}$. En effet, si $a \geq 0$, alors $0 \in A$, d'où A est non vide, et comme $1 \leq b$, l'entier a majore A. Si $a < 0$, alors $a \in A$, d'où A est non vide et 0 majore A. Par suite, l'ensemble A admet un plus grand élément q. On a

$$bq \leq a < b(q+1).$$

En posant $r = a - bq$, on a $0 \leq r < b$. □

De l'unicité du quotient et du reste de la division euclidienne, on déduit qu'un entier b divise un entier a si, et seulement si, le reste de division euclidienne de a par b est nul.

Exercice 13. — Soit n un entier naturel. Calculer la division euclidienne de

1. l'entier n^3+n^2+2n+1 par $n+1$,
2. l'entier $n^4+4n^3+6n^2$ par n^2+2.

FIGURE I.1.: Euclide de Samos (325 - 265 av. J.-C.)

Euclide est un mathématicien de la Grèce antique né vers 325 av. J.C. et mort vers 265 av. J.C.. Nous n'avons que très peu d'information sur la vie d'Euclide. L'article de Fabio Acerbi du site Image des mathématiques [1] *présente ce que nous savons à ce jour sur le personnage d'Euclide. Euclide est l'auteur des* Éléments *qui est un texte fondateur de la géométrie.*

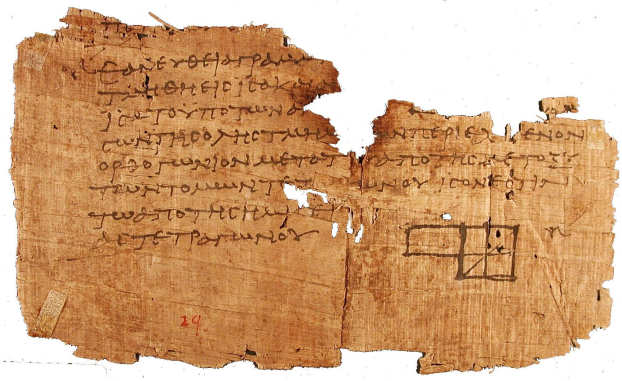


FIGURE I.2.: Un fragment des éléments d'Euclide, papyrus daté d'entre 75 et 125 de notre ère.

I.3.7. Les anneaux euclidiens.— Soit A un anneau commutatif. On appelle *algorithme euclidien* sur A toute application

$$\varphi : A-\{0\} \longrightarrow \mathbb{N},$$

telle que, pour tout $a \in A$ et tout $b \in A-\{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq+r, \quad \text{avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

1. Fabio Acerbi, « Euclide » - Images des Mathématiques, CNRS, 2010. En ligne, URL : `http://images.math.cnrs.fr/Euclide.html`

Un anneau commutatif A est dit *euclidien*, s'il vérifie les deux propriétés suivantes

i) A est *intègre*, i.e., pour tous éléments a et b de A,

$$ab = 0 \Rightarrow (\, a = 0 \text{ ou } b = 0\,).$$

ii) il existe sur A un algorithme euclidien.

I.3.8. Exemple.— L'anneau $\mathbb{Z}$ est euclidien. Il est en effet intègre et l'application valeur absolue $|\,|\,:\mathbb{Z}-\{0\}\longrightarrow\mathbb{N}$ est un algorithme euclidien, car, pour tout $a\in\mathbb{Z}$ et tout $b\in\mathbb{Z}-\{0\}$, il existe $q,r\in\mathbb{Z}$ tels que

$$a = bq + r, \quad \text{avec } |r| < |b| \text{ ou } r = 0.$$

Attention, le couple (q,r) n'est pas ici unique, par exemple, on a

$$5 = (-3)(-2) + (-1) \text{ avec } |-1| < |-3|,$$

et

$$5 = (-3)(-1) + 2 \text{ avec } |2| < |-3|.$$

Dans la suite, nous montrerons que si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

Exercice 14. — Montrer que l'anneau $\mathbb{D}$ des nombres décimaux, i.e., le sous-anneau de $\mathbb{Q}$, engendré par $1/10$, est euclidien.

I.3.9. Les idéaux.— Soit A un anneau commutatif. Un sous-ensemble I de A est appelé *idéal* de A, s'il vérifie les assertions suivantes

i) $0\in I$,

ii) si $u,v\in I$, alors $u+v\in I$,

iii) si $a\in A$ et $u\in I$, alors $au\in I$.

En particulier un idéal est un sous-groupe abélien de A pour l'addition.

Exercice 15. — Montrer que $\{0\}$ et A sont des idéaux de A.

Exercice 16. — Montrer que les idéaux de l'anneau $\mathbb{Z}$ des entiers relatifs sont les $n\mathbb{Z}$, où n est un entier naturel.

Dans la suite de ce cours, nous verrons quelques propriétés remarquables sur les idéaux des anneaux euclidiens. En particulier, nous montrerons que tout idéal d'un anneau euclidien est engendré par un élément. La notion d'idéal est centrale dans ce cours, nous la considérerons plus particulièrement dans le contexte des anneaux de polynômes à plusieurs indéterminées.

§ 4 Les polynômes à une indéterminée

I.4.1. Polynômes sur un corps.— Avant d'aborder la notion de polynôme, rappelons qu'il est important de distinguer les polynômes des fonctions polynomiales. En effet, considérons le polynôme $f = x^2 - x$ à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$. La fonction polynomiale associée $\widetilde{f}:\mathbb{Z}/2\mathbb{Z}\longrightarrow\mathbb{Z}/2\mathbb{Z}$, définie par

$$\widetilde{f}(a) = a^2 - a, \text{ pour tout } a\in\mathbb{Z}/2\mathbb{Z},$$

est nulle, car $\widetilde{f}(0) = 0$ et $\widetilde{f}(1) = 0$, alors que le polynôme f n'est pas nul.

Exercice 17. — Montrer qu'il n'existe que quatre fonctions polynomiales à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$ et une infinité de polynômes à coefficients dans ce corps.

La situation est différente pour les polynômes à coefficients dans les corps infinis, dans ce cas, il existe une correspondance biunivoque entre les polynômes et les fonctions polynomiales, cf. section I.4.5.

I.4.2. Les polynômes.— Soit $\mathbb{K}$ un corps. On appelle *polynôme* à coefficients dans $\mathbb{K}$, toute suite $f = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$, nulle à partir d'un certain rang. On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble de ces suites.

On définit sur l'ensemble $\mathbb{K}^{(\mathbb{N})}$ une addition et un produit externe par un scalaire en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$, $g = (b_n)_{n\in\mathbb{N}}$ et $\lambda \in \mathbb{K}$,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}}, \qquad \lambda f = (\lambda a_n)_{n\in\mathbb{N}}.$$

En outre, on définit une multiplication en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$, $g = (b_n)_{n\in\mathbb{N}}$,

$$fg = (c_n)_{n\in\mathbb{N}}, \qquad \text{avec} \qquad c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

I.4.3. L'algèbre des polynômes.— Ces trois opérations munissent l'ensemble $\mathbb{K}^{(\mathbb{N})}$ d'une structure de $\mathbb{K}$-*algèbre* associative, commutative et unitaire, c'est-à-dire,

i) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et du produit par un scalaire est un $\mathbb{K}$-espace vectoriel,

ii) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et de la multiplication est un anneau commutatif,

iii) pour tous $f, g \in \mathbb{K}^{(\mathbb{N})}$ et tous scalaires $\lambda, \mu \in \mathbb{K}$, on a

$$(\lambda f)(\mu g) = (\lambda\mu)(fg).$$

I.4.4. Notion d'indéterminée.— L'écriture des polynômes sous forme de suite est peu manipulable, aussi, on préfère la notation basée sur la notion d'*indéterminée*. Notons x le polynôme de $\mathbb{K}^{(\mathbb{N})}$ dont tous les termes sont nuls, sauf celui de degré 1 :

$$x = (0, 1, 0, \ldots).$$

Par convention, on pose $x^0 = 1$. On définit les puissances de x par récurrence, pour tout entier k, $x^{k+1} = xx^k$. Ainsi, si $f = (a_n)_{n\in\mathbb{N}}$, on montre que

$$f = \sum_{i=0}^{+\infty} a_i x^i.$$

Les scalaires a_i sont appelés les *coefficients* du polynôme f. On montre que deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients :

$$\sum_{k=0}^{+\infty} a_k x^k = \sum_{k=0}^{+\infty} b_k x^k \quad \text{si, et seulement si,} \quad a_k = b_k, \text{ pour tout } k \in \mathbb{N}.$$

On notera alors $\mathbb{K}[x]$ l'ensemble des *polynômes à une indéterminée* à coefficients dans le corps $\mathbb{K}$. Avec ces notations, l'addition des polynômes est définie de la façon suivante, pour

$f = \sum_{i=0}^{m} a_i x^i$ et $g = \sum_{j=0}^{n} b_j x^j$, alors

$$f+g = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k)x^k,$$

avec $a_k = 0$, pour $k > m$ et $b_k = 0$ pour $k > n$. Par ailleurs, pour la multiplication, on a

$$fg = \sum_{k=0}^{m+n} \left(\sum_{\substack{i,j\geq 0 \\ i+j=k}} (a_i b_j) \right) x^k$$

I.4.5. Fonction polynomiale.— Étant donné un polynôme $f = \sum_{i=0}^{n} a_i x^i$ de $\mathbb{K}[x]$, on définit la *fonction polynomiale* associée comme l'application

$$\widetilde{f} : \mathbb{K} \longrightarrow \mathbb{K},$$

qui, à tout $a \in \mathbb{K}$, associe le scalaire $f(a) \in \mathbb{K}$, obtenu en remplaçant dans l'expression de f l'indéterminée x par a.

Nous avons vu en I.4.1 que sur un corps fini, les notions de polynômes et de fonction polynomiale ne coïncident pas. Nous allons voir que c'est le cas lorsque le corps est infini, par exemple lorsque $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

Exercice 18. — Supposons que $\mathbb{K}$ est le corps $\mathbb{R}$ ou $\mathbb{C}$.

1. Montrer que l'application
$$\varphi : \mathbb{K}[x] \longrightarrow \mathbb{K}^{\mathbb{K}}$$
définie par $\varphi(f) = \widetilde{f}$ est injective.
2. Montrer que deux polynômes à coefficients dans $\mathbb{K}$ sont égaux si, et seulement si leurs fonctions polynomiales associées sont égales.

I.4.6. Degré d'un polynôme.— Soit f un polynôme de $\mathbb{K}[x]$. Si $f = 0$, on pose $\deg(f) = -\infty$, si $f = \sum_{i=0}^{m} a_i x^i$ est non nul, on note $\deg(f)$ le plus grand entier naturel n tel que a_n soit non nul. L'entier $\deg(f)$ est appelé le *degré* du polynôme f.

Un polynôme non nul f de degré $n \geq 0$ s'écrit de façon unique sous la forme

$$f = a_0 + a_1 x + \ldots + a_n x^n,$$

où a_n est non nul. Le degré de f est le plus grand exposant de x apparaissant dans f.

I.4.7. Les monômes.— On appellera *monôme* un polynôme de la forme x^k, où k est un entier naturel. La famille de monômes $(x^n)_{n\in N}$ forme une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[x]$. On l'appelle base canonique de $\mathbb{K}[x]$.

I.4.8. Terme de plus haut degré.— Le *coefficient de plus haut degré* (*leading coefficient*) d'un polynôme f de $\mathbb{K}[x]$, noté $\mathrm{lc}(f)$, est le coefficient du monôme de plus grand exposant. Le *terme*

de plus haut degré d'un polynôme f (*leading term*), noté $\mathrm{lt}(f)$, est le terme de plus haut degré de f. Par exemple, pour le polynôme $f = a_0 + a_1x + \ldots + a_nx^n$, on a

$$\deg(f) = n, \quad \mathrm{lt}(f) = a_nx^n, \quad \mathrm{lc}(f) = a_n.$$

Un polynôme est dit *unitaire*, si le coefficient de son terme de plus haut degré est égal à 1.

Exercice 19. — Montrer que pour tous polynômes f et g de $\mathbb{K}[x]$, on a

1. $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$,
2. $\mathrm{lt}(fg) = \mathrm{lt}(f)\,\mathrm{lt}(g)$.

§ 5 Arithmétique des polynômes

I.5.1. Divisibilité.— Soient f et g deux polynômes de $\mathbb{K}[x]$. On dit que g *divise* f, ou que f est *divisible* par g, ou encore que f est un multiple de g, s'il existe un polynôme q de $\mathbb{K}[x]$ tel que $f = gq$. On note alors $g|f$.

Exercice 20. — Montrer que le polynôme $x+3$ divise le polynôme x^3+27.

Exercice 21. — Montrer que pour deux polynômes f et g non nuls de $\mathbb{K}[x]$, $\deg(f) \leq \deg(g)$ si, et seulement si, $\mathrm{lt}(f) \mid \mathrm{lt}(g)$.

Exercice 22. — Soient f et g deux polynômes de $\mathbb{K}[x]$. Montrer que $f|g$ et $g|f$ si, et seulement si, il existe un scalaire non nul λ de $\mathbb{K}$ te que $f = \lambda g$.

I.5.2. La division euclidienne dans $\mathbb{K}[x]$.— Il existe sur l'anneau $\mathbb{K}[x]$ une division euclidienne comme celle que nous avons vue sur l'anneau $\mathbb{Z}$. Par exemple, considérons deux polynômes

$$f = x^3 - 3x^2 + 4x + 7, \qquad g = 2x^2 + 4x + 6,$$

de $\mathbb{Q}[x]$. La division de f par g a pour quotient $\frac{1}{2}x - \frac{5}{2}$ et pour reste $11x+22$. On les obtient en procédant de la même façon que la division des entiers :

$$\begin{array}{rrrr|l} x^3 & -3x^2 & +4x & +7 & 2x^2+4x+6 \\ \cline{5-5} x^3 & +2x^2 & +3x & & \frac{1}{2}x - \frac{5}{2} \\ \cline{1-4} & -5x^2 & +x & +7 & \\ & -5x^2 & -10x & -15 & \\ \cline{2-4} & & 11x & +22 & \end{array}$$

La première étape consiste à multiplier le polynôme g par $\frac{1}{2}x$, puis à soustraire le résultat à f, soit

$$f - \frac{x^3}{2x^2}g = f - \frac{1}{2}xg = -5x^2 + x + 7.$$

L'idée consiste à multiplier g par un terme, ici $\frac{x^3}{2x^2}$, de telle façon que le terme de plus haut degré de g multiplié par ce terme annule le terme de plus haut degré de f. On obtient ainsi un nouveau polynôme $h = -5x^2 + x + 7$, on dit que h est une *réduction* de f par g, on note

$$f \xrightarrow{g} h.$$

On répète alors ce processus, jusqu'à obtenir le reste

$$r = h - (-\frac{5}{2})g = 11x + 22.$$

La division se compose ainsi d'une suite de réductions par g :

$$f \xrightarrow{g} h \xrightarrow{g} r.$$

I.5.3. Le cas général.— Plus généralement, considérons deux polynômes

$$f = a_n x^n + \ldots + a_1 x + a_0, \quad g = b_m x^m + \ldots + b_1 x + b_0,$$

avec $\deg(f) = n \geq \deg(g) = m$. La première étape dans la division de f par g consiste à soustraire à f le produit

$$\frac{a_n}{b_m} x^{n-m} g,$$

qui, avec les notations définies en I.4.8, s'écrit

$$\frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g.$$

On obtient ainsi comme premier reste le polynôme

$$h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g.$$

On dit que f se *réduit* en h par g, on note

$$f \xrightarrow{g} h.$$

On répète alors l'opération de réduction par g, pour obtenir un nouveau reste :

$$h' = h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(g)} g.$$

Dans la réduction $f \xrightarrow{g} h$, on notera que le reste h a un degré strictement inférieur au degré de f. On peut alors poursuivre le processus de réduction, jusqu'à obtenir un reste, dont le degré est strictement inférieur au degré du polynôme g. On obtient ainsi une suite de réductions par g qui termine sur un reste r, tel que $\deg(r) < \deg(g)$:

$$f \xrightarrow{g} h \xrightarrow{g} h' \xrightarrow{g} \ldots \xrightarrow{g} r.$$

On montre ainsi l'existence du quotient et du reste dans le théorème suivant :

I.2 Théorème (division euclidienne). — Soient f et g deux polynômes de $\mathbb{K}[x]$, avec $g \neq 0$. Il existe un couple unique (q, r) de polynômes de $\mathbb{K}[x]$ tel que :

$$f = gq + r,$$

avec $\deg(r) < \deg(g)$.

Le polynôme q est appelé le *quotient* de la division euclidenne de f par g et le polynôme r est appelé le *reste* de la division euclidenne de f par g. Si le reste de la division euclidienne de f par g est nul, alors le polynôme g divise f.

Exercice 23. — Montrer l'unicité des polynômes q et r.

Exercice 24. — Étant donnés deux éléments distincts a et b d'un corps $\mathbb{K}$. Calculer le reste de la division euclidienne d'un polynôme f de $\mathbb{K}[x]$ par le polynôme $(x-a)(x-b)$ en fonction de $f(a)$ et $f(b)$.

Exercice 25. — Calculer le reste de la division de f par g avec

1. $f = x^3+x^2+x+1,\ g = x+1$,
2. $f = x^3+x^2+x+1,\ g = x-1$,
3. $f = x^3+3x^2-7x+5,\ g = x^2-3$,
4. $f = x^4+2x^3-4x^2+5,\ g = x^3+5$.

I.3 Théorème. — Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

Preuve. D'après le théorème I.2, l'application $\deg(:)\,\mathbb{K}[x]-\{0\} \longrightarrow \mathbb{N}$ est un algorithme euclidien sur $\mathbb{K}[x]$. □

ENTRÉE : $f, g \in \mathbb{K}[x]$ avec $g \neq 0$,
SORTIE : $q, r \in \mathbb{K}[x]$ tels que $f = gq + r$ avec $\big(r = 0$ ou $\deg(r) < \deg(g)\big)$.
INITIALISATION : $q := 0$; $r := f$
TANT QUE : $r \neq 0$ **ET** $\deg(g) \leq \deg(r)$ **FAIRE**

$$q := q + \frac{\mathrm{lt}(r)}{\mathrm{lt}(g)}$$
$$r := r - \frac{\mathrm{lt}(r)}{\mathrm{lt}(g)} g.$$

Algorithme de la division des polynômes d'une indéterminée.

Nous reviendrons sur cet algorithme de la division dans un prochain chapitre, en particulier pour ses nombreuses applications.

I.5.4. Polynômes premiers entre eux.— Deux polynômes sont dits *premiers entre eux*, si leurs seuls diviseurs communs sont les polynômes de degré nul. Plus généralement, des polynômes $f_1, \ldots, f_s$ de $\mathbb{K}[x]$ sont dits

- *premiers entre eux dans leur ensemble*, si les seuls polynômes qui divisent simultanément les polynômes $f_1, \ldots, f_s$ sont de degré nul,
- *premiers entre eux deux à deux*, si, pour tout i différent de j, les polynômes f_i et f_j sont premiers entre eux.

Si f_i et f_j sont premiers entre eux, alors les polynômes $f_1, \ldots, f_i, \ldots, f_j, \ldots, f_s$ sont premier entre eux dans leur ensemble. Attention, les polynômes $f_1 = x-1$, $f_2 = (x-1)(x-2)$ et $f_3 = x-3$ sont premiers entre eux dans leur ensemble, alors que les polynômes f_1 et f_2 ne sont pas premiers entre eux.

I.4 Théorème (Identité de Bézout). — Les polynômes $f_1, \ldots, f_s \in \mathbb{K}[x]$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe des polynômes $u_1, \ldots, u_s$ de $\mathbb{K}[x]$, tels que

$$u_1 f_1 + \cdots + u_s f_s = 1.$$

L'égalité $u_1 f_1 + \cdots + u_s f_s = 1$ s'appelle une *identité de Bézout*.

I.5.5. Exemples.— Les polynômes $x-1$ et $x+2$ sont premiers entre eux, on a l'identité de Bézout

$$-\frac{1}{3}(x-1) + \frac{1}{3}(x+2) = 1.$$

Les polynômes x^2-1 et $x+2$ sont premiers entre eux, une identité de Bézout est donnée par

$$\frac{1}{3}(x^2-1) + (-\frac{1}{3}x + \frac{2}{3})(x+2) = 1.$$

I.5.6. Calculer une identité de Bézout.— L'algorithme d'Euclide permet de calculer une identité de Bézout. Étant donnés deux polynômes f_1 et f_2, premiers entre eux, l'algorithme suivant permet de calculer une identité de Bézout

$$u_1 f_1 + u_2 f_2 = 1.$$

Soient $f_1, f_2 \in \mathbb{K}[x] - \{0\}$ deux polynômes premiers entre eux. On pose $r_0 = f_1$, $r_1 = f_2$. On calcule les divisions euclidiennes

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, \quad \deg(r_2) < \deg(r_1), \\
r_1 &= r_2 q_2 + r_3, \quad \deg(r_3) < \deg(r_2), \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad \deg(r_n) < \deg(r_{n-1}),
\end{aligned}$$

Alors, il existe $n_0 \geq 0$ tel que, pour tout $n \geq n_0$, $r_n = 0$. Les polynômes f_1 et f_2 sont premiers entre eux, par suite le dernier reste non nul r_{n_0-1} est une constante $b \in \mathbb{K} - \{0\}$. Pour déterminer u_1 et u_2 dans l'identité de Bézout, il suffit de partir de

$$r_{n_0-1} = b = r_{n_0-3} - r_{n_0-2} q_{n_0-2},$$

et en utilisant toutes les relations entre les restes, obtenir une relation de Bézout entre r_0 et r_1, comme dans l'exemple suivant.

I.5.7. Exemple.— Les polynômes x^4+1 et x^3+1 sont premiers entre eux. On calcule la division euclidienne de x^4+1 par x^3+1 :

$$x^4 + 1 = (x^3+1)(x) + (-x+1),$$

on calcule alors la division euclidienne de x^3+1 par $-x+1$:

$$x^3+1=(-x+1)(-x^2-x-1)+2.$$

Le dernier reste non nul est 2, on a alors

$$\begin{aligned}2&=(x^3+1)-(-x+1)(-x^2-x-1),\\&=(x^3+1)-((x^4+1)-(x^3+1)(x))(-x^2-x-1),\\&=(x^3+1)-(x^4+1)(-x^2-x-1)+(x^3+1)x(-x^2-x-1),\\&=(x^3+1)(1-x-x^2-x^3)+(x^4+1)(1+x+x^2).\end{aligned}$$

On obtient ainsi une relation de Bézout :

$$1=\frac{1}{2}(1-x-x^2-x^3)(x^3+1)+\frac{1}{2}(1+x+x^2)(x^4+1).$$

Exercice 26. — Trouver une relation de Bézout entre les polynômes f et g, avec

1. $f=x^2+2x-1, \quad g=x+2,$
2. $f=x^4+2x^3-x, \quad g=x^3+5,$
3. $f=x^2+2x-1, \quad g=x+2.$

Exercice 27 (Lemme de Gauss). — Soient f,g,h des polynômes de $\mathbb{K}[x]$. Montrer que si f et g sont premiers entre eux et que f divise gh, alors f divise h.

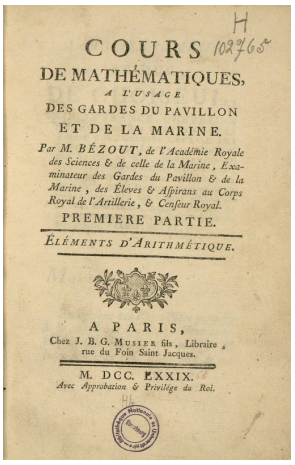

COURS
DE MATHÉMATIQUES,
A L'USAGE
DES GARDES DU PAVILLON
ET DE LA MARINE.
Par M. BÉZOUT, de l'Académie Royale des Sciences & de celle de la Marine, Examinateur des Gardes du Pavillon & de la Marine, des Élèves & Aspirans au Corps Royal de l'Artillerie, & Censeur Royal.
PREMIERE PARTIE.
ÉLÉMENTS D'ARITHMÉTIQUE.
A PARIS,
Chez J. B. G. MUSIER fils, Libraire, rue du Foin Saint Jacques.
M. DCC. LXXIX.
Avec Approbation & Privilège du Roi.

FIGURE I.3.: Étienne Bézout (1730 - 1783)

Étienne Bézout est un mathématicien français, auteur d'une Théorie générale des équations algébriques sur la théorie de l'élimination et des fonctions symétriques sur les racines d'une équation. Examinateur des élèves du corps de l'artillerie, il rédige un cours de mathématiques à l'usage de la marine et de l'artillerie, qui deviendra un ouvrage de référence pour les candidats au concours d'entrée à l'École polytechnique.

I.5.8. Racine d'un polynôme.— Soit f un polynôme de $\mathbb{K}[x]$. Un scalaire $a\in\mathbb{K}$ est dit *racine* de f si $f(a)=0$, c'est-à-dire, lorsque a est un zéro de la fonction polynomiale $\widetilde{f}$. On peut dire aussi que a est racine de f si, et seulement si, $x-a$ divise f.

Si $a_1, \ldots, a_p$ sont p racines distinctes de f, alors f est divisible par le polynôme

$$\prod_{i=1}^{p} (x - a_i).$$

Un polynôme non nul f de degré n admet au plus n racines distinctes. Si f admet n racines distinctes $a_1, \ldots, a_n$, alors, il se décompose sous la forme

$$f = \mathrm{lc}(f) \prod_{i=1}^{n} (x - a_i).$$

Exercice 28. — 1. Montrer les assertions ci-dessus.

2. En déduire que si f est un polynôme non nul à coefficients dans un corps K infini, alors sa fonction polynômiale associée $\tilde{f}$ n'est pas nulle.
3. Généraliser les résultats de l'exercice 18 à tout corps infini.

I.5.9. Racines multiples.— Soient f un polynôme de $\mathbb{K}[x]$ et a une racine de f. On appelle *ordre de multiplicité* de la racine a l'exposant de la plus grande puissance de $x - a$ qui divise f. Autrement dit, c'est l'entier h tel que $(x-a)^h$ divise f et $(x-a)^{h+1}$ ne divise pas f. Soit f un polynôme tel que

$$f = (x-a)^h q.$$

Alors a est racine d'ordre de multiplicité h si, et seulement si, a n'est pas racine du polynôme q.

I.5.10. Polynômes scindés.— Soit $f \in \mathbb{K}[x]$ un polynôme. On dit que f est *scindé* sur $\mathbb{K}$ s'il admet des racines $a_1, \ldots, a_p$ dans $\mathbb{K}$ d'ordre de multiplicité respectifs $h_1, \ldots, h_p$ telles que $h_1 + \ldots + h_p = \deg(f)$. On a alors

$$f = \mathrm{lc}(f) \prod_{i=1}^{p} (x - a_i)^{h_i},$$

avec $a_i \neq a_j$ si $i \neq j$ et $h_1 + \cdots + h_p = \deg(f)$.

I.5 Théorème (de D'Alembert-Gauss). — Tout polynôme non constant à coefficients dans $\mathbb{C}$ possède au moins une racine dans $\mathbb{C}$.

Ce théorème est appelé aussi théorème de D'Alembert-Gauss, ou encore *théorème fondamental de l'algèbre*.

On dit qu'un corps $\mathbb{K}$ est *algébriquement clos*, si tout polynôme non constant de $\mathbb{K}[x]$ possède une racine dans $\mathbb{K}$.

Exercice 29. — Montrer que si un corps $\mathbb{K}$ est algébriquement clos alors tout polynôme non nul de $\mathbb{K}[x]$ est scindé sur $\mathbb{K}$.

I.6 Corollaire. — Tout polynôme non nul de $\mathbb{C}[x]$ est scindé sur $\mathbb{C}$.

Exercice 30. — Montrer que le corps $\mathbb{R}$ n'est pas algébriquement clos.

Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On dit qu'un élément a de $\mathbb{L}$ est *algébrique* sur $\mathbb{K}$ s'il est racine d'un polynôme non nul de $\mathbb{K}[x]$. Par exemple $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ mais $\pi \in \mathbb{R}$ ne l'est pas (théorème d'Hermite-Lindemann, 1882). On dit que $\mathbb{L}$ est une *extension algébrique* de $\mathbb{K}$ si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Exercice 31. — Montrer que $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$.

Le corps $\mathbb{C}$ est l'unique extension algébrique [2] de $\mathbb{R}$ qui est algébriquement close. Plus généralement, on peut montrer que, pour tout corps $\mathbb{K}$, il existe une unique extension algébrique[2] $\mathbb{L}$ qui est algébriquement close. Le corps $\mathbb{L}$ est appelé la *clôture algèbrique* de $\mathbb{K}$. Par exemple $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

FIGURE I.4.: Jean Le Rond D'Alembert (1717 - 1783)

Jean Le Rond D'Alembert est un mathématicien, philosophe et encyclopédiste français. Il énonce le théorème de D'Alembert-Gauss dans le Traité de dynamique, qui ne sera démontré qu'un siècle après par Carl Friedrich Gauss. D'Alembert est célèbre pour ses nombreux travaux mathématiques, notamment sur les équations différentielles et les équations aux dérivées partielles. Il aborda des problèmes difficiles en physique avec le Traité de dynamique des systèmes, en astronomie avec le problème des trois corps, ou encore en musique avec la vibration des cordes.

§ 6 Les relations d'ordre

I.6.1. Relations d'ordre.— Soit E un ensemble non vide. Une *relation d'ordre* $\preccurlyeq$ sur E est une relation binaire $\preccurlyeq$ sur E satisfaisant les propriétés suivantes :

i) *réflexivité* : pour tout $x \in E$, $x \preccurlyeq x$,

ii) *antisymétrie* : $(x \preccurlyeq y \text{ et } y \preccurlyeq x) \Rightarrow x = y$.

iii) *transitivité* : $(x \preccurlyeq y \text{ et } y \preccurlyeq z) \Rightarrow x \preccurlyeq z$.

Un ensemble muni d'une relation d'ordre est appelé *ensemble ordonné*.

2. unique à isomorphisme près.

I.6.2. Exemples.— La relation $\leq$ est une relation d'ordre sur l'ensemble $\mathbb{R}$ des réels. La relation de divisibilité sur les entiers naturels non nuls : $n|m$ si, et seulement si, n divise m est une relation d'ordre sur $\mathbb{N}-\{0\}$. La relation d'inclusion $\subset$ est une relation d'ordre sur l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble E.

I.6.3. Ordre total.— Une relation d'ordre $\preccurlyeq$ sur E est dite *totale* si deux éléments de E sont toujours comparables par la relation d'ordre :

iv) pour tous $x, y \in E$, $x \preccurlyeq y$ ou $y \preccurlyeq x$.

On dit alors que l'ensemble est *totalement ordonné*. Par exemple l'ensemble $(\mathbb{N}, \leq)$ est totalement ordonné.

Exercice 32. —

1. Montrer que l'ensemble $(\mathbb{N}, |)$ n'est pas totalement ordonné.

2. Étant donné un ensemble E possédant au moins deux éléments, montrer que l'ensemble $(\mathscr{P}(E), \subset)$ n'est pas totalement ordonné.

I.6.4. Bon ordre.— Soient $(E, \preccurlyeq)$ un ensemble ordonné, A une partie non vide de E et x un élément de E. On dit que

- x est un *majorant* de A, ou que x *majore* A, lorsque, pour tout $a \in A$, $a \preccurlyeq x$,
- x est un *minorant* de A, ou que x *minore* A, lorsque, pour tout $a \in A$, $x \preccurlyeq a$,
- x est un *plus grand élément* de A, si $x \in A$ et x est un majorant de A,
- x est un *plus petit élément* de A, si $x \in A$ et x est un minorant de A.

Un ensemble ordonné $(E, \preccurlyeq)$ est dit *bien ordonné* et la relation $\preccurlyeq$ est appelée un *bon ordre* si la condition suivante est satisfaite :

v) toute partie non vide de E possède un plus petit élément pour la relation $\preccurlyeq$.

I.6.5. Remarque.—

– Un bon ordre ne possède pas de suite strictement décroissante infinie.
– Un bon ordre est un ordre total.
– Un ordre total qui ne possède pas de suite strictement décroissante infinie est un bon ordre.

En particulier, un ordre total est un bon ordre si et seulement s'il ne possède pas de suite strictement décroissante infinie.

I.6.6. Exemples.— On montre que l'ensemble $\mathbb{N}$ est bien ordonné par l'ordre $\leq$, c'est une conséquence de la définition de $\mathbb{N}$. L'ensemble $(\mathbb{Z}, \leq)$ n'est pas bien ordonné, car l'ensemble $\mathbb{Z}$ lui-même n'admet pas de plus plus petit élément. L'ensemble des réels positifs, muni de l'ordre $\leq$, n'est pas bien ordonné, l'intervalle ouvert $]0, 1[$ ne possède pas de plus petit élément.

I.6.7. Principe de récurrence sur un bon ordre.— Le principe de récurrence sur $\mathbb{N}$ s'étend aux ensembles bien ordonnés :

I.7 Proposition. — Soit un ensemble bien ordonné $(I, \preccurlyeq)$ et une famille $(P_i)_{i\in I}$ de propriétés. Si pour chaque $i \in I$, la propriété P_i est satisfaite dès que les propriétés P_j sont satisfaites pour tout $j \prec i$, alors les propriétés P_i sont satisfaites pour tout $i \in I$.

Autrement dit,

$$\text{si } \forall i \in I,\ (\forall j \prec i\ P_j) \Rightarrow P_i \text{ alors } \forall i \in I,\ P_i.$$

Preuve. Soit A l'ensemble des $i \in I$ tel que P_i n'est pas satisfaite. Si A est non vide, il possède un plus petit élément i_0. La propriété P_{i_0} n'est en particulier pas satisfaite, mais par contre les propriétés P_j le sont toutes pour $j < i_0$. □

Exercice 33. — Montrer la remarque I.6.5.

Exercice 34 (ordre produit). — Soit $(E, \preccurlyeq)$ un ensemble ordonné. On définit la relation $\preccurlyeq_{\text{prod}}$ sur $E \times E$ en posant

$$(x,y) \preccurlyeq_{\text{prod}} (x',y'), \quad \text{si, et seulement si, } x \preccurlyeq x' \text{ et } y \preccurlyeq y'.$$

1. Montrer que $\preccurlyeq_{\text{prod}}$ est une relation d'ordre.
2. Montrer que cette relation n'est pas totale lorsque E contient au moins deux éléments.

Exercice 35 (ordre lexicographique). — Soit $(E, \preccurlyeq)$ un ensemble ordonné. On définit la relation $\preccurlyeq_{\text{lex}}$ sur $E \times E$ en posant

$$(x,y) \preccurlyeq_{\text{lex}} (x',y'), \quad \text{si, et seulement si, } \quad (x \preccurlyeq x' \text{ et } x \neq x') \text{ ou } (x = x' \text{ et } y \preccurlyeq y').$$

1. Montrer que $\preccurlyeq_{\text{lex}}$ est une relation d'ordre.
2. Montrer que si $\preccurlyeq$ est une relation d'ordre total sur E, alors $\preccurlyeq_{\text{lex}}$ est une relation d'ordre totale.
3. Montrer que si $\preccurlyeq$ est un bon ordre sur E, alors $\preccurlyeq_{\text{lex}}$ est un bon ordre sur $E \times E$.

Exercice 36. — On considère l'ensemble ordonné $(\mathbb{N}, \leq)$.

1. Montrer que $\preccurlyeq_{\text{prod}}$ n'est pas un bon ordre sur $\mathbb{N} \times \mathbb{N}$.
2. Montrer que $\preccurlyeq_{\text{lex}}$ est un bon ordre sur $\mathbb{N} \times \mathbb{N}$.

Exercice 37. — Soit Σ un alphabet fini (un ensemble fini de lettres totalement ordonné, c.à.d. muni d'un ordre alphabétique) et Σ^* l'ensemble des mots sur cet alphabet (ensemble des suites finies de lettres de l'alphabet). (Par exemple, si $\Sigma = \{a,b,c\}$, alors *abac*, *ccbaba*, *bacaaccbb* sont des mots dans Σ^*.)

1. Montrer que si Σ contient au moins deux lettres, alors l'ordre alphabétique sur Σ^* n'est pas un bon ordre.
2. Définir un bon ordre sur Σ^*.

CHAPITRE
II

Polynômes, ensembles algébriques affines et idéaux

Sommaire

§ 1 Les polynômes à plusieurs indéterminées

Nous avons vu dans le premier chapitre la notion de polynôme à une indéterminée. Dans cette section, nous introduisons les polynômes à plusieurs indéterminées à coefficients dans un corps.

II.1.1. Les monômes.— Un *monôme* en les indéterminées $x_1, x_2, \ldots, x_n$ est un produit de la forme

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n},$$

où $\alpha_1, \ldots, \alpha_n$ sont des entiers naturels. On appelle *degré total* d'un tel monôme, la somme

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

Par exemple, les monômes

$$x_1^4 x_2^3 x_3^2, \quad x_1^2 x_3^2, \quad x_3^5$$

sont des monômes de degré total 9, 4 et 5 respectivement.

II.1.2. Notations.— En notant α un n-uplet $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ d'entiers naturels, on notera

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

En particulier, on pose $x^{(0,0,\ldots,0)} = 1$. Le degré total du monôme x^α sera noté

$$|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

II.1.3. Les polynômes.— Un *polynôme* f d'indéterminées $x_1,\dots,x_n$ à coefficients dans un corps $\mathbb{K}$ est une combinaison linéaire (finie) à coefficients dans $\mathbb{K}$ de monômes d'indéterminées $x_1,\dots,x_n$. Avec les notations précédentes, un polynôme f s'écrit sous la forme

$$f=\sum_{\alpha} a_\alpha x^\alpha,$$

où a_α est un scalaire dans $\mathbb{K}$ et la somme est indexée par un nombre fini de n-uplets $\alpha=(\alpha_1,\dots,\alpha_n)$.

La somme et le produit de deux polynômes d'indéterminés $x_1,\dots,x_n$ est encore un polynôme d'indéterminées $x_1,\dots,x_n$. On a

II.1 Proposition. — L'ensemble des polynômes d'indéterminées $x_1,\dots,x_n$, muni de l'addition et de la multiplication forme un anneau commutatif, noté $\mathbb{K}[x_1,\dots,x_n]$.

II.1.4. Notation.— Lorsque l'on considérera des polynômes avec un petit nombre d'indéterminées, on utilisera les lettres sans indice x, y, z, …, pour désigner les indéterminées. Les anneaux des polynômes d'une, deux et trois indéterminées seront ainsi notés $\mathbb{K}[x]$, $\mathbb{K}[x,y]$ et $\mathbb{K}[x,y,z]$ respectivement. Par exemple, le polynôme

$$f=\frac{1}{2}x^4y^3z^2+2x^2z^2-\frac{1}{5}xyz+z^5$$

est un polynôme de $\mathbb{Q}[x,y,z]$.

II.1.5. Définitions.— Soit $f=\sum_{\alpha} a_\alpha x^\alpha$ un polynôme de $\mathbb{K}[x_1,\dots,x_n]$,

- **i)** le scalaire a_α est appelé le *coefficient* du monôme x^α,
- **ii)** si $a_\alpha\neq 0$, $a_\alpha x^\alpha$ est un *terme* du polynôme f,
- **iii)** le *degré total* du polynôme f, noté $\deg(f)$, est le degré total maximum $|\alpha|$, tel que le coefficient a_α soit non nul.

Par exemple, le polynôme

$$f=2xy^2z^2+3x^2z^2-5xyz^3+z^5$$

possède 4 termes de degrés 5, 4, 5 et 5 respectivement, il est de degré total 5. Notons que trois termes sont de même degré total maximal 5 avec des monômes différents. Cette situation n'est pas possible avec des polynômes d'une seule indéterminée. Dans la suite de ce cours, nous expliciterons les méthodes permettant d'ordonner les termes dans un polynôme à plusieurs indéterminées.

II.1.6. Remarque sur la construction de l'anneau des polynômes à plusieurs indéterminées.— De la même façon que nous avons construit l'anneau $\mathbb{K}[x]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, on peut construire l'anneau $A[x]$ des polynômes à coefficients dans un anneau commutatif A. Étant donné un anneau de polynômes $A[x_1]$, on peut construire l'anneau des polynômes à une indéterminée x_2 à coefficients dans $A[x_1]$, que l'on note $(A[x_1])[x_2]$. De la même façon, on peut construire l'anneau $(A[x_2])[x_1]$. Ces deux anneaux

sont canoniquement isomorphes par l'isomorphisme [1] suivant :

$$(A[x_1])[x_2] \longrightarrow (A[x_2])[x_1]$$
$$\sum_{\alpha_2}\left(\sum_{\alpha_1} a_{\alpha_1,\alpha_2}\, x_1^{\alpha_1}\right) x_2^{\alpha_2} \longmapsto \sum_{\alpha_1}\left(\sum_{\alpha_2} a_{\alpha_1,\alpha_2}\, x_2^{\alpha_2}\right) x_1^{\alpha_1}$$

On note cet anneau $A[x_1,x_2]$ et ses éléments sont notés

$$\sum_{\alpha_1,\alpha_2} a_{\alpha_1,\alpha_2}\, x_1^{\alpha_1} x_2^{\alpha_2}.$$

Par itération, on peut construire l'anneau des polynômes à n indéterminées à coefficients dans A, noté

$$A[x_1,\ldots,x_n] = (A[x_1,\ldots,x_{n-1}])[x_n],$$

ses éléments sont les sommes finies

$$\sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n}\, x_1^{\alpha_1}\ldots x_n^{\alpha_n}.$$

§ 2 Les ensembles algébriques affines

II.2.1. Fonction polynomiale.— Étant donné un polynôme $f = \sum_{\alpha} a_\alpha x^\alpha$ de $\mathbb{K}[x_1,\ldots,x_n]$, on définit la *fonction polynomiale* associée comme l'application

$$\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K},$$

qui à tout $(a_1,\ldots,a_n) \in \mathbb{K}^n$ associe le scalaire $f(a_1,\ldots,a_n) \in \mathbb{K}$, obtenu en remplaçant dans l'expression de f l'indéterminée x_i par a_i, pour tout i.

Nous avons déjà vu en I.4.1 que les notions de polynôme et de fonction polynomiale ne coïncident pas lorsque $\mathbb{K}$ est un corps fini. Pour les corps infinis, tels que $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on a cependant

II.2 Proposition. — Soit $\mathbb{K}$ un corps infini et soit f un polynôme de $\mathbb{K}[x_1,\ldots,x_n]$. Alors f est le polynôme nul de $\mathbb{K}[x_1,\ldots,x_n]$ si, et seulement si, la fonction polynomiale associée $\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K}$ est la fonction nulle.

Exercice 38. — L'objectif est de montrer la proposition II.2.

1. Montrer que la fonction polynomiale du polynôme nul est la fonction nulle.

1. Soient A et B deux anneaux. Un *morphisme d'anneaux* de A dans B est une application $f : A \longrightarrow B$ vérifiant les assertions suivantes

i) $f(a+b) = f(a)+f(b)$, pour tous $a,b \in A$,

ii) $f(ab) = f(a)f(b)$, pour tous $a,b \in A$,

iii) $f(1) = 1$.

Un *isomorphisme* d'anneaux est un morphisme d'anneaux bijectif.

2. Montrer la réciproque dans le cas où $n = 1$: si $f \in \mathbb{K}[x]$ possède une fonction polynomiale nulle, alors f est nul.
3. Montrer la réciproque dans le cas général, par récurrence sur l'entier n.

Exercice 39. — On suppose que $\mathbb{K}$ est le corps $\mathbb{Z}/2\mathbb{Z}$.
1. Considérons le polynômes $f = x^2y + y^2x$ de $\mathbb{K}[x,y]$. Montrer que la fonction polynomiale $\widetilde{f}$ est nulle.
2. Trouver un polynôme non nul de $\mathbb{K}[x,y,z]$ à trois indéterminées, dont la fonction polynomiale est nulle.

On déduit de la proposition II.2, le résultat suivant

II.3 Proposition. — Soit $\mathbb{K}$ un corps infini et soient f, g deux polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Alors les polynômes f et g sont égaux si, et seulement si, les fonctions polynomiales $\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K}$ et $\widetilde{g} : \mathbb{K}^n \longrightarrow \mathbb{K}$ sont égales.

Exercice 40. — Montrer la proposition II.3.

II.2.2. Espaces affines de dimension n.— Étant donné un corps $\mathbb{K}$ et $n \geq 1$ un entier naturel, on appelle *espace affine* de dimension n sur $\mathbb{K}$ l'ensemble

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{K}\}.$$

L'espace $\mathbb{K}^1$ est appelé la *droite affine*, l'espace $\mathbb{K}^2$ est appelé le *plan affine* .

II.2.3. Ensembles algébriques affines.— Soit $\mathbb{K}$ un corps et soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. On note

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid f_i(a_1, \ldots, a_n) = 0, \quad \text{pour tout } i \in [\![1, s]\!]\}$$

Le sous-ensemble $\mathbf{V}(f_1, \ldots, f_s)$ de $\mathbb{K}^n$ est appelé l'*ensemble algébrique affine*,ou *variété affine*, définie par les polynômes $f_1, \ldots, f_s$. L'ensemble algébrique affine $\mathbf{V}(f_1, \ldots, f_s)$ est ainsi le sous-ensemble de $\mathbb{K}^n$ formé des solutions du système d'équations

$$\begin{cases} f_1(a_1, \ldots, a_n) = 0 \\ f_2(a_1, \ldots, a_n) = 0 \\ \qquad \vdots \\ f_s(a_1, \ldots, a_n) = 0 \end{cases}$$

Exercice 41. — Montrer que l'ensemble vide et l'espace affine $\mathbb{K}^n$ sont des ensembles algébriques affines.

Exercice 42. — Montrer qu'un point de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 43. — On suppose que $n = 1$. Si f n'est pas le polynôme nul de $\mathbb{K}[x]$, montrer que $\mathbf{V}(f)$ est un ensemble fini. Ainsi, les ensembles algébriques affines de la droite affine sont la droite elle-même et les ensembles finis.

Exercice 44. — Montrer que deux polynômes différents peuvent définir le même ensemble algébrique affine.

II.2.4. Exemples dans $\mathbb{R}^2$.— Pour les exemples suivants, on considère que $\mathbb{K}$ est le corps des réels. Dans le plan $\mathbb{R}^2$, l'ensemble algébrique affine $\mathbf{V}(x^2+y^2-1)$ est le cercle centré sur l'origine et de rayon 1.

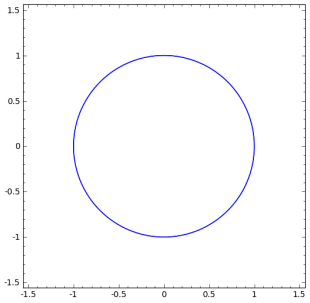


FIGURE II.1.: Cercle $\mathbf{V}(1-x^2-y^2)$

Les commandes Sage pour tracer la figure II.1 sont

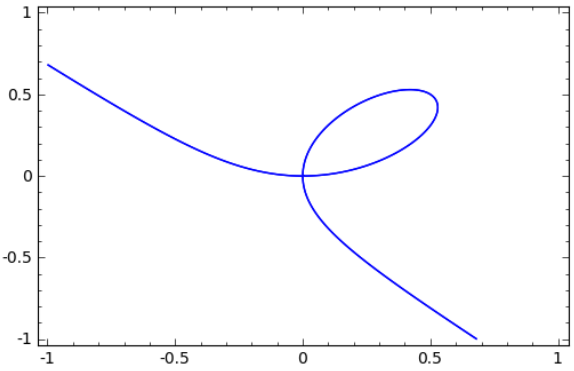
```
sage: R.<x, y> = RR[]
sage: C = Curve(x^2 + y^2 -1)
sage: C.plot((x,-1.5,1.5), (y,-1.5,1.5))
```

L'ensemble algébrique affine réel $\mathbf{V}(x^2+y^2+1)$ est l'ensemble vide, car l'équation $x^2+y^2=-1$ ne possède pas de solution réelle

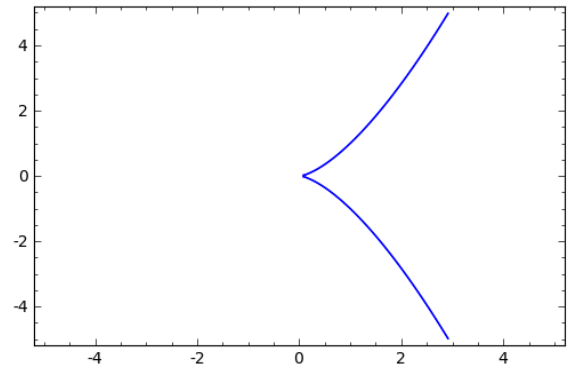
Exercice 45. — Montrer qu'un ensemble algébrique affine $\mathbf{V}(f)$ défini par un polynôme f de $\mathbb{R}[x,y]$ n'est pas toujours une partie connexe de $\mathbb{R}^2$.

Exercice 46. — Tracer les ensembles algébriques suivants dans $\mathbb{R}^2$:

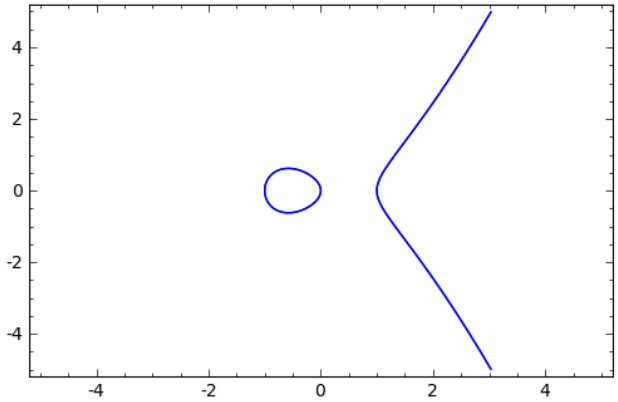
1. $\mathbf{V}(x^2+4y^2+2x-16y+1)$,
2. $\mathbf{V}(x^2-y^2)$,
3. $\mathbf{V}(2x+y-1,3x-y+2)$,
4. $\mathbf{V}(y^2-x(x-1)(x-2))$.



(a) Cubique nodale $\mathbf{V}(x^3+y^3-xy)$

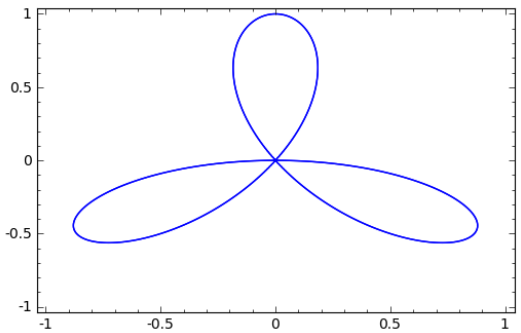


(b) Cubique cuspidale $\mathbf{V}(y^2-x^3)$

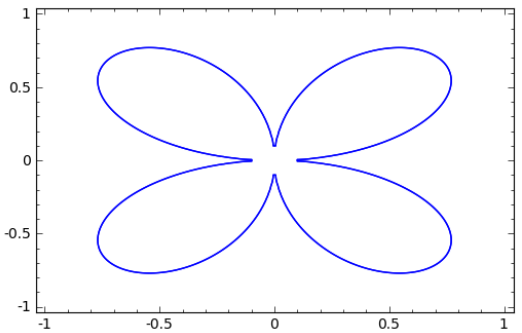


(c) Une cubique non singulière $\mathbf{V}(y^2-x(x-1)(x+1))$

FIGURE II.2.: Des cubiques $\mathbf{V}(f)$ (f de degré 3).

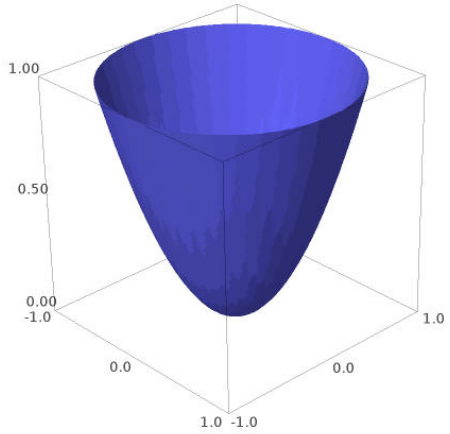


(a) Trifolium $\mathbf{V}((x^2+y^2)^2+3x^2y-y^3)$

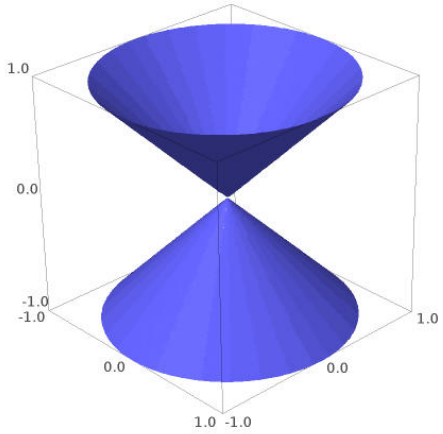


(b) Quadrifolium $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$

II.2.5. Exemples dans $\mathbb{R}^3$.— Le paraboloïde de révolution, obtenu par rotation d'une parabole $z=x^2$ autour de l'axe Oz.



(c) Paraboloïde de révolution $\mathbf{V}(z-x^2-y^2)$



(d) Cône de révolution $\mathbf{V}(z^2-x^2-y^2)$

Les commandes Sage pour le tracé du paraboloïde :

```
sage: var('x,y,z')
sage: h = lambda x,y,z:z-x^2-y^2
sage: f = implicit_plot3d(h,(x,-1,1),(y,-1,1),(z,0,1),\
....:                     plot_points=100, smooth=True, adaptative=True)
sage: f
```

Exercice 47.— Tracer les ensembles algébriques suivants dans $\mathbb{R}^3$:

1. $\mathbf{V}(x^2+y^2+z^2-1)$,
2. $\mathbf{V}(x^2+y^2-1)$,
3. $\mathbf{V}(x+2, y-3/2, z)$,
4. $\mathbf{V}(xz^2-xy)$,
5. $\mathbf{V}(x^2+y^2+z^2-1, x^2+y^2+(z-1)^2-1)$.

Exercice 48.— Décrire l'équation de l'ensemble algébrique affine constitué du cylindre de rayon 1 centré sur l'axe des y.

Exercice 49.— On considère l'ensemble

$$X = \{(x,x) \mid x \in \mathbb{R} - \{1\}\} \subset \mathbb{R}^2.$$

1. Montrer que si f est un polynôme de $\mathbb{R}[x,y]$, tel que la fonction polynomiale $\widetilde{f}$ s'annule sur X, alors $f(1,1) = 0$.
2. En déduire que X n'est pas un ensemble algébrique affine de $\mathbb{R}^2$.

II.2.6. Un exemple en robotique.— En conclusion de ce cours, nous développerons un exemple d'application de l'étude des ensembles algébriques affines à la robotique. L'idée est la suivante. Considérons un bras de robot articulé dont les mouvements sont dans un plan ; le bras est constitué de deux segments

- un segment de longueur 2 est fixé à l'origine par une rotule,
- un deuxième segment de longueur 1 est fixé à l'extrémité du premier segment par une autre rotule.

Les états du bras sont déterminés par deux couples de coordonnées (x,y) et (z,w) qui correspondent à l'extrémité de chaque segment. Une configuration du bras du robot peut ainsi être vue comme un 4-uplet

$$(x,y,z,w) \in \mathbb{R}^4.$$

Notons que, si l'on considère le problème en dimension 3, le système admettra 6 indéterminées. Tous les points de $\mathbb{R}^4$ ne sont pas une configuration du bras du robot. En particulier, des points du plan ne seront pas atteignables par le bras. L'ensemble des configurations du robot est défini par les équations

$$\begin{cases} x^2+y^2 &= 4, \\ (x-z)^2+(y-w)^2 &= 1. \end{cases}$$

Par exemple, l'origine $(z,w)=(0,0)$ n'est pas atteignable par l'extrémité du bras du robot. En effet, le système

$$\begin{cases} x^2+y^2 &= 4, \\ x^2+y^2 &= 1. \end{cases}$$

ne possède pas de solution. Par contre, le point $(z,w)=(1,0)$ est atteignable, car le système

$$\begin{cases} x^2+y^2 &= 4, \\ (x-1)^2+y^2 &= 1. \end{cases}$$

est équivalent au système

$$\begin{cases} x^2+y^2 &= 4, \\ -2x &= -4. \end{cases}$$

Il admet donc pour solution $(x,y)=(2,0)$. Le point du plan de coordonnées $(z,w)=(4,0)$ n'est pas atteignable par le bras du robot, car le système

$$\begin{cases} x^2+y^2 &= 4, \\ x^2+(y-4)^2 &= 1. \end{cases}$$

ne possède pas de solution. La seconde équation s'écrit $x^2+y^2-8y+16=1$, or, d'après la première équation, on a $-8y=-19$, soit $y=19/8>2$. Le système n'a donc pas de solution.

II.2.7. Opérations sur les ensembles algébriques affines.— L'intersection et la réunion d'ensembles algébriques affines sont encore des ensembles algébriques affines.

II.4 Proposition. — Si $\mathbf{V}$ et $\mathbf{W}$ sont deux ensembles algébriques affines, alors il en est de même pour $\mathbf{V}\cup\mathbf{W}$ et $\mathbf{V}\cap\mathbf{W}$.

Preuve. Supposons que

$$\mathbf{V}=\mathbf{V}(f_1,\dots,f_s), \quad \mathbf{W}=\mathbf{V}(g_1,\dots,g_t).$$

On a

$$\mathbf{V}\cap\mathbf{W}=\mathbf{V}(f_1,\dots,f_s,g_1,\dots,g_t),$$

car un élément de $\mathbf{V}\cap\mathbf{W}$ annule à la fois les polynômes $f_1,\dots,f_s$ et les polynômes $g_1,\dots,g_t$. Ainsi $\mathbf{V}\cap\mathbf{W}$ est un ensemble algébrique affine.

Par ailleurs, on a

$$\mathbf{V}\cup\mathbf{W}=\mathbf{V}(f_ig_j \mid i\in[\![1,s]\!],\ j\in[\![1,t]\!]).$$

Un élément de $\mathbf{V}$ annule tous les polynômes f_i, il annulent donc tous les polynômes f_ig_j. Ainsi $\mathbf{V}$ est un sous-ensemble de $\mathbf{V}(f_ig_j)$. On montre de la même façon, que $\mathbf{W}$ est un sous-ensemble de $\mathbf{V}(f_ig_j)$, ainsi, $\mathbf{V}\cup\mathbf{W}\subset\mathbf{V}(f_ig_j)$. Montrons l'inclusion réciproque. Considérons $(a_1,\dots,a_n)\in$

$\mathbf{V}(f_i g_j)$, on a soit $(a_1,\dots,a_n) \in \mathbf{V}$ qui termine le raisonnement, soit $f_{i_0}(a_1,\dots,a_n) \neq 0$, pour au moins un $i_0 \in [\![1,s]\!]$. Comme $f_{i_0} g_j(a_1,\dots,a_n) = 0$, pour tout j, alors $g_j(a_1,\dots,a_n) = 0$, pour tout j, ainsi $(a_1,\dots,a_n) \in \mathbf{W}$. Par suite, $\mathbf{V}(f_i g_j) \subset \mathbf{V} \cup \mathbf{W}$. □

De ce résultat, on déduit

II.5 Proposition. — Toute intersection finie et toute réunion finie d'ensembles algébriques affines est un ensemble algébrique affine.

II.2.8. Exemples.— L'ensemble algébrique affine de $\mathbb{R}^3$ suivant

$$\mathbf{V}(x^2+z^2-1, x^2+y^2+(z-1)^2-1)$$

est l'intersection de la sphère de rayon 1 centrée en $(0,0,1)$ et du cylindre de rayon 1 centré sur l'axe des y.

L'ensemble algébrique affine

$$\mathbf{V}((x^2+z^2-1)(x^2+y^2+(z-1)^2-1))$$

est la réunion des mêmes sphère et cylindre.

Exercice 50. — Montrer que tout sous-ensemble fini de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 51. — Décrire et tracer l'ensemble algébrique affine de $\mathbb{R}^2$ défini par

$$\mathbf{V}(x^2+z^2-1, x^2+y^2+z^2-1).$$

Exercice 52. — Donner une description géométrique de l'ensemble algébrique affine $V(x^2+y^2)$ de $\mathbb{C}^2$.

§ 3 Les idéaux

Définition II.6. — Un sous-ensemble I de $\mathbb{K}[x_1,\dots,x_n]$ est un *idéal* s'il satisfait aux assertions suivantes :

i) $0 \in I$,

ii) si $f, g \in I$, alors $f+g \in I$,

iii) si $f \in I$ and $h \in \mathbb{K}[x_1,\dots,x_n]$, alors $hf \in I$.

II.3.1. Idéal engendré par une famille de polynômes.— Soient $f_1,\dots,f_s$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$. On notera

$$\langle f_1,\dots,f_s\rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_i \in \mathbb{K}[x_1,\dots,x_n] \right\}$$

II.7 Proposition.— L'ensemble $\langle f_1,\dots,f_s\rangle$ forme un idéal de $\mathbb{K}[x_1,\dots,x_n]$.

Preuve. L'idéal $\langle f_1,\dots,f_s\rangle$ contient le polynôme nul, car

$$0 = 0f_1 + 0f_2 + \ldots + 0f_s.$$

Soient $f = \sum_{i=1}^{s} h_i f_i$ et $g = \sum_{i=1}^{s} k_i f_i$, alors

$$f + g = \sum_{i=1}^{s} (h_i + k_i) f_i \in I,$$

et si en outre $h \in \mathbb{K}[x_1,\dots,x_n]$, on a

$$hf = \sum_{i=1}^{s} h h_i f_i \in I.$$

Ainsi, $\langle f_1,\dots,f_s\rangle$ est un idéal. □

Définition II.8.— L'idéal $\langle f_1,\dots,f_s\rangle$ est appelé l'*idéal engendré* par $f_1,\dots,f_s$.

II.3.2. Idéal de type fini.— On dit qu'un idéal I de $\mathbb{K}[x_1,\dots,x_n]$ est *finiment engendré*, ou de *type fini*, s'il existe des polynômes $f_1,\dots,f_s \in \mathbb{K}[x_1,\dots,x_n]$, tels que $I = \langle f_1,\dots,f_s\rangle$. On dit alors que les polynômes $f_1,\dots,f_s$ forment une *base* de l'idéal I. Nous verrons plus loin, que tout idéal de $\mathbb{K}[x_1,\dots,x_n]$ est finiment engendré, ce résultat est appelé le théorème de la base de Hilbert.

II.9 Proposition.— Soient $f_1,\dots,f_s$ et $g_1,\dots,g_t$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$ tels que

$$\langle f_1,\dots,f_s\rangle = \langle g_1,\dots,g_t\rangle,$$

alors $\mathbf{V}(f_1,\dots,f_s) = \mathbf{V}(g_1,\dots,g_t)$.

Preuve. Supposons que $\langle f_1,\dots,f_s\rangle = \langle g_1,\dots,g_t\rangle$. Soit $(a_1,\dots,a_n) \in \mathbf{V}(f_1,\dots,f_s)$, comme pour tout $j \in [\![1,t]\!]$, il existe une décomposition

$$g_j = h_1 f_1 + \ldots + h_s f_s,$$

on a $g_j(a_1,\dots,a_n) = 0$. On montre ainsi que $\mathbf{V}(f_1,\dots,f_s) \subset \mathbf{V}(g_1,\dots,g_t)$. L'inclusion réciproque se montre de la même façon. □

Exercice 53.— Soit I un idéal de $\mathbb{K}[x_1,\dots,x_n]$ et soient $f_1,\dots,f_s$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$. Montrer que les deux assertions suivantes sont équivalentes

i) $f_1,\dots,f_s \in I$,

ii) $\langle f_1,\dots,f_s\rangle \subset I$.

Exercice 54. — Montrer les égalités des idéaux suivants de $\mathbb{Q}[x,y]$,

1. $\langle x+y, x-y\rangle = \langle x,y\rangle$,
2. $\langle x+xy, y+xy, x^2, y^2\rangle = \langle x,y\rangle$,
3. $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle = \langle x^2-4, y^2-1\rangle$.

II.3.3. Idéal d'un ensemble algébrique affine.— Soit $\mathbf{V}$ un ensemble algébrique affine de $\mathbb{K}^n$. On pose

$$I(\mathbf{V}) = \{f \in \mathbb{K}[x_1,\ldots,x_n] \mid f(a_1,\ldots,a_n) = 0 \text{ pour tout } (a_1,\ldots,a_n) \in \mathbf{V}\}.$$

II.10 Proposition. — Ainsi défini, l'ensemble $I(\mathbf{V})$ est un idéal.

Preuve. L'ensemble $I(\mathbf{V})$ contient le polynôme nul, car il s'annule sur tous les points de $\mathbb{K}^n$, donc en particulier sur tous les points de $\mathbf{V}$. Soient f et g deux polynômes de $I(\mathbf{V})$, pour tout point $(a_1,\ldots,a_n)$ de $\mathbf{V}$, on a

$$(f+g)(a_1,\ldots,a_n) = f(a_1,\ldots,a_n) + g(a_1,\ldots,a_n) = 0+0 = 0.$$

Ainsi $f+g$ est un polynôme de $I(\mathbf{V})$. Si de plus $h \in \mathbb{K}[x_1,\ldots,x_n]$, on a

$$(hf)(a_1,\ldots,a_n) = h(a_1,\ldots,a_n) f(a_1,\ldots,a_n) = 0.$$

D'où $hf \in I(\mathbf{V})$. Ainsi $I(\mathbf{V})$ est un idéal. □

Définition II.11. — L'idéal $I(\mathbf{V})$ est appelé l'*idéal de l'ensemble algébrique affine* $\mathbf{V}$.

L'idée avec cette notion est d'associer à l'ensemble algébrique affine $\mathbf{V}$, objet de nature géométrique, un objet algébrique $I(\mathbf{V})$ afin de traduire les propriétés géométriques sous forme algébrique.

Exercice 55. — Montrer que $I(\mathbf{V}(x^n, y^m)) = \langle x,y\rangle$.

II.3.4. Relation entre idéaux et ensembles algébriques affines.— Considérons une famille de polynômes de $\mathbb{K}[x_1,\ldots,x_n]$:

$$f_1,\ldots,f_s.$$

On peut construire l'ensemble algébrique affine engendré par ces polynômes

$$\mathbf{V}(f_1,\ldots,f_s),$$

puis l'idéal de l'ensemble algébrique affine

$$I(\mathbf{V}(f_1,\ldots,f_s)).$$

Une question naturelle est : a-t-on

$$I(\mathbf{V}(f_1,\ldots,f_s)) = \langle f_1,\ldots,f_s\rangle ?$$

La réponse est négative en général :

II.12 Proposition. — Si $f_1,\dots,f_s$ sont des polynômes de $\mathbb{K}[x_1,\dots,x_n]$, alors

$$\langle f_1,\dots,f_s\rangle \subset I(\mathbf{V}(f_1,\dots,f_s)), \tag{II.1}$$

de plus, cette inclusion est stricte en général.

Preuve. Soit $f \in \langle f_1,\dots,f_s\rangle$, alors il existe une décomposition

$$f = h_1 f_1 + \dots + h_s f_s,$$

où les h_i sont des polynômes de $\mathbb{K}[x_1,\dots,x_n]$. Pour tout $(a_1,\dots,a_n) \in \mathbf{V}(f_1,\dots,f_s)$, on a $f_i(a_1,\dots,a_n) = 0$, pour tout $i \in [\![1,s]\!]$, par suite $f(a_1,\dots,a_n) = 0$. Ainsi f s'annule sur tous les points de $\mathbf{V}(f_1,\dots,f_s)$, ce qui entraîne que $f \in I(\mathbf{V}(f_1,\dots,f_s))$.

Pour montrer que l'inclusion est stricte, il suffit de considérer l'exemple suivant

$$\langle x^2, y^2\rangle \subset I(\mathbf{V}(x^2,y^2)).$$

Or $\mathbf{V}(x^2,y^2) = \{(0,0)\}$, car c'est l'ensemble des (x,y) tels que $x^2 = y^2 = 0$. Ainsi $I(\mathbf{V}(x^2,y^2)) = \langle x,y\rangle$. L'inclusion est stricte, car le polynôme x ne peut pas s'écrire sous la forme

$$x = h_1(x,y)x^2 + h_2(x,y)y^2.$$

□

Exercice 56. — Montrer que l'inclusion (II.1) est stricte en considérant le polynôme x^2+y^2+1 de $\mathbb{R}[x,y]$.

Exercice 57. — Soient $\mathbf{V}$ et $\mathbf{W}$ des ensembles algébriques affines de $\mathbb{K}^n$.

1. Montrer que $\mathbf{V} \subset \mathbf{W}$ si, et seulement si, $I(\mathbf{W}) \subset I(\mathbf{V})$.
2. Montrer que $\mathbf{V} = \mathbf{W}$ si, et seulement si, $I(\mathbf{V}) = I(\mathbf{W})$.

Exercice 58. — On considère les polynômes $f_1 = x+y^2-z^3+2z$, $f_2 = x-y^2-z^3+2z^2-2z+2$, $g_1 = x-z^3+z^2+1$ et $g_2 = y^2-z^2+2z-1$ de $\mathbb{Q}[x,y,z]$.

1. Montrer que les idéaux $I = \langle f_1,f_2\rangle$ et $J = \langle g_1,g_2\rangle$ de $\mathbb{Q}[x,y,z]$ sont égaux ; c'est-à-dire l'égalité suivante :

$$\langle x+y^2-z^3+2z, x-y^2-z^3+2z^2-2z+2\rangle = \langle x-z^3+z^2+1, y^2-z^2+2z-1\rangle.$$

2. On considère les ensembles algébriques affines de $\mathbb{Q}^3$ suivants :
$W = V(x+y^2-z^3+2z, x-y^2-z^3+2z^2-2z+2)$, $W_1 = V(x-z^3+z^2+1, y-z+1)$ et $W_2 = V(x-z^3+z^2+1, y+z-1)$.
Montrer l'égalité $W = W_1 \cup W_2$; c'est-à-dire l'égalité

$$V(x+y^2-z^3+2z, x-y^2-z^3+2z^2-2z+2) = V(x-z^3+z^2+1, y-z+1) \cup V(x-z^3+z^2+1, y+z-1).$$

II.3.5. Problèmes.— Voici des problèmes que nous allons aborder dans la suite de ce cours.

a) Problème de la description d'un idéal :

- est-ce que tout idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ possède un nombre fini de générateurs ? Autrement dit, existe-t-il une famille de polynômes $f_1,\ldots,f_s$ tels que $I=\langle f_1,\ldots,f_s\rangle$?
- si oui, comment déterminer une telle famille génératrice ?
- existe-t-il une famille génératrice « plus intéressante » que les autres ?

b) Problème de l'appartenance à un idéal :

étant donné un idéal $I=\langle f_1,\ldots,f_s\rangle$ et un polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$, déterminer si $f\in I$.

c) Problème de la résolution d'équations polynomiales :

étant donnés des polynômes $f_1,\ldots,f_s$ de $\mathbb{K}[x_1,\ldots,x_s]$, trouver les solutions dans $\mathbb{K}^n$ du système d'équations polynomiales

$$\begin{cases} f_1(x_1,\ldots,x_n)=0 \\ \vdots \\ f_s(x_1,\ldots,x_n)=0 \end{cases}$$

d) Problème d'impliciter une présentation paramétrée : *étant donné un paramétrage*

$$x_i=g_i(t_1,\ldots,t_m),\quad i\in[\![1,n]\!],\quad g_i\in\mathbb{K}[x_1,\ldots,x_m],$$

d'un ensemble algébrique affine $\mathbf{V}$ de $\mathbb{K}^n$, déterminer des polynômes $f_1,\ldots,f_s$ de $\mathbb{K}[x_1,\ldots,x_n]$, tels que

$$\mathbf{V}=\mathbf{V}(f_1,\ldots,f_s).$$

CHAPITRE
III

Algorithmes de division

Sommaire

§ 1 Préliminaires : systèmes d'équations linéaires

III.1.1. Systèmes d'équations linéaires.— L'algorithme d'élimination de Gauss-Jordan permet de déterminer les solutions d'un système d'équations linéaires, *i.e.*, des systèmes d'équations de la forme

$$\begin{cases} f_1(x_1,\ldots,x_n) = 0 \\ \qquad\vdots \\ f_s(x_1,\ldots,x_n) = 0 \end{cases}$$

où tous les polynômes $f_1,\ldots,f_s$ de $\mathbb{K}[x_1,\ldots,x_n]$ sont linéaires en les indéterminées $x_1,\ldots,x_n$.

III.1.2. Exemple.— Considérons les polynômes linéaires suivants

$$f_1 = x+y-z, \quad f_2 = 2x+3y+2z$$

de $\mathbb{R}[x,y,z]$. Soit $I = \langle f_1, f_2\rangle$ l'idéal engendré par ces deux polynômes et soit $\mathbf{V}(f_1,f_2)$ l'ensemble algébrique affine formé des solutions du système linéaire suivant

$$\begin{cases} x+y-z = 0 \\ 2x+3y+2z = 0 \end{cases}$$

La méthode d'élimination de Gauss-Jordan pour la résolution de ce système consiste à choisir un pivot, par exemple l'indéterminée x dans la première équation et à éliminer les termes contenant cette indéterminée dans les autres équations. Le système se réduit ainsi au système suivant

$$\begin{cases} \boxed{x} + y - z = 0 \\ \quad y + 4z = 0 \end{cases}$$

Les solutions du système satisfont ainsi

$$y = -4z, \quad x = 5z.$$

Cette méthode d'élimination par ligne consiste à changer l'ensemble générateur de l'idéal $I = \langle f_1, f_2 \rangle$ par un autre ensemble générateur. On soustrait deux fois la première ligne à la seconde et on remplace la seconde ligne par cette nouvelle ligne. On construit ainsi un nouveau polynôme

$$f_3 = f_2 - 2f_1 = y + 4z,$$

qui remplace le polynôme f_2 dans le système. Comme $f_3 = f_2 - 2f_1$, on a $f_3 \in I$ et comme $f_2 = 2f_1 + f_3$, on a $f_2 \in \langle f_1, f_3 \rangle$, ainsi

$$I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle .$$

On modifie ainsi l'ensemble des générateurs de I permettant de déterminer plus facilement l'ensemble algébrique affine :

$$\mathbf{V}(f_1, f_2) = \mathbf{V}(f_1, f_3) = \{(5z, -4z, z) \mid z \in \mathbb{R}\}.$$

Le processus par lequel le polynôme f_2 est remplacé par f_3 en utilisant f_1 est appelé une *réduction* de f_2 par f_1, on note

$$f_2 \xrightarrow{f_1} f_3.$$

Le nouveau polynôme f_3 apparaît comme un reste de la division du polynôme $2x + 3y + 2z$ par $x + y - z$:

$$\begin{array}{rrr|l} 2x & +3y & +2z & x + y - z \\ \cline{4-4} 2x & +2y & -2z & 2 \\ \cline{1-3} & y & +4z & \end{array}$$

III.1.3. Question de l'appartenance à un idéal.— Étant donné un polynôme f de $\mathbb{R}[x, y, z]$, a-t-on $f \in I = \langle f_1, f_3 \rangle$? Si f est dans I, il peut s'écrire comme combinaison des polynômes générateurs de I :

$$f = h_1 f_1 + h_3 f_3,$$

avec $h_1, h_3 \in \mathbb{R}[x, y, z]$. Si le « *terme dominant* » (le pivot !) de f_1 est x et le « *terme dominant* » de f_3 est y, tout polynôme de $\mathbb{R}[x, y, z]$ se réduit via f_1 et f_3 en un polynôme d'indéterminée z. De plus, un polynôme en z ne peut pas être réduit par réduction via f_1 et f_3. On a

$$f \in I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle \quad \text{si, et seulement si,} \quad f \xrightarrow{f_1, f_3} 0.$$

III.1.4. Exemple.— Considérons maintenant la situation de 3 polynômes linéaires

$$f_1 = y - z, \quad f_2 = x + 2y + 3z, \quad f_3 = 3x - 4y + 2z$$

de $\mathbb{R}[x,y,z]$. On considère l'idéal engendré par ces trois polynômes, $I = \langle f_1, f_2, f_3 \rangle$ et l'ensemble algébrique affine $\mathbf{V}(f_1, f_2, f_3)$ formée des solutions du système suivant

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ 3x - 4y + 2z = 0 \end{cases}$$

Par élimination, on peut réduire ce système au suivant

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ -10y - 7z = 0 \end{cases}$$

en retranchant 3 fois la seconde ligne à la troisième, puis au système

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ -17z = 0 \end{cases}$$

en retranchant -10 fois la première ligne à la troisième On a les réduction

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z.$$

On a un nouvel ensemble générateur pour I :

$$I = \langle f_1, f_2, f_3 \rangle = \langle f_1, f_2, -17z \rangle .$$

L'objectif est d'étudier la situation plus générale où les polynômes ne sont pas linéaires. Pour faire la division, on doit choisir un ordre sur les indéterminées. En effet, dans le deuxième exemple, on a considéré comme premier pivot x, fait l'élimination dans la troisième équation, puis l'élimination de y. Le choix de cet ordre est essentiel pour la généralisation aux polynômes non linéaires. L'ordre est ici

$$x < y < z.$$

Avec cet ordre, le terme dominant de f_1 est y, celui de f_2 est x et celui de f_3 est $3x$. La réduction

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z.$$

consiste à soustraire des multiples de f_1 et f_2 dans f_3. On utilise les termes dominants de f_1 et f_2. Le terme $-17z$ ne peut être réduit plus en utilisant les termes dominants de f_1 et f_2.

§ 2 Structure des idéaux d'un anneau euclidien

On commence notre étude par le cas des polynômes à une indéterminée.

III.2.1. Retour sur les anneaux euclidiens.— On rappelle qu'un anneau euclidien est un anneau commutatif A vérifiant les deux propriétés suivantes

i) A est *intègre*, i.e., pour tous éléments a et b de A,

$$ab = 0 \Rightarrow (\, a = 0 \text{ ou } b = 0\,).$$

ii) il existe sur A un algorithme euclidien, i.e., une application

$$\varphi : A - \{0\} \longrightarrow \mathbb{N},$$

telle que, pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq + r, \quad \text{avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

III.1 Théorème. — Si A est un anneau euclidien, tout idéal de A est engendré par un élément.

Preuve. Soit A un anneau euclidien, muni d'un algorithme euclidien φ, et soit I un idéal de A. Si I est nul, il est engendré par 0, on a $I = \langle 0 \rangle$. Si I est non nul, alors $\varphi(I - \{0\})$ est une partie non vide de $\mathbb{N}$, elle a donc un plus petit élément n. Soit $b \in I - \{0\}$, tel que $\varphi(b) = n$. Tout élément a de I s'écrit $a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b) = n$. Or

$$r = a - bq \in I,$$

donc par minimalité de n, on ne peut pas avoir $\varphi(r) < n$, d'où nécessairement $r = 0$. Par suite, tout élément a de I s'écrit $a = bq$, ainsi $I = \langle b \rangle$. □

III.2.2. Anneaux principaux.— Soit A un anneau et I un idéal de A. On dit que I est *principal* s'il est engendré par un élément, c'est-à-dire, s'il existe un élément a de A, tel que $I = \langle a \rangle$. Un anneau est dit *principal* s'il est intègre et si tout idéal de A est principal. Le théorème III.1 montre l'implication

$$\text{euclidien} \quad \Rightarrow \quad \text{principal}.$$

III.2 Théorème. —

i) L'anneau $\mathbb{Z}$ est principal.

ii) Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est principal.

Preuve. C'est une conséquence immédiate du fait que les anneaux $\mathbb{Z}$ et $\mathbb{K}[x]$ sont euclidiens. □

Exercice 59. —

1. Montrer que l'anneau $\mathbb{Z}[x]$ n'est pas principal. [indication : considérer l'idéal engendré par les polynômes 2 et x]
2. Montrer que si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x,y]$ n'est pas principal. [indication : considérer l'idéal engendré par les polynômes x et y.]

§ 3 Les idéaux de $\mathbb{K}[x]$

III.3.1. Générateurs des idéaux de $\mathbb{K}[x]$.— Soit $\mathbb{K}$ un corps. D'après la section précédente, tout idéal I de $\mathbb{K}[x]$ est engendré par un élément. Dans ce cas, la construction de la preuve du théorème III.1 s'exprime de la façon suivante. L'idéal nul est engendré par le polynôme nul. Soit I un idéal non nul de $\mathbb{K}[x]$; notons g le polynôme non nul de I de plus petit degré. Pour tout polynôme f de I, d'après le théorème de la division euclidienne, théorème I.2, il existe des polynômes q et r de $\mathbb{K}[x]$ tels que

$$f = qg + r,$$

avec $\deg(r) < \deg(g)$. Si r est non nul, alors $r = f - qg \in I$, ce qui contredit le choix de g, car $\deg(r) < \deg(g)$. Par conséquent, on a $r = 0$ et $f = qg$. Ainsi $I \subseteq \langle g \rangle$. Comme $g \in I$, on a l'égalité :

$$I = \langle g \rangle .$$

Le polynôme g ainsi obtenu est unique à un facteur près. C'est une conséquence du fait que si $\langle g_1 \rangle = \langle g_2 \rangle$, alors g_1 divise g_2 et g_2 divise g_1, donc il existe un scalaire λ tel que $g_1 = \lambda g_2$. On peut dire que le polynôme g obtenu dans cette preuve est le « *meilleur* » polynôme générateur pour l'idéal I.

III.3.2. Problème du calcul d'un générateur.— Étant donné un idéal I de $\mathbb{K}[x]$, comment calculer un polynôme g tel que $I = \langle g \rangle$? Dans un premier temps, nous allons aborder ce problème dans le cas d'un idéal engendré par deux polynômes, dont l'un au moins n'est pas nul :

$$I = \langle f_1, f_2 \rangle .$$

Par exemple, comment trouver un générateur pour l'idéal $I = \langle f_1, f_2 \rangle$ avec $f_1 = x^4 - 1$ et $f_2 = x^6 - 1$?

III.3.3. Plus grand commun diviseur.— Rappelons que le *plus grand commun diviseur* de f_1 et f_2, noté $\mathrm{pgcd}(f_1, f_2)$, est le polynôme g vérifiant les trois assertions suivantes

i) g divise f_1 et g divise f_2,

ii) si un polynôme h de $\mathbb{K}[x]$ divise f_1 et f_2, alors h divise g,

iii) $\mathrm{lc}(g) = 1$.

On a

III.3 Proposition. — Soient f_1 et f_2 deux polynômes de $\mathbb{K}[x]$, dont l'un au moins est non nul. Alors, le pgcd de f_1 et f_2 existe et on a

$$\langle f_1, f_2 \rangle = \langle \mathrm{pgcd}(f_1, f_2) \rangle .$$

Preuve. D'après la section III.3.1, il existe un polynôme g de $\mathbb{K}[x]$ tel que

$$\langle f_1, f_2 \rangle = \langle g \rangle .$$

Le polynôme g étant unique à un facteur près, on peut supposer que $\mathrm{lc}(g) = 1$. Montrons que $g = \mathrm{pgcd}(f_1, f_2)$. Comme $f_1, f_2 \in \langle g \rangle$, alors g divise à la fois f_1 et f_2. Supposons qu'un polynôme h

divise à la fois f_1 et f_2. Comme g est dans l'idéal $\langle f_1, f_2\rangle$, il existe une décomposition de g en

$$g = h_1 f_1 + h_2 f_2,$$

où h_1 et h_2 sont deux polynômes de $\mathbb{K}[x]$. Par suite, h divise g. □

Remarque III.4. — La preuve de la proposition précédente permet également de montrer l'existence et l'unicité du pgcd de deux polynômes.

Le problème de trouver un unique générateur de l'idéal $\langle f_1, f_2\rangle$ se réduit ainsi à celui du calcul du pgcd de f_1 et f_2.

Exercice 60. — Soient f et g deux polynômes de $\mathbb{K}[x]$. Montrer qu'il existe des polynômes u et v de $\mathbb{K}[x]$, tels que

$$uf + vg = \text{pgcd}(f, g).$$

III.3.4. Algorithme de la division euclidienne.— L'*algorithme d'Euclide* permet de calculer le pgcd en utilisant l'algorithme de division vu dans le premier chapitre. Il est basé sur le résultat suivant :

III.5 Proposition. — Soient f_1 et f_2 deux polynômes de $\mathbb{K}[x]$, dont l'un au moins est non nul. Alors,

$$\text{pgcd}(f_1, f_2) = \text{pgcd}(f_1 - qf_2, f_2),$$

pour tout polynôme q de $\mathbb{K}[x]$.

Preuve. Soit q un polynôme non nul. On a $f_1 = f_1 - qf_2 + qf_2$, par suite

$$\langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle .$$

D'après la proposition III.3, on a

$$\langle \text{pgcd}(f_1, f_2)\rangle = \langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle = \langle \text{pgcd}(f_1 - qf_2, f_2)\rangle .$$

Par suite, $\text{pgcd}(f_1, f_2)$ et $\text{pgcd}(f_1 - qf_2, f_2)$ sont égaux à une constante multiplicative près. Le pgcd de deux polynômes étant de coefficient dominant égal à 1, on en déduit l'égalité recherchée $\text{pgcd}(f_1, f_2) = \text{pgcd}(f_1 - qf_2, f_2)$. □

ENTRÉE : $f_1, f_2 \in \mathbb{K}[x]$, non tous les deux nuls,

SORTIE : $f = \text{pgcd}(f_1, f_2)$.

INITIALISATION : $f := f_1$; $g := f_2$

TANT QUE : $g \neq 0$ **FAIRE**

$f \xrightarrow{g} r$, où r est le reste de la division de f par g,

$f := g$,

$g := r$,

$f := \frac{1}{\text{lc}(f)} f$.

L'algorithme d'Euclide.

Exercice 61. — Montrer que l'algorithme d'Euclide termine.

III.3.5. Exemple.— Illustrons l'algorithme d'Euclide sur le calcul du pgcd des polynômes $f_1 = x^3 + x^2 - 5x + 3$ et $f_2 = x^2 + x - 2$ de $\mathbb{Q}[x]$.

INITIALISATION : $f := x^3 + x^2 - 5x + 3$, $g := x^2 + x - 2$.
Début de la boucle **TANT QUE :**
Première itération de la boucle **TANT QUE :**
$x^3 + x^2 - 5x + 3 \xrightarrow{g} -3x + 3$,
$f := x^2 + x - 2$,
$g := -3x + 3$,
Deuxième itération de la boucle **TANT QUE :**
$x^2 + x - 2 \xrightarrow{g} 0$,
$f := -3x + 3$,
$g := 0$,
Arrêt de la boucle **TANT QUE :**
$f := \frac{1}{\text{lc}(f)} f = \frac{1}{-3}(-3x + 3) = x - 1$.

Par suite, $\text{pgcd}(f_1, f_2) = x - 1$.

III.3.6. Exemple.— Pour calculer le pgcd des polynômes $f_1 = x^4 - 1$ et $f_2 = x^6 - 1$:

$$\begin{aligned} x^4 - 1 &= 0(x^6 - 1) + x^4 - 1, \\ x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1 \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0. \end{aligned}$$

Ainsi

$$\text{pgcd}(f_1, f_2) = \text{pgcd}(x^6 - 1, x^4 - 1) = \text{pgcd}(x^4 - 1, x^2 - 1) = \text{pgcd}(x^2 - 1, 0) = x^2 - 1.$$

En conséquence,

$$\langle f_1, f_2 \rangle = \langle x^2 - 1 \rangle .$$

III.3.7. Cas d'un idéal engendré par plus de deux polynômes.— Considérons un idéal $I = \langle f_1, \ldots, f_s \rangle$ de $\mathbb{K}[x]$ engendré par des polynômes non tous nuls. Rappelons que le *plus grand commun diviseur* des polynômes $f_1, \ldots, f_s$, noté $\text{pgcd}(f_1, \ldots, f_s)$, est le polynôme g vérifiant les trois assertions suivantes

i) g divise f_i, pour tout $i \in [\![1, s]\!]$

ii) si un polynôme h de $\mathbb{K}[x]$ divise f_i, pour tout $i \in [\![1, s]\!]$, alors h divise g,

iii) $\text{lc}(g) = 1$.

On a

III.6 Proposition. — Soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x]$, non tous nuls. Alors,

i) $\langle f_1, \ldots, f_s \rangle = \langle \text{pgcd}(f_1, \ldots, f_s) \rangle$,

ii) pour $s \geq 3$, alors $\text{pgcd}(f_1, \ldots, f_s) = \text{pgcd}(f_1, \text{pgcd}(f_2, \ldots, f_s))$.

Preuve. Montrons l'assertion **i)**. L'anneau $\mathbb{K}[x]$ étant principal, il existe un polynôme g de $\mathbb{K}[x]$ tel que

$$\langle f_1, \ldots, f_s \rangle = \langle g \rangle .$$

Le polynôme g étant unique à une constante près, on peut supposer que $\text{lc}(g) = 1$. Montrons que $g = \text{pgcd}(f_1, \ldots, f_s)$. Comme $f_1, \ldots, f_s \in \langle g \rangle$, alors g divise tous les polynômes $f_1, \ldots, f_s$. Supposons qu'un polynôme h divise tous les polynômes $f_1, \ldots, f_s$. Comme g est dans l'idéal $\langle f_1, \ldots, f_s \rangle$, il existe une décomposition de g en

$$g = h_1 f_1 + h_2 f_2 + \ldots + h_s f_s,$$

où $h_1, h_2, \ldots, h_s$ sont des polynômes de $\mathbb{K}[x]$. Par suite, h divise g.

Montrons l'assertion **ii)**. Posons $h = \text{pgcd}(f_2, \ldots, f_s)$. D'après **i)**, on a $\langle f_2, \ldots, f_s \rangle = \langle h \rangle$. Ainsi

$$\langle f_1, \ldots, f_s \rangle = \langle f_1, h \rangle .$$

Toujours d'après **i)**,

$$\text{pgcd}(f_1, \ldots, f_s) = \text{pgcd}(f_1, h) = \text{pgcd}(f_1, \text{pgcd}(f_2, \ldots, f_s)).$$

□

III.3.8. Exemple.— Calculons le générateur de l'idéal

$$I = \left\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \right\rangle \subset \mathbb{K}[x].$$

On a

$$\begin{aligned} \text{pgcd}(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \text{pgcd}(x^3 - 3x + 2, \text{pgcd}(x^4 - 1, x^6 - 1)) \\ &= \text{pgcd}(x^3 - 3x + 2, x^2 - 1) = x - 1. \end{aligned}$$

Ainsi

$$I = \langle x - 1 \rangle .$$

III.3.9. Problèmes.— Nous pouvons répondre dans le cas d'une indéterminée aux problèmes posés dans le chapitre précédent.

a) Problème de la description d'un idéal :

- tout idéal I de $\mathbb{K}[x]$ possède un unique générateur,
- il existe un « *meilleur* » générateur, c'est le pgcd des polynômes qui engendrent I.

b) Problème de l'appartenance à un idéal :

étant donné un idéal $I = \langle f_1, \ldots, f_s \rangle$ et un polynôme f de $\mathbb{K}[x]$, pour déterminer si $f \in I$, on calcule $g = \text{pgcd}(f_1, \ldots, f_s)$, puis on divise f par g. Le reste de cette division est nul si, et seulement si, $f \in I$, i.e.,

$$f \xrightarrow{g} 0 \quad \text{si, et seulement si,} \quad f \in I = \langle g \rangle .$$

c) Problème de la résolution d'équations polynomiales :

étant donnés des polynômes $f_1, \ldots, f_s$ de $\mathbb{K}[x]$, les solutions dans $\mathbb{K}$ du système d'équations polynomiales

$$\begin{cases} f_1(x) = 0 \\ \quad \vdots \\ f_s(x) = 0 \end{cases}$$

sont les solutions de l'équation

$$g(x) = 0,$$

où $g = \text{pgcd}(f_1, \ldots, f_s)$.

III.3.10. Exemple.— Comment déterminer si le polynôme $f = x^3 + 4x^2 + 3x - 7$ appartient à l'idéal

$$I = \left\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \right\rangle .$$

On a montré que $I = \langle x - 1 \rangle$. On a calcule la division de f par $x - 1$:

$$x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1.$$

Ainsi, la réduction de f par $x - 1$ est 1 :

$$x^3 + 4x^2 + 3x - 7 \xrightarrow{x-1} 1$$

On en déduit que f n'appartient pas à l'idéal I.

Exercice 62. — Déterminer si le polynôme f est contenu dans l'idéal I de $\mathbb{K}[x]$.

1. $f = x^2 - 3x + 2$, $I = \langle x - 2 \rangle$,
2. $f = x^5 - 4x + 1$, $I = \left\langle x^3 - x^2 + x \right\rangle$,
3. $f = x^2 - 4x + 4$, $I = \left\langle x^4 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8 \right\rangle$,
4. $f = x^3 - 1$, $I = \left\langle x^9 - 1, x^5 + x^3 - x^2 - 1 \right\rangle$.

Exercice 63. — Étant donnés des polynômes $f_1, \ldots, f_s$ de $\mathbb{K}[x]$, existe-t-il un algorithme pour décider si l'ensemble algébrique affine $\mathbf{V}(f_1, \ldots, f_s)$ est non vide ? Dans le cas où $\mathbb{K} = \mathbb{C}$ la réponse est affirmative.

1. Soit f est un polynôme non nul de $\mathbb{C}[x]$, montrer que $\mathbf{V}(f)$ est vide si, et seulement si, f est constant.
2. Soit $f_1,\dots,f_s$ des polynômes de $\mathbb{C}[x]$. Montrer que $\mathbf{V}(f_1,\dots,f_s)$ est vide si, et seulement si, $\operatorname{pgcd}(f_1,\dots,f_s)=1$.
3. Décrire une méthode algorithmique pour déterminer si $\mathbf{V}(f_1,\dots,f_s)$ est non vide.
4. Que peut-on dire dans le cas où $\mathbb{K}=\mathbb{R}$?

III.3.11. En conclusion.— Nous avons vu que la notion de réduction via l'algorithme de division est un point clef dans la résolution des problèmes mentionnés en III.3.9. Nous n'avons pas mis en évidence l'importance d'ordonner les termes dans le cas d'une seule indéterminée, car il existe un ordre naturel dans ce cas, celui donné par le degré des termes. Dans la réduction

$$f \xrightarrow{g} f - \frac{\operatorname{lt}(f)}{\operatorname{lt}(g)}g,$$

le reste $f-\frac{\operatorname{lt}(f)}{\operatorname{lt}(g)}g$ est de degré strictement inférieur au degré de f. C'est la raison pour laquelle l'algorithme termine ; c'est une conséquence du fait que

$$n<m \quad \text{si, et seulement si} \quad x^n \text{ divise } x^m.$$

La fin de ce chapitre est consacré au problème de cette réduction dans le cas de plusieurs indéterminées.

§ 4 Les ordres monomiaux

Nous noterons $\mathscr{M}(x_1,\dots,x_n)$, ou $\mathscr{M}$ s'il n'y a pas de confusion, l'ensemble des monômes en les indéterminées $x_1,\dots,x_n$:

$$\mathscr{M}(x_1,\dots,x_n)=\{x^\alpha \mid \alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n\}.$$

III.4.1. Ordre monomial.— Un *ordre monomial* sur $\mathscr{M}$ est une relation $\preccurlyeq$ vérifiant les assertions suivantes

i) $\preccurlyeq$ est un ordre total sur $\mathscr{M}$,

ii) si $x^\alpha \preccurlyeq x^\beta$, alors $x^\alpha x^\gamma \preccurlyeq x^\beta x^\gamma$, pour tous x^α, x^β et x^γ dans $\mathscr{M}$,

iii) $1 \preccurlyeq x^\alpha$, pour tout $x^\alpha \in \mathscr{M}$.

III.4.2. Ordre lexicographique.— Étant donné un *ordre alphabétique*

$$x_n < \dots < x_2 < x_1$$

i.e., un ordre sur l'ensemble des indéterminées, on définit l'*ordre lexicographique* $\preccurlyeq_{\text{lex}}$ sur $\mathscr{M}$ en posant, pour tous n-uplets d'entiers naturels $\alpha=(\alpha_1,\dots,\alpha_n)$ et $\beta=(\beta_1,\dots,\beta_n)$,

$$x^\alpha \preccurlyeq_{\text{lex}} x^\beta$$

si, et seulement si, les premières coordonnées α_i et β_i, en partant de la gauche dans α et β, qui sont différentes satisfont à $\alpha_i<\beta_i$.

III.4.3. Exemple.— Supposons que l'on ait deux indéterminées avec l'ordre alphabétique $y < x$, on a

$$1 = y^0 \preccurlyeq_{\text{lex}} y \preccurlyeq_{\text{lex}} y^2 \preccurlyeq_{\text{lex}} y^3 \preccurlyeq_{\text{lex}} \cdots \preccurlyeq_{\text{lex}} x \preccurlyeq_{\text{lex}} yx \preccurlyeq_{\text{lex}} y^2x \preccurlyeq_{\text{lex}} \cdots \preccurlyeq_{\text{lex}} x^2 \preccurlyeq_{\text{lex}} yx^2 \preccurlyeq_{\text{lex}} \cdots$$

III.4.4. Remarque.— L'ordre lexicographique dépend de l'ordre alphabétique sur les indéterminées. Tout ordre alphabétique sur les indéterminées $x_1, \ldots, x_n$ définit un ordre lexicographique sur $\mathscr{M}(x_1, \ldots, x_n)$.

Exercice 64. — Montrer qu'il existe $n!$ ordres lexicographiques possibles sur cet ensemble de monômes.

Notons que $x^\alpha \preccurlyeq_{\text{lex}} x^\beta$ si, et seulement si, le premier entier non nul dans le n-uplet

$$\beta - \alpha = (\beta_1 - \alpha_1, \ldots, \beta_n - \alpha_n) \in \mathbb{Z}^n$$

est positif. Par exemple, si $z < y < x$, on a

a) $y^2z^4 \preccurlyeq_{\text{lex}} xy^2$, car $\beta - \alpha = (1, 0, -4)$,

b) $x^3y^2z^1 \preccurlyeq_{\text{lex}} x^3y^2z^4$, car $\beta - \alpha = (0, 0, 3)$.

c) $y^3z^4 \preccurlyeq_{\text{lex}} x$, car $\beta - \alpha = (1, -3, -4)$.

III.7 Proposition. — L'ordre lexicographique $\preccurlyeq_{\text{lex}}$ est un ordre monomial.

Exercice 65. — Montrer la proposition III.7.

III.4.5. Propriétés des ordres monomiaux.—

III.8 Proposition. — Soit $\preccurlyeq$ un ordre monomial sur $\mathscr{M}$. Soient x^α et x^β deux monômes de $\mathscr{M}$, tels que x^α divise x^β, alors $x^\alpha \preccurlyeq x^\beta$.

Preuve. Si le monôme x^α divise le monôme x^β, il existe alors un monôme x^γ dans $\mathscr{M}$, tel que $x^\beta = x^\alpha x^\gamma$. L'ordre $\preccurlyeq$ étant monomial, on a $1 \preccurlyeq x^\gamma$, d'où $x^\alpha \preccurlyeq x^\alpha x^\gamma = x^\beta$. □

Exercice 66. — Montrer qu'il n'y a qu'un seul ordre monomial sur $\mathscr{M}(x_1)$.

Tout bon ordre est un ordre total, remarque I.6.5. La réciproque est fausse en général, cependant pour les ordres monomiaux, on a

III.9 Proposition. — Tout ordre monomial sur $\mathscr{M}$ est un bon ordre.

En particulier, toute suite décroissante de monômes

$$\ldots \preccurlyeq x^{\alpha_{i_k}} \preccurlyeq \ldots \preccurlyeq x^{\alpha_{i_2}} \preccurlyeq x^{\alpha_{i_1}}$$

termine.

Exercice 67. — 1. Soit $\preccurlyeq$ un ordre monomial sur $\mathscr{M}(x_1,\ldots,x_{n+1})$, montrer que $\preccurlyeq$ induit un ordre monomial sur $\mathscr{M}(x_1,\ldots,x_n)$.

2. Soient x^α et x^β deux mônomes de $\mathscr{M}(x_1,\ldots,x_n)$, et k, l deux entiers naturels tels que

$$x^\alpha x_{n+1}^k \preccurlyeq x^\beta x_{n+1}^l.$$

Montrer que

$$x^\alpha \preccurlyeq x^\beta \text{ ou } k \leq l.$$

3. Montrer la proposition III.9. (Indication : on fera une récurrence sur le nombre d'indéterminée.)

III.4.6. Définitions.— Fixons un ordre monomial $\preccurlyeq$ sur $\mathscr{M}(x_1,\ldots,x_n)$. Tout polynôme non nul f de $\mathbb{K}[x_1,\ldots,x_n]$ peut s'écrire sous la forme

$$f = a_1 x^{\alpha_{i_1}} + a_2 x^{\alpha_{i_2}} + \ldots + a_r x^{\alpha_{i_r}},$$

où les a_k sont des scalaires non nul, les $x^{\alpha_{i_k}}$ des monômes de $\mathscr{M}(x_1,\ldots,x_n)$ deux à deux distincts et

$$x^{\alpha_{i_r}} \preccurlyeq \ldots \preccurlyeq x^{\alpha_{i_2}} \preccurlyeq x^{\alpha_{i_1}}.$$

Le n-uplet α_{i_1} est appelé le *multidegré* de f, on le note multideg(f) :

$$\text{multideg}(f) = \alpha \text{ tel que } x^\alpha \text{ est le plus grand monôme apparaissant dans } f.$$

On dit alors

i) que a_1 est le *coefficient de plus haut degré* de f (*leading coefficient*) de f, noté lc(f),

ii) que $a_1 x^{\alpha_{i_1}}$ est le *terme de plus haut degré* f (*leading term*), noté lt(f),

iii) que $x^{\alpha_{i_1}}$ est le *monôme de plus haut degré de* f (*leading monomial*), noté lm(f).

Si g est un second polynôme non nul de $\mathbb{K}[x_1,\ldots,x_n]$, on dit que f est de multidegré plus petit que g si le monôme de plus haut degré de f est plus petit que celui de g :

$$\text{multideg}(f) \leq \text{multideg}(g) \text{ si } \text{lm}(f) \preccurlyeq \text{lm}(g).$$

On pose, par ailleurs lc(0) = lt(0) = lm(0) = 0.

III.4.7. Remarque.— Un ordre monomial étant un bon ordre, on peut faire des raisonnements par récurrence sur le multidegré.

III.4.8. Exemple.— Considérons l'ordre alphabétique $z < y < x$ et soit f le polynôme

$$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2,$$

on a,

$$\text{multideg}(f) = (3,0,0),\ \text{lc}(f) = -5,\ \text{lm}(f) = x^3,\ \text{lt}(f) = -5x^3.$$

Exercice 68. — On fixe un ordre monomial sur $\mathscr{M}(x_1,\ldots,x_n)$.

1. Montrer que pour tous polynôme f et monôme m de $\mathbb{K}[x_1,\ldots,x_n]$, on a

$$\text{lt}(mf) = m\,\text{lt}(f).$$

2. Soient f et g des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$, a-t-on toujours $\mathrm{lt}(fg) = \mathrm{lt}(f)\,\mathrm{lt}(g)$?
3. Soient $f_1,\ldots,f_s,g_1,\ldots,g_s$ des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$. A-t-on

$$\mathrm{lm}(f_1g_1+\ldots+f_sg_s) = \mathrm{lm}(f_i)\mathrm{lm}(g_i),$$

pour un $i \in [\![1,s]\!]$?

III.10 Proposition. — On fixe un ordre monomial sur $\mathscr{M}(x_1,\ldots,x_n)$. Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. Le multidegré vérifie les propriétés suivantes :

i) $\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$;

ii) si $f+g$ est non nul, alors $\mathrm{multideg}(f+g) \leq \max(\mathrm{multideg}(f), \mathrm{multideg}(g))$ et si, de plus $\mathrm{multideg}(f) \neq \mathrm{multideg}(g)$, on a l'égalité.

Exercice 69. — Montrer la Proposition III.10.

Exercice 70. — On fixe un ordre monomial sur $\mathscr{M}(x_1,\ldots,x_n)$. Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. On admettra qu'il existe un unique polynôme d (le pgcd de f et g, noté $\mathrm{pgcd}(f,g)$) dans $\mathbb{K}[x_1,\ldots,x_n]$ [1] vérifiant

i) d divise f et d divise g,

ii) si un polynôme h de $\mathbb{K}[x_1,\ldots,x_n]$ divise f et g, alors h divise d,

iii) $\mathrm{lc}(d) = 1$.

1. Vérifier que $< f,g > \subseteq < \mathrm{pgcd}(f,g) >$.
2. Montrer que l'idéal $< f,g >$ est principal si et seulement si $< f,g > = < \mathrm{pgcd}(f,g) >$.
3. Montrer que $\mathrm{pgcd}(f,g)$ a un multidegré maximal parmi les diviseurs communs de f et g.
4. Vérifier que tout polynôme non nul de $< f,g >$ a un multidegré supérieur ou égal à celui de $\mathrm{pgcd}(f,g)$.
5. Montrer que si l'idéal $< f,g >$ contient un polynôme de même multidegré que celui de $\mathrm{pgcd}(f,g)$, alors $< f,g > = < \mathrm{pgcd}(f,g) >$.
6. On considère $K[x,y]$ et un ordre monomial sur $\mathscr{M}(x,y)$ tel que $y \preccurlyeq x$. Montrer que y a un multidegré minimal parmi les polynômes non nuls de l'idéal $< x,y >$.
7. Vérifier que 1 est le pgcd de x et y.

III.4.9. Ordre lexicographique gradué.— Étant donné un ordre alphabétique $x_n < \ldots < x_2 < x_1$, on définit l'*ordre lexicographique gradué* $\preccurlyeq_{\mathrm{grlex}}$ sur $\mathscr{M}$ de la façon suivante : pour $\alpha = (\alpha_1,\ldots,\alpha_n)$ et $\beta = (\beta_1,\ldots,\beta_n)$, on pose

$$x^\alpha \preccurlyeq_{\mathrm{grlex}} x^\beta$$

si, et seulement si,

$$\left(\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i\right) \quad \text{ou} \quad \left(\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \quad \text{et} \quad x^\alpha \preccurlyeq_{\mathrm{lex}} x^\beta\right).$$

1. Ce résultat suit du fait que, de même que pour une seule indéterminée, l'anneau $\mathbb{K}[x_1,\ldots,x_n]$ est un anneau factoriel, c'est-à-dire que tout polynôme se factorise de manière unique en produit de facteurs irréductibles.

Par exemple, avec $y < x$, on a

$$1 \preccurlyeq_{\text{grlex}} y \preccurlyeq_{\text{grlex}} x \preccurlyeq_{\text{grlex}} y^2 \preccurlyeq_{\text{grlex}} xy \preccurlyeq_{\text{grlex}} x^2 \preccurlyeq_{\text{grlex}} y^3$$

Exercice 71. — Montrer que $\preccurlyeq_{\text{grlex}}$ est un ordre monomial.

Exercice 72. — On considère les ordres $\preccurlyeq_{\text{lex}}$ et $\preccurlyeq_{\text{grlex}}$ sur $\mathscr{M}(x,y,z)$ à partir de l'ordre alphabétique $x > y > z$.

Classer par ordre lexicographique croissant, puis par ordre lexicographique gradué croissant les monômes suivants :

$$x^2y^3z^4, \quad x^3z, \quad x^2y^4, \quad y^7z^2, \quad xyz^2.$$

Exercice 73. — Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. Montrer que $\deg(fg) = \deg(f) + \deg(g)$ où deg désigne le degré total.

§ 5 Algorithme de division en plusieurs indéterminées

L'objectif de cette partie est de définir un algorithme de division pour les polynômes à plusieurs indéterminées qui généralise l'algorithme de division pour les polynômes à une indéterminée.

Dans $\mathbb{K}[x]$, la division d'un polynôme f par g donne une décomposition de f sous la forme

$$f = qg + r,$$

avec $\deg(r) < \deg(g)$, théorème I.2. Dans le cas général, l'objectif est de divisiser un polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$ par un ensemble de polynômes $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$. Nous allons voir que cela consiste à écrire le polynôme f sous la forme

$$f = u_1f_1 + \ldots + u_sf_s + r,$$

où les *quotients* sont les polynômes $u_1,\ldots,u_s \in \mathbb{K}[x_1,\ldots,x_n]$ et le *reste* est le polynôme $r \in \mathbb{K}[x_1,\ldots,x_n]$.

Le principe de l'algorithme de division d'un polynôme f à plusieurs indéterminées par un ensemble de polynômes $f_1,\ldots,f_s$ est le même que dans le cas à une seule indéterminée :

1. fixer un ordre sur les termes,
2. remplacer le terme dominant de f en multipliant un des f_i par un terme approprié et soustraire le résultat à f ; ce terme est alors un terme du quotient u_i,
3. procèder ainsi avec tous les polynômes $f_1,\ldots,f_s$.

III.5.1. Premier exemple.— Posons $f = xy^2 + 1$, $f_1 = xy + 1$ et $f_2 = y + 1$. On fixe l'ordre alphabétique $y < x$ et l'ordre lexicographique associé sur les termes. Le terme dominant $\mathrm{lt}(f) = xy^2$ est divisible par les termes dominants $\mathrm{lt}(f_1) = xy$ et $\mathrm{lt}(f_2) = y$:

$$\begin{array}{rl|l} xy^2 & +1 & xy+1 \\ \hline xy^2 & +y & y \\ \hline 1 & -y & \end{array}$$

$$\begin{array}{rr|l} 1 & -y & y+1 \\ \hline -y & -1 & -1 \\ \hline & 2 & \end{array}$$

Comme $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas 2, ce reste est irréductible. On a obtenu les réductions [2]

$$xy^2+1 \xrightarrow{f_1} 1-y \xrightarrow{f_2} 2.$$

On écrit

$$xy^2 \xrightarrow{f_1,f_2} 2.$$

Le polynôme f s'écrit alors sous la forme

$$xy^2+1 = y(xy+1)+(-1)(y+1)+2.$$

Nous aurions commencé par la division par f_2 :

$$\begin{array}{rr|l} xy^2 & +1 & y+1 \\ \hline xy^2 & +xy & xy \\ \hline -xy & +1 & \end{array}$$

$$\begin{array}{rr|l} -xy & +1 & xy+1 \\ \hline -xy & -1 & -1 \\ \hline 2 & & \end{array}$$

Comme $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas 2, ce reste est irréductible. On a obtenu les réductions

$$xy^2+1 \xrightarrow{f_2} -xy+1 \xrightarrow{f_1} 2,$$

soit

$$xy^2 \xrightarrow{f_2,f_1} 2.$$

Le polynôme f s'écrit alors sous la forme

$$xy^2+1 = (-1)(xy+1)+(xy)(y+1)+2.$$

On notera que les restes de ces deux divisions sont égaux, mais les quotients différents. Après la première réduction par f_2, on peut encore appliquer la réduction par f_2, car $\mathrm{lt}(f_2)$ divise $-xy$:

$$\begin{array}{rr|l} xy^2 & +1 & y+1 \\ \hline xy^2 & +xy & xy \\ \hline -xy & +1 & \end{array}$$

$$\begin{array}{rr|l} -xy & +1 & y+1 \\ \hline -xy & -x & -x \\ \hline x & +1 & \end{array}$$

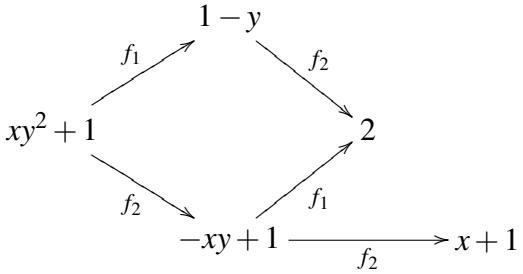
Le polynôme $x+1$ est le dernier reste, car les termes x et 1 ne sont pas divisibles par les

2. voir partie suivante 6

termes dominants de f_1 et f_2. Dans ce cas, la décomposition est

$$xy^2+1=(0)(xy+1)+(xy-x)(y+1)+(x+1).$$

La situation est la suivante :



III.5.2. Deuxième exemple.— Soient $f=x^2y+xy^2+y^2$, $f_1=xy-1$ et $f_2=y^2-1$. Comme dans les exemples précédents, on considère l'ordre lexicographique, avec l'ordre alphabétique $y<x$. On effectue la division de f par f_1 puis par f_2

$$\begin{array}{rl|l} x^2y & +xy^2 & +y^2 & xy & -1 \\ \hline x^2y & -x & & x & \\ \hline & x+xy^2 & +y^2 & & \end{array}$$

$$x^2y+xy^2+y^2 \xrightarrow{f_1} x+xy^2+y^2$$

$$\begin{array}{rl|l} xy^2 & +x & +y^2 & xy & -1 \\ \hline xy^2 & -y & & y & \\ \hline & x+y & +y^2 & & \end{array}$$

$$xy^2+x+y^2 \xrightarrow{f_1} x+y+y^2$$

Les termes dominants $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas le terme dominant $\mathrm{lt}\left(x+y^2+y\right)=x$. Cependant, $x+y^2+y$ n'est pas le reste, car $\mathrm{lt}(f_2)$ divise y^2. On extrait alors le terme x du reste et on poursuit la division :

$$\begin{array}{rl|l} y^2 & +y & y^2 & -1 \\ \hline y^2 & -1 & 1 & \\ \hline & y+1 & & \end{array}$$

$$x+y^2+y \xrightarrow{f_2} x+y+1$$

Après cette division, le reste est $x+y+1$. Les termes dominants de f_1 et f_2 ne divisent aucun terme de $x+y+1$, qui est ainsi le dernier reste. On a

$$\begin{aligned} x^2y+xy^2+y^2 &= (x)(xy-1)+(y)(xy-1)+(1)(y^2-1)+x+y+1 \\ &= (x+y)(xy-1)+(1)(y^2-1)+x+y+1 \end{aligned}$$

et

$$x^2y+xy^2+y^2 \xrightarrow{f_1,f_2} x+y+1.$$

Ces exemples illustrent le théorème suivant et le second exemple éclaire le fonctionnement de l'algorithme de division associé.

III.11 Théorème. — Soit $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Étant donné un ordre monomial $\preccurlyeq$ sur $\mathscr{M}(x_1, \ldots, x_n)$, tout polynôme non nul f de $\mathbb{K}[x_1, \ldots, x_n]$ s'écrit sous la forme

$$f = u_1 f_1 + \ldots + u_s f_s + r,$$

où $u_1, \ldots, u_s, r$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, tels que $r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$. On a de plus, pour tout quotient $u_i \neq 0$,

$$\mathrm{multideg}(u_i f_i) \leq \mathrm{multideg}(f).$$

Preuve. On fait un raisonnement par récurrence sur le multidegré. Soit f un polynôme non nul et supposons que le résultat est vérifié pour tout polynôme non nul de multidegré strictement inférieur à celui de f. Alors,

– ou bien il existe i, tel que $\mathrm{lt}(f_i)$ divise $\mathrm{lt}(f)$. Dans ce cas on choisit un tel j et on effectue la division de f par f_j et on obtient

$$f = \frac{\mathrm{lt}(f)}{\mathrm{lt}(f_j)} f_j + g$$

avec g nul ou $\mathrm{multideg}(g) < \mathrm{multideg}(f)$. Si g est nul, le résultat est vérifié car

$$\mathrm{multideg}\left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_j)} f_j\right) = \mathrm{multideg}(f).$$

Sinon, par hypothèse de récurrence,

$$g = u'_1 f_1 + \ldots + u'_j f_j + \ldots + u'_s f_s + r$$

où $u'_1, \ldots, u'_s, r$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, tels que
– $r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$;
– $\mathrm{multideg}(u'_i f_i) \leq \mathrm{multideg}(g) < \mathrm{multideg}(f)$ pour tout $u'_i \neq 0$.
On obtient

$$f = u'_1 f_1 + \ldots + \left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_i)} + u'_i\right) f_i + \ldots + u'_s f_s + r$$

avec les propriétés souhaitées car

$$\mathrm{multideg}\left(\left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_i)} + u'_i\right) f_i\right) = \mathrm{multideg}(f);$$

– ou bien le terme dominant $\mathrm{lt}(f)$ de f n'est divisible pas aucun des $\mathrm{lt}(f_i)$. Dans ce cas, si $f = \mathrm{lt}(f)$ c'est terminé, sinon on applique l'hypothèse de récurrence à $g = f - \mathrm{lt}(f)$. Alors

$$g = u_1 f_1 + \ldots + u_i f_i + \ldots + u_s f_s + r'$$

avec les bonnes propriétés et donc

$$f = u_1 f_1 + \ldots + u_i f_i + \ldots + u_s f_s + (\mathrm{lt}(f) + r')$$

avec les propriétés souhaitées.

□

Notons que dans les exemples précédents, les quotients u_i et le reste r ne sont pas uniques. Ils dépendent du choix de la suite des divisions effectuées.

III.5.3. Algorithme de division dans $\mathbb{K}[x_1,\ldots,x_n]$.— La preuve du théorème III.11 correspond à l'algorithme de division suivant

ENTRÉE : $f_1,\ldots,f_s,f \in \mathbb{K}[x_1,\ldots,x_n]$,
SORTIE : $u_1,\ldots,u_s,r \in \mathbb{K}[x_1,\ldots,x_n]$ tels que
$r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1),\ldots,\mathrm{lt}(f_s)$.
INITIALISATION : $u_1 := 0, \ldots u_s := 0, \quad r := 0, \quad p := f$;
TANT QUE : $p \neq 0$ **FAIRE**
  $i := 1$
  $div := faux$
  TANT QUE : $\left(i \leq s \text{ ET } div = faux \right)$ **FAIRE**
    SI ($\mathrm{lt}(f_i)$ divise $\mathrm{lt}(p)$) **ALORS**
      $u_i := u_i + \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$
      $p := p - \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$
      $div := vrai$
    SINON $i := i + 1$
  SI $div = faux$ **ALORS**
    $r := r + \mathrm{lt}(p)$
    $p := p - \mathrm{lt}(p)$

Algorithme de la division des polynômes à plusieurs indéterminées.

Cet algorithme est constitué de deux parties principales :
– une *étape de division*, si $\mathrm{lt}(f_i)$ divise $\mathrm{lt}(p)$ pour un i, l'algorithme procède à la division comme dans le cas d'une seule indéterminée avec le premier i vérifiant cette condition,
– une *étape de reste*, si $\mathrm{lt}(f_i)$ ne divise $\mathrm{lt}(p)$ pour aucun i, l'algorithme rajoute $\mathrm{lt}(p)$ au reste.

Le polynôme r obtenu par cet algorithme est appelé le *reste* de la division de f par $f_1,\ldots,f_s$, on note

$$f \xrightarrow{f_1,\ldots,f_s} r.$$

III.5.4. Remarque sur la non unicité du reste.— Contrairement à la division dans le cas d'une seule indéterminée, le reste n'est pas unique, il dépend de l'ordre des polynômes $f_1,\ldots,f_s$

dans l'algorithme de division. En effet, reprenons le deuxième exemple avec $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ et $f_2 = y^2 - 1$, avec l'ordre lexicographique associé à l'ordre alphabétique $y < x$. On a effectué la division de f par f_1 puis par f_2

$$f \xrightarrow{f_1} x + xy^2 + y^2 \xrightarrow{f_1} x + y + y^2 \xrightarrow{f_2} x + y + 1$$

soit

$$f \xrightarrow{f_1, f_2} x + y + 1.$$

Changeons l'ordre des diviseurs en prenant pour premier diviseur f_2 :

$$\begin{array}{l|l} x^2y + xy^2 + y^2 & y^2 - 1 \\ \hline xy^2 - x & x \\ \hline x^2y + y^2 + x & \end{array}$$

$$\begin{array}{l|l} x^2y + y^2 + x & y^2 - 1 \\ \hline y^2 - 1 & 1 \\ \hline x^2y + x + 1 & \end{array}$$

On divise alors le reste obtenu par f_1 :

$$\begin{array}{l|l} x^2y + x + 1 & xy - 1 \\ \hline x^2y - x & x \\ \hline 2x + 1 & \end{array}$$

On a ainsi

$$x^2y + xy^2 + y^2 = (x)(xy - 1) + (x + 1)(y^2 - 1) + 2x + 1.$$

Soit

$$f \xrightarrow{f_2} x^2y + y^2 + x \xrightarrow{f_2} x^2y + x + 1 \xrightarrow{f_1} 2x + 1$$

et donc

$$f \xrightarrow{f_2, f_1} 2x + 1.$$

Le reste obtenu par ce chemin de réduction n'est pas le même. Cet exemple illustre que l'ordre des polynômes $f_1, \ldots, f_s$ dans l'algorithme de division a une influence sur le reste r et les polynômes $u_1, \ldots, u_s$. Ce point est une obstruction à la résolution du problème de l'appartenance à un idéal. En effet, si après la division de f par $f_1, \ldots, f_s$, on obtient un reste nul, i.e.,

$$f = u_1 f_1 + \ldots + u_s f_s,$$

alors $f \in I = \langle f_1, \ldots, f_s \rangle$. On a

$$\text{si } f \xrightarrow{f_1, \ldots, f_s} 0, \quad \text{alors } f \in I.$$

Cependant, la réciproque n'est pas vraie comme le montre l'exemple suivant.

III.5.5. Exemple.— Soient $f = xy^2 - x$ et I l'idéal de $\mathbb{K}[x,y]$ engendré par les polynômes $f_1 = xy+1$ et $f_2 = y^2 - 1$. On a

$$xy^2 - x = y(xy+1) + 0(y^2-1) + (-x-y),$$

soit

$$f \xrightarrow{f_1,f_2} -x-y.$$

Mais si on considère l'ordre f_2, f_1, on a

$$xy^2 - x = x(y^2-1) + 0(xy+1) + 0,$$

ainsi

$$f \xrightarrow{f_2,f_1} 0,$$

par suite $f \in I$. C'est ainsi que l'on peut avoir $f \in I$ sans que f se réduise à 0 par un ensemble de polynômes qui engendrent I. L'algorithme de division que nous venons de construire présente sur ce point une difficulté. Pour remédier à cela, l'objectif est de construire un « *bon* » ensemble de générateurs pour l'idéal I. C'est-à-dire un ensemble de générateurs G de l'idéal I, pour lequel le reste de la division par G est unique, peu importe l'ordre utilisé sur les diviseurs $g_1, g_2, \ldots, g_t$ avec $G = \{g_1, \ldots, g_t\}$, et que l'on ait ainsi

$$f \in I \quad \text{si, et seulement si,} \quad f \xrightarrow{g_1,\ldots,g_t} 0.$$

L'existence d'un ensemble de générateur satisfaisant cette propriété fera l'objet du prochain chapitre et un algorithme de construction d'un tel ensemble du chapitre suivant .

Exercice 74.— Soit $f = x^7y^2 + x^3y^2 - y + 1$ un polynôme de $\mathbb{K}[x,y]$ et soient $f_1 = xy^2 - x$ et $f_2 = x - y^3$.

1. Calculer le reste de la division de f par f_1, f_2 en utilisant l'ordre lexicographique et l'ordre lexicographique gradué.
2. Même question avec les diviseurs dans l'ordre f_2, f_1.

Exercice 75.— Soient $f = xy^2z^2 + xy - yz$, $f_1 = x - y^2$, $f_2 = y - z^3$, $f_3 = z^2 - 1$. En utilisant l'ordre lexicographique,

1. calculer le reste de la division de f par f_1, f_2, f_3,
2. calculer le reste de la division de f par f_3, f_2, f_1.

Exercice 76.— On étudie la division du polynôme $f = x^3 - x^2y - x^2z + x$ par les polynômes $f_1 = x^2y - z$ et $f_2 = xy - 1$.

1. En utilisant l'ordre lexicographique gradué, calculer le reste de la division de f par f_1, f_2, puis par f_2, f_1.
2. Les deux restes sont différents, à quel moment dans le processus de division cette différence apparaît ?
3. Posons $r = r_1 - r_2$. A-t-on $r \in \langle f_1, f_2 \rangle$? Si oui, donner une décomposition $r = u_1 + u_2 f_2$, sinon expliquer pourquoi ?
4. Calculer le reste de la division de r par f_1, f_2. Ce résultat était-il prévisible ?
5. Trouver un autre polynôme $g \in \langle f_1, f_2 \rangle$, tel que le reste de la division de g par f_1, f_2 est non nul.
6. L'algorithme de la division donne-t-il une solution pour le problème de l'appartenance à l'idéal $\langle f_1, f_2 \rangle$?

Exercice 77. — 1. En utilisant l'ordre lexicographique gradué, donner un élément g de l'idéal

$$\langle f_1, f_2\rangle = \left\langle 2xy^2 - x, 3x^2y - y - 1\right\rangle \subset \mathbb{R}[x,y]$$

dont le reste de la division par f_1, f_2 est non nul.

2. Même question avec l'idéal

$$\langle f_1, f_2, f_3\rangle = \left\langle x^4y^2 - z, x^3y^2 - z, x^3y^3 - 1, x^2y^4 - 2z\right\rangle \subset \mathbb{R}[x,y,z].$$

§ 6 Division et réduction

III.6.1. Exemple.— Soit $f_1 = x^3 - 2xy \in \mathbb{Q}[x,y]$ muni de l'ordre lexicographique associé à $y < x$.

On peut interpréter la division d'un polynôme de $\mathbb{Q}[x,y]$ par f_1 comme une *réduction* par f_1. La division de x^3 par f_1 est de reste $2xy$ et en terme de réduction on a

$$x^3 \xrightarrow{f_1} 2xy.$$

Pour calculer le reste de la division de $x^4 + 3x^3y$ par f_1, on remplace Dans l'expression $x^4 + 3x^3y$, les occurrences du terme x^3 par le terme $2xy$:

$$x^4 + 3x^3y \xrightarrow{f_1} x(2xy) + 3x^3y \xrightarrow{f_1} x(2xy) + 3(2xy)y = 2x^2y + 6xy^2.$$

Le polynôme $2x^2y + 6xy^2$ ne possède pas de terme divisible par x^3 et correspond ainsi au reste recherché.

III.6.2. Réduction.— Soient f, g, h trois polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, avec g non nul. On dit que f se *réduit en une étape* en h modulo g et on note

$$f \xrightarrow{g} h,$$

si $\mathrm{lt}(g)$ divise un terme non nul X de f et que

$$h = f - \frac{X}{\mathrm{lt}(g)} g.$$

En particulier, un ordre monomial fixé, on a, pour tout polynôme f,

$$\mathrm{lt}(f) \xrightarrow{f} \mathrm{lt}(f) - f.$$

Par exemple, si $f = x^3y^2 - x^2y^3 + x$, avec l'ordre lexicographique gradué et $y < x$, on a

$$x^3y^2 \xrightarrow{f} x^2y^3 - x.$$

III.6.3. Exemple.— Considérons les polynômes $f = 6x^3y - x + y^4 + 4y^3 - 1$ et $g = 2xy + y^3$ de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique induit par $y < x$. On a $\mathrm{lt}(g) = 2xy$ qui divise $6x^3y$, d'où la réduction

$$f \xrightarrow{g} -3x^2y^3 - x + y^4 + 4y^3 - 1.$$

Si l'on considère l'ordre lexicographique gradué avec $y < x$, alors $\mathrm{lt}(g) = y^3$ et on a la réduction

$$f \xrightarrow{g} 6x^3y + y^4 - 8xy - x - 1.$$

Noter que, dans ce cas, la réduction ne porte ni sur le terme dominant de f qui vaut $6x^3y$, ni sur le terme de plus haut degré divisible par y^3. En général, on fera en premier la réduction sur le terme de plus haut degré divisible par $\mathrm{lt}(g) = y^3$, soit

$$f \xrightarrow{g} 6x^3y - 2xy^2 + 4y^3 - x - 1.$$

III.6.4. Définition.— Soient f, h des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ et $F = \{f_1, \ldots, f_s\}$ une famille de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$. On dit que f se *réduit* en h modulo F et on note

$$f \xrightarrow{F} h,$$

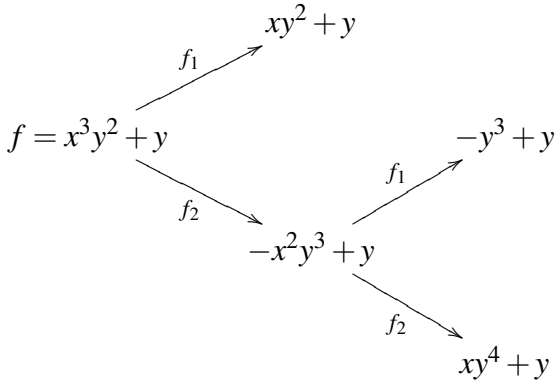
s'il existe une suite de réductions en une étape

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \ldots h_{i_{k-1}} \xrightarrow{f_{i_k}} h,$$

où $f_{i_j} \in F$ et $h_j \in \mathbb{K}[x_1, \ldots, x_n]$.

III.6.5. Exemple.— Soient $f_1 = x^2y - y$ et $f_2 = x^2 + xy$ des polynômes de $\mathbb{Q}[x, y]$, avec l'ordre lexicographique associé à $y < x$. On a donc en particulier $x^2y \xrightarrow{f_1} y$ et $x^2 \xrightarrow{f_2} xy$.

Soit $F = \{f_1, f_2\}$ et $f = x^3y^2 + y$. Alors,



soit

$$x^3y^2 + y \xrightarrow{F} xy^2 + y,$$
$$x^3y^2 + y \xrightarrow{F} -y^3 + y \text{ et}$$
$$x^3y^2 + y \xrightarrow{F} xy^4 + y,$$

ce qui correspond aux 3 réductions sous *formes normales* de f modulo F.

III.6.6. Formes normales.— Un polynôme r est dit en *forme normale* par rapport à un ensemble $F = \{f_1, \ldots, f_s\}$ de polynômes non nuls, si $r = 0$ ou si aucun des termes de r n'est divisible par $\mathrm{lt}(f_i)$, pour $i \in [\![1, s]\!]$. On dit aussi que le polynôme r ne peut pas être réduit modulo F.

III.6.7. Remarque.— Dans le cas de l'algorithme de division présenté dans la partie précédente, on choisit un ordre pour les polynômes $f_1, \ldots, f_s$. Une réduction sous forme normale d'un

polynôme modulo F correspond également à une division par les polynômes de F, mais sans fixer d'ordre sur le choix des diviseurs successifs. Par exemple, la réduction $x^3y^2+y \xrightarrow{F} -y^3+y$ en III.6.5 ne correspond ni à la division par f_1, f_2 $\left(x^3y^2+y \xrightarrow{f_1,f_2} xy^2+y\right)$, ni à la division par f_2, f_1 $\left(x^3y^2+y \xrightarrow{f_2,f_1} xy^4+y\right)$.

Pour un polynôme non nul f de $\mathbb{K}[x_1,\ldots,x_n]$, si $f \xrightarrow{F} r$, où r est en forme normale relativement à F, alors il existe des quotients $u_1,\ldots,u_s$ dans $\mathbb{K}[x_1,\ldots,x_n]$ tels que

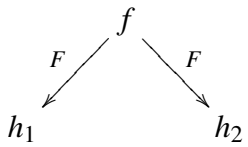
$$f = u_1f_1 + \ldots + u_sf_s + r$$

est une décomposition de f satisfaisant les propriétés du théorème III.11 : multideg$(u_if_i) \leq$ multideg(f) pour tout $u_i \neq 0$. En particulier, si $f \xrightarrow{F} 0$ alors $f \in \langle f_1,\ldots,f_s\rangle$.

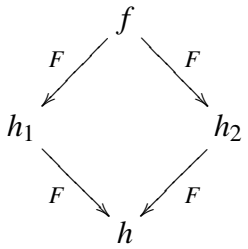
Réciproquement, par l'algorithme de division par $f_1,\ldots,f_s$, il existe toujours un polynôme r en forme normale par rapport à F tel que $f \xrightarrow{F} r$.

Exercice 78. — Reprendre l'exemple III.6.5 avec l'ordre lexicographique associé à $y > x$ et déterminer pour cet ordre les réductions de f modulo F sous forme normale.

III.6.8. Confluence.— Soit $F = \{f_1,\ldots,f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. On dit qu'une paire de réductions sur un même polynôme f modulo F

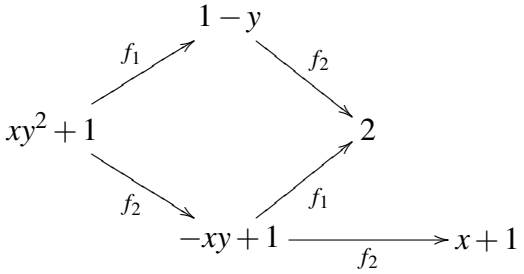


est *confluente* s'il existe un couple de réductions vers un même polynôme

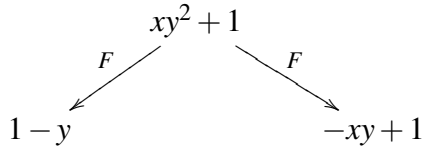


La relation de réduction $\xrightarrow{F}$ est dite *confluente* si toute paire l'est.
On verra que cette dernière propriété caractérise le fait d'être une *bonne* base.

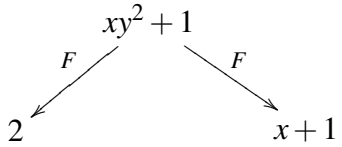
III.6.9. Exemple.— Reprenons le premier exemple III.5.1. Soient $f = xy^2+1$, $f_1 = xy+1$ et $f_2 = y+1$ trois polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique induit par $y < x$ et posons $F = \{f_1, f_2\}$. On a



La paire de réductions



est confluente, par contre la paire de réductions



ne l'est pas. La relation de réduction $\xrightarrow{F}$ n'est donc pas confluente.

Exercice 79. — Soit $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$. Montrer que relation de réduction $\xrightarrow{F}$ est confluente si, et seulement si, tout polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ a une unique réduction sous forme normale modulo F.

Exercice 80. — Soient $f_1 = x^2y - yz$, $f_2 = xy^2 - z^2$ et $f_3 = xz - y^2$ des polynômes de $\mathbb{R}[x, y, z]$, avec l'ordre lexicographique associé à $z < y < x$. Montrer que pour $F = \{f_1, f_2, f_3\}$, la relation de réduction $\xrightarrow{F}$ n'est pas confluente.

CHAPITRE
IV

Les bases de Gröbner

Sommaire

Dans ce chapitre, on considère un anneau de polynômes $\mathbb{K}[x_1,\dots,x_n]$ et on munit $\mathscr{M}[x_1,\dots,x_n]$ d'un ordre monomial.

§ 1 Les idéaux monomiaux

IV.1.1. Définition.— Un idéal I de $\mathbb{K}[x_1,\dots,x_n]$ est dit *monomial*, s'il existe une partie A de $\mathbb{N}^n$, éventuellement infinie, telle que I soit constitué de tous les polynômes s'exprimant comme somme finie de la forme

$$\sum_{\alpha\in A} h_\alpha x^\alpha,$$

où les h_α sont des polynômes de $\mathbb{K}[x_1,\dots,x_n]$.

Autrement dit, un idéal I est monomial s'il est engendré par des monômes, *i.e.* s'il existe une partie A de $\mathbb{N}^n$, telle que

$$I = \langle x^\alpha \mid \alpha \in A\rangle .$$

IV.1.2. Exemples.— L'idéal $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle$ est un idéal monomial de $\mathbb{K}[x,y]$. L'idéal $I = \langle x-y\rangle$ n'est pas monomial.

IV.1 Proposition. — Soit $I = \langle x^\alpha \mid \alpha \in A\rangle$ un idéal monomial. Un monôme x^β est dans I si, et seulement si, x^β est divisible par x^α, pour un $\alpha \in A$.

Preuve. Si x^β est divisible par un monôme x^α, $\alpha \in A$, alors, il existe un polynôme h de $\mathbb{K}[x_1,\ldots,x_n]$, tel que $x^\beta = hx^\alpha$, d'où $x^\beta \in I$.

Supposons que x^β soit un monôme de I. Il existe alors une décomposition

$$x^\beta = h_{\alpha(1)}x^{\alpha(1)} + \ldots + h_{\alpha(s)}x^{\alpha(s)},$$

où $h_{\alpha(i)} \in \mathbb{K}[x_1,\ldots,x_n]$ et $\alpha(i) \in A$. En développant chaque polynôme $h_{\alpha(i)}$, le terme de droite se décompose en une combinaison linéaire de monômes, et chaque monôme est divisible par un $x^{\alpha(i)}$. Par suite, x^β est divisible par un $x^{\alpha(i)}$. □

IV.2 Proposition. — Soit I un idéal monomial et soit f un polynôme de $\mathbb{K}[x_1,\ldots,x_n]$. Les assertions suivantes sont équivalentes

i) $f \in I$,

ii) tout terme de f est dans I,

iii) f est une combinaison linéaire de monômes de I.

Preuve. Supposons que $I = \langle x^\alpha \mid \alpha \in A\rangle$. Les implications **iii)** ⇒ **ii)** ⇒ **i)** sont immédiates. Si $f \in I$, alors

$$f = h_{\alpha(1)}x^{\alpha(1)} + \ldots + h_{\alpha(s)}x^{\alpha(s)},$$

où les $h_{\alpha(i)} \in \mathbb{K}[x_1,\ldots,x_n]$ et $\alpha(i) \in A$. En décomposant chaque polynôme $h_{\alpha(i)}$ en combinaison linéaire de monômes, on obtient **iii)**. □

On en déduit que deux idéaux monomiaux sont égaux, si et seulement si, ils contiennent les mêmes monômes.

IV.1.3. Le lemme de Dickson.— Le résultat suivant est important dans la suite, car il nous permettra de montrer que tout idéal de $\mathbb{K}[x_1,\ldots,x_n]$ possède une base finie.

IV.3 Théorème (lemme de Dickson). — Soit $I = \langle x^\alpha \mid \alpha \in A\rangle$ un idéal monomial de $\mathbb{K}[x_1,\ldots,x_n]$. Alors, il existe $\alpha(1),\ldots,\alpha(s) \in A$ tels que

$$I = \left\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\right\rangle.$$

En d'autres termes, tout idéal monomial possède une base finie.

Exercice 81. — Montrer le lemme de Dickson IV.3 pour les idéaux monomiaux de $\mathbb{K}[x]$.

Preuve. **(Idée !)** On procède par récurrence sur n. Pour le cas $n = 1$, voir l'exercice précédent. On suppose le théorème vrai au rang $n-1$. On considère alors l'anneau des polynômes à n indéterminées, que l'on notera $\mathbb{K}[x_1,\ldots,x_{n-1},y]$. Les monômes en les indéterminées $x_1,\ldots,x_{n-1},y$, s'écrivent sous la forme $x^\alpha y^m$, avec $\alpha = (\alpha_1,\ldots,\alpha_{n-1}) \in \mathbb{N}^{n-1}$ et $m \in \mathbb{N}$.

Supposons que I soit un idéal monomial de $\mathbb{K}[x_1,\ldots,x_{n-1},y]$. Considérons l'idéal J de $\mathbb{K}[x_1,\ldots,x_{n-1}]$ engendré par les monômes x^α, pour lesquels il existe m (dépendant de α) tel que $x^\alpha y^m \in I$.

Comme J est un idéal monomial de $\mathbb{K}[x_1,\dots,x_{n-1}]$, d'après l'hypothèse de récurrence, il existe $\alpha(1),\dots,\alpha(s)\in\mathbb{N}$, tels que

$$J=\left\langle x^{\alpha(1)},\dots,x^{\alpha(s)}\right\rangle.$$

Par construction de J, pour tout $i\in[\![1,s]\!]$, il existe $m_i\in\mathbb{N}$ tel que $x^{\alpha(i)}y^{m_i}\in I$. Soit $m=\max\{m_i \mid i\in[\![1,s]\!]\}$. Pour tout entier $k\in[\![0,m-1]\!]$, on définit l'idéal J_k de $\mathbb{K}[x_1,\dots,x_{n-1}]$ engendré par les monômes x^β, tels que $x^\beta y^k\in I$. D'après l'hypothèse de récurrence, J_k admet une base finie :

$$J_k=\left\langle x^{\alpha_k(1)},\dots,x^{\alpha_k(s_k)}\right\rangle.$$

On montre alors (exercice !) que l'idéal I est engendré par les monômes suivants

$$\begin{aligned}
x^{\alpha(1)}y^m,\dots,x^{\alpha(s)}y^m &\in J\\
x^{\alpha_0(1)},\dots,x^{\alpha_0(s_0)} &\in J_0\\
x^{\alpha_1(1)}y,\dots,x^{\alpha_1(s_1)}y &\in J_1\\
&\vdots\\
x^{\alpha_{m-1}(1)}y^{m-1},\dots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1} &\in J_{m-1}
\end{aligned}$$

Reste à montrer que cet ensemble fini de générateurs peut être choisi à partir d'un ensemble de générateurs de l'idéal. Ceci est une conséquence de la proposition IV.1 (exercice !). □

§ 2 Le théorème de la base de Hilbert

IV.2.1. L'idéal des termes dominants.— Soit I un idéal non nul de $\mathbb{K}[x_1,\dots,x_n]$. On note $\mathrm{lt}(I)$ l'ensemble des termes dominants des éléments de I :

$$\mathrm{lt}(I)=\{\mathrm{lt}(f) \mid f\in I\}.$$

On note $\langle\mathrm{lt}(I)\rangle$ l'idéal engendré par les éléments de $\mathrm{lt}(I)$, on l'appelle l'*idéal des termes dominants* de I. (L'idéal des termes dominants dépend de l'ordre monomial considéré.)

IV.2.2. Remarque.— Supposons que $I=\langle f_1,\dots,f_s\rangle$, pour tout $i\in[\![1,s]\!]$, on a

$$\mathrm{lt}(f_i)\in\mathrm{lt}(I)\subset\langle\mathrm{lt}(I)\rangle,$$

par suite

$$\langle\mathrm{lt}(f_1),\dots,\mathrm{lt}(f_s)\rangle\subset\langle\mathrm{lt}(I)\rangle.$$

Il est cependant possible que cette inclusion soit stricte, comme l'illustre l'exemple suivant.

IV.2.3. Exemple.— On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x,y]$, avec $y<x$. Soient $I=\langle f_1,f_2\rangle$ l'idéal de $\mathbb{R}[x,y]$ engendré par les polynômes $f_1=xy+1$ et $f_2=y^2-1$. Considérons le polynôme $f=xy^2-x$, on a

$$xy^2-x=y(xy+1)+0(y^2-1)+(-x-y),$$

et

$$xy^2 - x = x(y^2-1) + 0(xy+1) + 0.$$

La seconde équation montre que $f \in I$ et d'après la première équation, on a

$$-x - y = f - yf_1 \in I.$$

Ainsi $x+y \in I$ et $\mathrm{lt}(x+y) = x \in \langle \mathrm{lt}(I) \rangle$. Or

$$x \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle = \langle xy, y^2 \rangle,$$

car x n'est pas divisible par xy ou y^2. L'inclusion

$$\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle \subset \langle \mathrm{lt}(I) \rangle,$$

est ainsi stricte.

IV.4 Proposition. — Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ différent de l'idéal $\{0\}$. Alors

i) l'idéal $\langle \mathrm{lt}(I) \rangle$ est monomial,

ii) il existe des polynômes $g_1, \ldots, g_t \in I$, tels que $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$.

Preuve. Montrons **i)**. Considérons l'idéal engendré par les monômes dominants des polynôme non nul de I,

$$\langle \mathrm{lm}(g) \mid g \in I - \{0\} \rangle.$$

On a $\mathrm{lt}(g) = \mathrm{lc}(g)\mathrm{lm}(g)$, ainsi $\mathrm{lm}(g)$ et $\mathrm{lt}(g)$ ne diffèrent que d'un facteur multiplicatif près de $\mathbb{K}$, par suite

$$\langle \mathrm{lm}(g) \mid g \in I - \{0\} \rangle = \langle \mathrm{lt}(g) \mid g \in I - \{0\} \rangle,$$

Or $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g) \mid g \in I - \{0\} \rangle$, d'où

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lm}(g) \mid g \in I - \{0\} \rangle$$

et $\langle \mathrm{lt}(I) \rangle$ est un idéal monomial.

Montrons **ii)**. Comme $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lm}(g) \mid g \in I - \{0\} \rangle$, d'après le lemme de Dickson, théorème IV.3, il existe des polynômes $g_1, \ldots, g_t$ tels que

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle$$

comme, pour tout i, $\mathrm{lm}(g_i)$ et $\mathrm{lt}(g_i)$ ne diffèrent que d'un facteur multiplicatif près de $\mathbb{K}$, par suite

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle.$$

□

Exercice 82. — Soit I l'idéal de $\mathbb{R}[x,y,z]$ engendré par les trois polynômes

$$g_1 = xy^2 - xz + y, \quad g_2 = xy - z^2, \quad g_3 = x - yz^4.$$

En utilisant l'ordre lexicographique, donner un polynôme g de I tel que

$$\mathrm{lt}(g) \notin \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2), \mathrm{lt}(g_3) \rangle .$$

Exercice 83. — On considère les idéaux étudiés dans les exercices 76 et 77 du chapitre précédent :

1. $I = \langle f_1, f_2 \rangle \subset \mathbb{R}[x,y,z]$ avec $f_1 = x^2y - z$ et $f_2 = xy - 1$.
2. $I = \langle f_1, f_2 \rangle \subset \mathbb{R}[x,y]$ avec $f_1 = 2xy^2 - x$, $f_2 = 3x^2y - y - 1$.
3. $I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{R}[x,y,z]$ avec $f_1 = x^4y^2 - z$, $f_2 = x^3y^2 - z$, $f_3 = x^3y^3 - 1$, $f_4 = x^2y^4 - 2z$.

En utilisant l'ordre lexicographique gradué, dans chaque cas, montrer que l'idéal $\langle \mathrm{lt}(I) \rangle$ est strictement plus grand que l'idéal engendré par les termes $\mathrm{lt}(f_i)$.

IV.2.4. Le théorème de la base de Hilbert.— De la proposition IV.4 et de l'algorithme de division, nous montrons que tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ est engendré par un nombre fini de polynômes.

IV.5 Théorème (Théorème de la base de Hilbert). — Tout idéal I de $\mathbb{K}[x_1, \ldots, x_n]$ possède un nombre fini de générateurs, *i.e.*, il existe des polynômes $g_1, \ldots, g_t$ de I, tels que $I = \langle g_1, \ldots, g_t \rangle$.

Autrement dit, tout idéal de $\mathbb{K}[x_1, \ldots, x_n]$ possède une base finie.

Preuve. Fixons un ordre monomial sur $\mathscr{M}(x_1, \ldots, x_n)$. Si I est l'idéal nul, on peut prendre 0 comme générateur : $I = \{0\} = \langle 0 \rangle$. Supposons I non nul, alors il contient au moins un polynôme non nul. D'après la proposition IV.4 **ii)**, il existe des polynômes $g_1, \ldots, g_t$ de I tels que

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle .$$

Montrons que $I = \langle g_1, \ldots, g_t \rangle$. Comme $g_1, \ldots, g_t \in I$, l'inclusion $\langle g_1, \ldots, g_t \rangle \subset I$ est immédiate. Inversement, soit f un polynôme de I et $G = \{g_1, \ldots, g_t\}$. L'algorithme de division par $g_1, \ldots, g_t$ donne une réduction $f \xrightarrow{G} r$ de f modulo G sous forme normale, c'est-à-dire une décomposition

$$f = u_1 g_1 + \ldots + u_t g_t + r,$$

où $u_1, \ldots, u_t, r$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, tels que $r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)$. Montrons que $r = 0$. On a

$$r = f - u_1 g_1 - \ldots - u_t g_t \in I.$$

Si $r \neq 0$, alors

$$\mathrm{lt}(r) \in \langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle .$$

D'après la proposition IV.1, $\mathrm{lt}(r)$ est alors divisible par un $\mathrm{lt}(g_i)$, ce qui contredit la propriété de r. Par suite, $r = 0$ et on a

$$f = u_1 g_1 + \ldots + u_t g_t \in \langle g_1, \ldots, g_t \rangle .$$

Ainsi $I \subset \langle g_1, \ldots, g_t \rangle$, qui termine la preuve. □

IV.2.5. Suites croissantes d'idéaux.— Voici une première application du théorème de la base de Hilbert.

IV.6 Théorème (Propriété des suites croissantes d'idéaux). — Si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

est une suite croissante d'idéaux de $\mathbb{K}[x_1,\ldots,x_n]$, alors il existe un rang $N \geq 1$ tel que

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

Exercice 84 (preuve du théorème IV.6). — Considérons une suite croissante d'idéaux de $\mathbb{K}[x_1,\ldots,x_n]$:

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

1. Montrer que $I = \bigcup_{i=1}^{\infty} I_i$ est un idéal de $\mathbb{K}[x_1,\ldots,x_n]$.
2. En déduire le théorème IV.6.

IV.2.6. Ensemble algébrique affine d'un idéal.— Voici une autre application, de nature géométrique, du théorème de la base de Hilbert.

Soit I un idéal de $\mathbb{K}[x_1,\ldots,x_n]$. On note $\mathbf{V}(I)$ le sous-ensemble de $\mathbb{K}^n$ défini par

$$\mathbf{V}(I) = \{(a_1,\ldots,a_n) \in \mathbb{K}^n \mid f(a_1,\ldots,a_n) = 0, \text{ pour tout } f \in I\}.$$

Du théorème de la base de Hilbert, on déduit

IV.7 Proposition. — Pour tout idéal I de $\mathbb{K}[x_1,\ldots,x_n]$, $\mathbf{V}(I)$ est un ensemble algébrique affine. En particulier, si $I = \langle f_1,\ldots,f_s\rangle$, alors $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$.

Exercice 85. — Montrer la proposition IV.7.

§ 3 Les bases de Gröbner

La base $\{g_1,\ldots,g_t\}$ obtenue dans le théorème de la base de Hilbert, théorème IV.5 vérifie $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle$. Comme nous avons vu avec l'exemple IV.2.3, toutes les bases ne satisfont pas à cette propriété.

IV.3.1. Définition.— Un ordre monomial étant fixé, un sous-ensemble fini $G = \{g_1,\ldots,g_t\}$ d'un idéal I est appelé *base de Gröbner* (ou *base standard*) si

$$\langle \mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle = \langle \mathrm{lt}(I)\rangle .$$

IV.3.2. Remarque.— Un sous-ensemble fini $G = \{g_1, \ldots, g_t\}$ d'un idéal I est une base de Gröbner si, et seulement si, le terme dominant de tout élément de I est divisible par un des $\mathrm{lt}(g_i)$.

Exercice 86. — Vérifier la remarque IV.3.2.

IV.3.3. Exemple.— On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x,y]$ avec l'ordre alphabétique $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x,y]$ engendré par les polynômes $f_1 = xy+1$ et $f_2 = y^2 - 1$. On a vu dans l'exemple IV.2.3 que l'inclusion

$$\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle \subset \langle \mathrm{lt}(I) \rangle,$$

est stricte, par suite $\{f_1, f_2\}$ n'est pas une base de Gröbner de I.

IV.3.4. Exemple.— On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x,y]$ avec l'ordre alphabétique $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x,y]$ engendré par les polynômes $f_1 = xy+1$ et $f_2 = y+1$. Montrons que $\{f_1, f_2\}$ n'est pas une base de Gröbner de I. Le polynôme $f = xy^2 - 1$ a deux décompositions

$$\begin{aligned} f &= 0(xy+1) + (xy-x)(y+1) + (x-1) \\ f &= (y)(xy+1) + (-1)(y+1) + 0. \end{aligned}$$

D'après la deuxième équation, $f \in I$, d'où d'après la première équation $x-1 \in I$ et $x = \mathrm{lt}(x-1) \in \mathrm{lt}(I)$. Or $x \notin \langle xy, y \rangle$, car ni xy, ni y ne divisent x. On en déduit que l'inclusion

$$\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle \subset \langle \mathrm{lt}(I) \rangle,$$

est stricte, $\{f_1, f_2\}$ n'est donc pas une base de Gröbner de I.

IV.3.5. Exemple.— Considérons les polynômes $g_1 = z+x$ et $g_2 = y-x$ de $\mathbb{Q}[x,y,z]$. On utilise l'ordre lexicographique sur $\mathbb{Q}[x,y,z]$ avec $x < y < z$. Montrons que $G = \{g_1, g_2\}$ est une base de Gröbner de l'idéal $I = \langle g_1, g_2 \rangle$. Supposons le contraire, c'est-à-dire qu'il existe $f \in I$, tel que

$$\mathrm{lt}(f) \notin \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2) \rangle = \langle z, y \rangle.$$

Alors z ne divise pas $\mathrm{lt}(f)$ et y ne divise pas $\mathrm{lt}(f)$. En raison de l'ordre lexicographique, z et y n'apparaissent pas non plus dans les autres termes de f. Par suite, f est un polynôme en la seule indéterminée x. Par ailleurs, on a

$$f = h_1(z+x) + h_2(y-x),$$

avec $h_1, h_2 \in \mathbb{Q}[x,y,z]$. On a alors pour tous $a, c \in \mathbb{Q}$,

$$f(a,a,c) = h_1(a,a,c)(a+c).$$

Comme $\mathbb{Q}$ est infini et y n'apparaît pas dans les termes de f, on en déduit que $f = h_1(x,x,z)(x+z)$. Par suite $z+x$ divise f, qui est contradictoire avec le fait que f est d'une seule indéterminée x. Ainsi, G est une base de Gröbner de I.

IV.3.6. Exemple.— Considérons les polynômes $g_1 = x - y^2 w$, $g_2 = y - zw$, $g_3 = z - w^3$ et $g_4 = w^3 - w$ de $\mathbb{Q}[x,y,z,w]$. On considère l'ordre lexicographique avec l'ordre alphabétique

$w < z < y < x$. Montrons que $G = \{g_1, g_2, g_3, g_4\}$ est une base de Gröbner de l'idéal $I = \langle g_1, g_2, g_3, g_4\rangle$. On procède comme dans l'exemple précédent. Supposons le contraire, soit qu'il existe un polynôme $f \in I$ tel que

$$\mathrm{lt}(f) \notin \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2), \mathrm{lt}(g_3), \mathrm{lt}(g_4)\rangle = \left\langle x, y, z, w^3\right\rangle.$$

Par suite, f est un polynôme d'une seule indéterminée w tel que $\mathrm{lt}(f)$ n'est pas divisible par w^3. Comme $f \in I$, on a une décomposition

$$f = h_1(x - y^2w) + h_2(y - zw) + h_3(z - w^3) + h_4(w^3 - w).$$

Alors pour tout $a \in \mathbb{Q}$, on a

$$f(a^9, a^4, a^3, a) = h_4(a^9, a^4, a^3, a)(a^3 - a).$$

Comme x, y et z n'apparaissent pas dans f et comme $\mathbb{Q}$ est infini, on obtient $f = h_4(w^9, w^4, w^3, w)(w^3 - w)$. Par suite, $w^3 - w$ divise f, ce qui est contradictoire avec le fait que w^3 ne divise par $\mathrm{lt}(f)$. Ainsi G est une base de Gröbner de I.

IV.8 Proposition. — Un ordre monomial étant fixé, tout idéal non nul de $\mathbb{K}[x_1, \ldots, x_n]$ possède une base de Gröbner. De plus, tout base de Gröbner d'un idéal forme une base de cet idéal.

Preuve. Soit I un idéal non nul de $\mathbb{K}[x_1, \ldots, x_n]$. Soit $G = \{g_1, \ldots, g_t\}$ un ensemble de polynômes comme construit dans la preuve du théorème de la base de Hilbert, théorème IV.5. Par construction, c'est une base de Gröbner.

Pour la seconde assertion, si $g_1, \ldots, g_s$ sont des polynômes de I vérifiant $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\rangle$, toujours d'après la preuve du théorème IV.5, $I = \langle g_1, \ldots, g_t\rangle$. C'est donc une base de I. □

Exercice 87. — On utilise l'ordre lexicographique gradué avec l'ordre alphabétique $z < y < x$. Soit $I = \langle f_1, f_2, f_3\rangle$ l'idéal de $\mathbb{R}[x, y, z]$ engendré par les polynômes

$$f_1 = x^4y^2 - z^5, \quad f_2 = x^3y^3 - 1, \quad f_3 = x^2y^4 - 2z.$$

L'ensemble $\{f_1, f_2, f_3\}$ forme-t-il une base de Gröbner pour I ?

Exercice 88. — On utilise l'ordre lexicographique avec l'ordre alphabétique $z < y < x$. Soit $I = \langle f_1, f_2\rangle$ l'idéal de $\mathbb{R}[x, y, z]$ engendré par les polynômes

$$f_1 = x - z^2, \quad f_2 = y - z^3.$$

L'ensemble $\{f_1, f_2\}$ forme-t-il une base de Gröbner pour I ?

§ 4 Premières propriétés des bases de Gröbner

IV.9 Proposition. — Soit I un idéal de $\mathbb{K}[x_1,\ldots,x_n]$ et soit $G=\{g_1,\ldots,g_t\}$ une base de Gröbner de I. Soit f un polynôme de $\mathbb{K}[x_1,\ldots,x_n]$. Il existe un unique $r\in\mathbb{K}[x_1,\ldots,x_n]$ qui satisfait aux deux assertions suivantes :

i) aucun des termes de r n'est divisible par l'un des $\mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)$,

ii) il existe $g\in I$, tel que $f=g+r$.

En particulier, r est *le reste de la division* de f par G, peu importe l'ordre utilisé sur les éléments de G pendant la division. De plus, le polynôme r est l'unique réduction sous forme normale du polynôme f modulo G, on l'appelle également *la forme normale* de f modulo G.

Preuve. Le théorème III.11, qui s'obtient par division de f par $g_1,...,g_t$, montre l'existence d'un tel polynôme r sous forme normale par rapport à G.

Montrons l'unicité de r. Supposons qu'il existe r et r' satisfaisant les deux assertions :

$$f=g+r=g'+r'.$$

Alors

$$r-r'=g'-g\in I.$$

Ainsi, si $r\neq r'$, on a

$$\mathrm{lt}\left(r-r'\right)\in\langle\mathrm{lt}(I)\rangle=\langle\mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)\rangle.$$

Par suite, $\mathrm{lt}(r-r')$ est divisible par un $\mathrm{lt}(g_i)$. Or, ceci est impossible puisque aucun terme de r, ni de r', n'est divisible par $\mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)$. Par suite, $r-r'$ doit être nul, ce qui montre l'unicité.

Les deux dernières assertions de la proposition sont une conséquence de l'unicité de r. □

Attention, même si le reste est unique, les quotients $u_1,\ldots,u_t$ peuvent être différents d'une décomposition à l'autre.

Il suit de la proposition précédente que la donnée d'une base de Gröbner permet de répondre au problème de l'appartenance à un idéal.

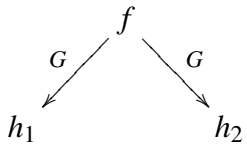
IV.10 Proposition. — Soient un idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ et une base $G=\{g_1,\ldots,g_t\}$ de I. Si G est une base de Gröbner de I, alors pour tout polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$ on a

$$f\in I,\quad \text{si, et seulement si,}\quad f\xrightarrow{g_1,\ldots,g_t}0\quad \text{si, et seulement si,}\quad f\xrightarrow{G}0.$$

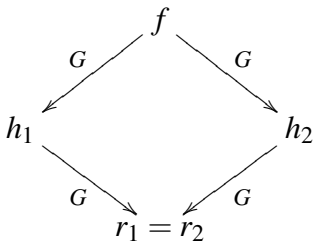
On verra dans le chapitre suivant que c'est en fait une caractérisation des bases de Gröbner. On verra également que G est une base de Gröbner, si, et seulement si, la relation de réduction modulo G est confluente. On peut déjà vérifier l'implication pour cette dernière assertion.

IV.4.1. Remarque.— Si $G = \{g_1, \ldots, g_t\}$ est une base de Gröbner de l'idéal $\langle g_1, \ldots, g_t \rangle$, alors la relation $\xrightarrow{G}$ est confluente.

Considérons une paire de réductions sur un même polynôme f modulo G



Soit r_1 et r_2 les formes normales de h_1 et h_2, respectivement, modulo G. Mais alors $f \xrightarrow{G} r_1$ et $f \xrightarrow{G} r_2$, donc $r_1 = r_2$ est également la forme normale de f modulo G.



Exercice 89. — Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et G une base de Gröbner de I. On note $\widehat{f}^G$, le reste de la division de f par G (ou forme normale de f modulo G).

1. Montrer que $\widehat{f}^G = \widehat{g}^G$ si, et seulement si, $f - g \in I$.

2. Montrer que

$$\widehat{f+g}^G = \widehat{f}^G + \widehat{g}^G.$$

3. Montrer que

$$\widehat{fg}^G = \widehat{\widehat{f}^G \widehat{g}^G}^G.$$

Exercice 90. — Soient G et G' deux bases de Gröbner d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$, relativement à un même ordre monomial. Montrer que pour tout polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$, si $f \xrightarrow{G} r$ et $f \xrightarrow{G'} r'$, où r et r' sont en forme normale respectivement pour G et G', alors $r = r'$.

CHAPITRE
V

L'algorithme de Buchberger

Sommaire

On fixe pour tout ce chapitre un ordre monomial sur $\mathscr{M}[x_1,\ldots,x_n]$. On a vu dans le chapitre précédent que tout idéal de $\mathbb{K}[x_1,\ldots,x_n]$ possède une base finie avec de bonnes propriétés (base de Gröbner). L'objectif de ce chapitre est de donner un algorithme permettant de calculer une base de Gröbner d'un idéal à partir d'une famille génératrice finie de cet idéal.

§ 1 Introduction

Soit $I=\langle f_1,\ldots,f_s\rangle$ un idéal de $\mathbb{K}[x_1,\ldots,x_n]$, on suppose que les polynômes f_i sont non nuls. Rappelons que par définition, l'ensemble $G=\{f_1,\ldots,f_s\}$ forme une base de Gröbner si

$$\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(f_1),\ldots,\mathrm{lt}(f_s)\rangle .$$

Tout polynôme f de I se décompose sous la forme

$$f = h_1 f_1 + \ldots + h_s f_s,$$

où les h_i sont des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$. Une obstruction à être une base de Gröbner apparaît lorsque le terme dominant dans une telle décomposition n'est pas dans l'idéal engendré par les $\mathrm{lt}(f_i)$, comme l'illustre l'exemple suivant.

V.1.1. Exemple.— Considérons l'idéal $I=\langle f_1,f_2\rangle$ de $\mathbb{R}[x,y]$ avec $f_1=x^3-2xy$ et $f_2=x^2y-2y^2+x$. Pour l'ordre lexicographique gradué, l'ensemble $F=\{f_1,f_2\}$ n'est pas une base de Gröbner. En effet, les termes dominants $\mathrm{lt}(f_1)=x^3$ et $\mathrm{lt}(f_2)=x^2y$ s'annulent dans l'expression

suivante :

$$yf_1 - xf_2 = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2 \in I.$$

Le terme dominant $\mathrm{lt}(yf_1 - xf_2) = -x^2$ n'est pas divisible par $\mathrm{lt}(f_1)$ ou $\mathrm{lt}(f_2)$, par suite, $\mathrm{lt}\left(-x^2\right)$ n'est pas dans l'idéal $\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle$.

Pour former une base de Gröbner de I à partir de l'ensemble générateur $\{f_1, f_2\}$, il faudrait corriger cette obstruction en ajoutant le polynôme $f_3 = -x^2$ à l'ensemble générateur. À ce stade, rien ne nous assure que $\{f_1, f_2, f_3\}$ constitue une base de Gröbner. Le polynôme f_3 est-il source de nouvelles obstructions ?

Dans ce chapitre, nous introduisons la notion de *S-polynôme* et de *paire critique associée* permettant de décrire et calculer ces obstructions. On présentera ensuite, l'algorithme de Buchberger qui calcule une base de Gröbner, par une méthode de complétion de l'ensemble générateur par de nouveaux générateurs permettant de résoudre toutes les obstructions.

V.1.2. Paires critiques.— On peut comprendre aussi l'obstruction qu'il y a pour $\{f_1, f_2\}$ de former une base de Gröbner de I, en utilisant la notion de « *paire critique* ». Cette notion permet de mettre en évidence les obstructions en utilisant la relation de *réduction*.

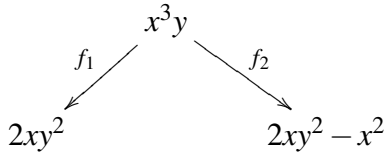
On a naturellement une réduction modulo $f_1 = x^3 - 2xy$ de son terme dominant x^3 :

$$x^3 \xrightarrow{f_1} 2xy.$$

De même pour f_2 :

$$x^2y \xrightarrow{f_2} 2y^2 - x.$$

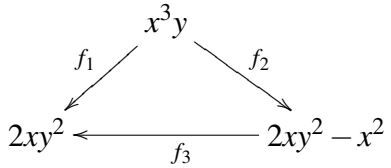
On appellera *paire critique*, l'interaction de deux telles réductions sur le *ppcm* de x^3 et x^2y :



Ajouter le polynôme $f_3 = x^2$, consiste à ajouter la réduction

$$x^2 \xrightarrow{f_3} 0$$

et à rendre confluente cette paire critique :



V.1.3. Exemple.— Soient $f_1 = xy - y$ et $f_2 = x - y^2$ des polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique donné par $y < x$. Soit I l'idéal engendré par $F = \{f_1, f_2\}$. On a $\mathrm{lt}(f_1) = xy$ et $\mathrm{lt}(f_2) = -x$, dans l'expression suivante, ces deux termes dominants s'annulent :

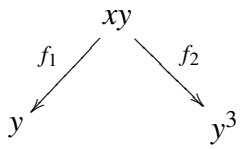
$$f_1 - yf_2 = (xy - y) - y(x - y^2) = -y + y^3.$$

Comme combinaison des polynômes f_1 et f_2, le polynôme $f_3 = -y + y^3$ est dans I. On a cependant $\mathrm{lt}(f_3) = y^3$ non divisible par $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$, donc F n'est pas une base de Gröbner de I. Le polynôme f_3 forme ainsi une obstruction à ce que l'ensemble F soit une base de Gröbner pour I. On peut corriger cela en ajoutant le polynôme f_3 à l'ensemble générateur F. On cherche alors les obstructions à ce que l'ensemble $F' = \{f_1, f_2, f_3\}$ soit une base de Gröbner pour I.

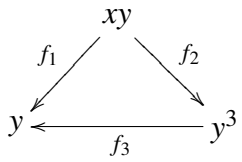
Interprétons ces obstructions en terme de paires critiques. On considère les deux réductions

$$xy \xrightarrow{f_1} y, \qquad x \xrightarrow{f_2} y^2.$$

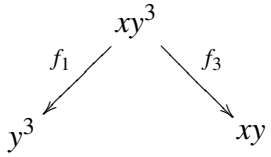
Il apparaît une paire critique



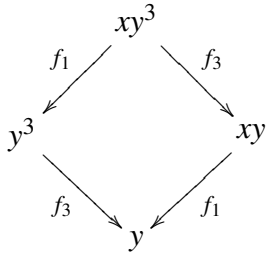
Cette paire critique est confluente lorsque l'on ajoute $f_3 = y^3 - y$:



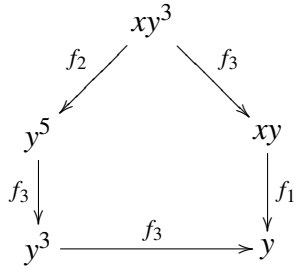
Avec la réduction $y^3 \xrightarrow{f_3} y$, il apparaît une nouvelle paire critique entre les réductions provenant de f_1 et f_3 :



Cette paire critique s'avère être déjà confluente



De même la paire critique associée à f_2 et f_3 est confluente :



Toutes les paires critiques sont alors confluentes. Nous allons voir que cela suffit à montrer que $\{f_1, f_2, f_3\}$ forme une base de Gröbner de I.

§ 2 Les S-polynômes, les paires critiques et le critère de Buchberger

V.2.1. Plus petit commun multiple.— Soient f et g deux polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Le *plus petit commun multiple* (ppcm) des polynômes f et g, noté $\mathrm{ppcm}(f,g)$, est l'unique polynôme m de $\mathbb{K}[x_1,\dots,x_n]$ vérifiant les trois assertions suivantes

i) f divise m et g divise m,

ii) si f et g divisent un polynôme h de $\mathbb{K}[x_1,\dots,x_n]$, alors m divise h,

iii) $\mathrm{lc}(m)=1$.

L'existence du ppcm sera admise. Dans le cas particulier de monômes, cette existence est immédiate.

V.2.2. Les S-polynômes.— Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Notons $\alpha=\mathrm{multideg}(f)$ et $\beta=\mathrm{multideg}(g)$. Le ppcm de $\mathrm{lm}(f)$ et $\mathrm{lm}(g)$ est le monôme

$$x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g)),$$

où $\gamma=(\gamma_1,\dots,\gamma_n)$, avec $\gamma_i=\max(\alpha_i,\beta_i)$, pour tout $i\in[\![1,n]\!]$.

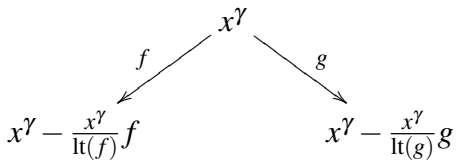
On appelle *S-polynôme* de f et g le polynôme

$$S(f,g)=\frac{x^\gamma}{\mathrm{lt}(f)}f-\frac{x^\gamma}{\mathrm{lt}(g)}g.$$

V.2.3. Remarque.— Étant donnés deux polynômes non nuls f et g de $\mathbb{K}[x_1,\dots,x_n]$, et $x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))$, alors

$$\mathrm{multideg}(S(f,g))<\gamma.$$

V.2.4. Les paires critiques.— En terme de réductions, la notion de S-polynôme s'interprète comme un couple de réductions qui « *chevauchent* » sur un même monôme. On appelle *paire critique* associée à deux polynômes non nuls f et g (ou paire critique associée au S-polynôme $S(f,g)$), le couple de réductions modulo f et g de $x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))$:



V.2.5. Exemple.— Considérons les polynômes

$$f=x^3y^2-x^2y^3+x,\qquad g=3x^4y+y^2$$

de $\mathbb{R}[x,y]$ avec l'ordre lexicographique gradué et $y<x$. Alors $\mathrm{lm}(f)=x^3y^2$ et $\mathrm{lm}(g)=x^4y$ et

$$\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))=x^4y^2.$$

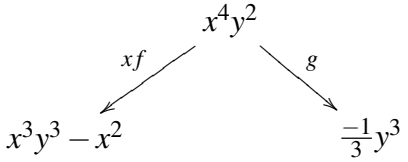
D'où

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2}f - \frac{x^4y^2}{3x^4y}g, \\ &= xf - \frac{1}{3}yg, \\ &= x^4y^2 - x^3y^3 + x^2 - x^4y^2 - \frac{1}{3}y^3, \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

En terme de paires critiques, avec les réductions

$$x^3y^2 \xrightarrow{f} x^2y^3 - x, \qquad 3x^4y \xrightarrow{g} -y^2$$

on a la paire critique



Cet exemple illustre que les S-polynômes annulent les termes dominants dans les combinaisons de générateurs.

Exercice 91. — En considérant l'ordre lexicographique, Calculer le S-polynôme $S(f,g)$ dans les cas suivants

1. $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$,
2. $f = x^4y - z^2$, $g = 3xz^2 - y$,
3. $f = x^7y^2z + 2xyz$, $g = 2x^7y^2z + 4$,
4. $f = xy + z^3$, $g = z^2 - 3z$.

Exercice 92. — Étant donnés deux polynômes f et g de $\mathbb{K}[x_1,\ldots,x_n]$, le S-polynôme $S(f,g)$ dépend-t-il de l'ordre monomial ? Illustrer à l'aide d'un exemple.

Exercice 93. — Montrer la remarque V.2.3

Exercice 94. — Soient f et g deux polynômes de $\mathbb{K}[x_1,\ldots,x_n]$.

1. Vérifier que

$$S(f,g) = S\left(\frac{f}{\mathrm{lc}(f)}, \frac{g}{\mathrm{lc}(g)}\right).$$

2. Montrer que si $\mathrm{lt}(f)$ divise $\mathrm{lt}(g)$, alors

$$\langle f,g\rangle = \langle f, S(f,g)\rangle.$$

Le résultat suivant montre que toute élimination de termes dominants entre des polynômes qui ont le même multidegré peut s'exprimer en terme de S-polynômes.

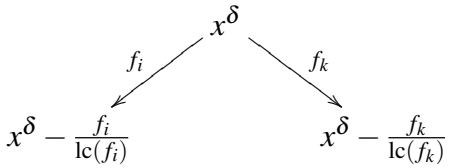
V.1 Proposition. — Soit une combinaison linéaire

$$f = c_1 f_1 + \ldots + c_s f_s, \quad c_i \in \mathbb{K},$$

telle que, pour tout $i \in [\![1,s]\!]$, $\text{multideg}(f_i) = \delta \in \mathbb{N}^n$. Si $\text{multideg}(f) < \delta$, alors

i) f est une combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(f_i, f_k)$, pour $i,k \in [\![1,s]\!]$;

ii) de plus, pour tous $i,k \in [\![1,s]\!]$, la paire critique associée à $S(f_i,f_k)$ est de la forme



et, en particulier, $\text{multideg}\big(S(f_i,f_k)\big) < \delta$.

Preuve. Pour tout $i \in [\![1,s]\!]$, on a $\text{lc}(c_i f_i) = c_i \text{lc}(f_i)$ et $\text{multideg}(c_i f_i) = \text{multideg}(f_i) = \delta$. Or, par hypothèse $\text{multideg}(c_1 f_1 + \ldots + c_s f_s) < \delta$, donc nécessairement

$$c_1 \text{lc}(f_1) + \ldots + c_s \text{lc}(f_s) = 0. \tag{V.1}$$

On a

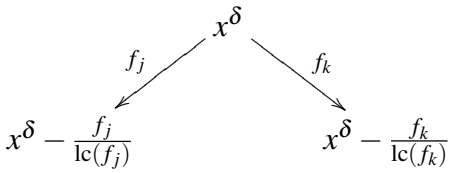
$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i \text{lc}(f_i) \frac{f_i}{\text{lc}(f_i)} \\ &= c_1 \text{lc}(f_1)\left(\frac{f_1}{\text{lc}(f_1)} - \frac{f_2}{\text{lc}(f_2)}\right) + (c_1 \text{lc}(f_1) + c_2 \text{lc}(f_2))\left(\frac{f_2}{\text{lc}(f_2)} - \frac{f_3}{\text{lc}(f_3)}\right) \\ &\quad + \ldots + (c_1 \text{lc}(f_1) + \ldots + c_{s-1}\text{lc}(f_{s-1}))\left(\frac{f_{s-1}}{\text{lc}(f_{s-1})} - \frac{f_s}{\text{lc}(f_s)}\right) \\ &\quad + (c_1 \text{lc}(f_1) + \ldots + c_s \text{lc}(f_s)) \frac{f_s}{\text{lc}(f_s)}.\end{aligned}$$

Avec l'équation (V.1), on obtient

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i = c_1 \text{lc}(f_1)\left(\frac{f_1}{\text{lc}(f_1)} - \frac{f_2}{\text{lc}(f_2)}\right) + (c_1 \text{lc}(f_1) + c_2 \text{lc}(f_2))\left(\frac{f_2}{\text{lc}(f_2)} - \frac{f_3}{\text{lc}(f_3)}\right) \\ + \ldots + (c_1 \text{lc}(f_1) + \ldots + c_{s-1}\text{lc}(f_{s-1}))\left(\frac{f_{s-1}}{\text{lc}(f_{s-1})} - \frac{f_s}{\text{lc}(f_s)}\right).\end{aligned} \tag{V.2}$$

Par ailleurs, pour tout $i \in [\![1,s]\!]$, $\text{lt}(f_i) = \text{lc}(f_i) x^\delta$. Il suit que, pour tous $j,k \in [\![1,s]\!]$,

$$\text{ppcm}(\text{lm}(f_j), \text{lm}(f_k)) = x^\delta,$$



et

$$S(f_j, f_k) = \frac{f_j}{\mathrm{lc}(f_j)} - \frac{f_k}{\mathrm{lc}(f_k)}.$$

L'équation (V.2) s'écrit alors

$$\sum_{i=1}^{s} c_i f_i = c_1 \mathrm{lc}(f_1) S(f_1, f_2) + (c_1 \mathrm{lc}(f_1) + c_2 \mathrm{lc}(f_2)) S(f_2, f_3) \qquad \text{(V.3)}$$
$$+ \ldots + (c_1 \mathrm{lc}(f_1) + \ldots + c_{s-1} \mathrm{lc}(f_{s-1})) S(f_{s-1}, f_s).$$

□

V.2 Proposition. — Soient f et g deux polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$ et $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes non nuls contenant f et g. Soit $\alpha, \beta \in \mathbb{N}^n$.

i) Si $S(f,g) \xrightarrow{F} 0$, alors $S(x^\alpha f, x^\beta g) \xrightarrow{F} 0$.

ii) Si la paire critique associée à $S(f,g)$ est confluente modulo F, alors celle associée à $S(x^\alpha f, x^\beta g)$ l'est aussi.

iii) Si la paire critique associée à $S(f,g)$ est confluente modulo F, alors on a la décomposition

$$S(f,g) = u_1 f_1 + \ldots + u_s f_s$$

avec pour tout quotient $u_i \neq 0$,

$$\mathrm{multideg}(u_i f_i) < \gamma$$

où $x^\gamma = \mathrm{ppcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.

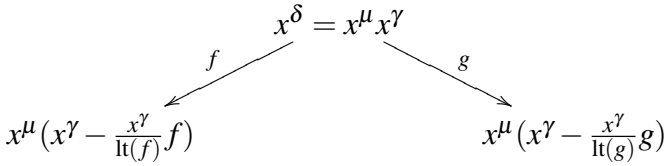
Preuve. Notons que

$$x^\gamma = \mathrm{ppcm}(\mathrm{lm}(f), \mathrm{lm}(g))$$

divise

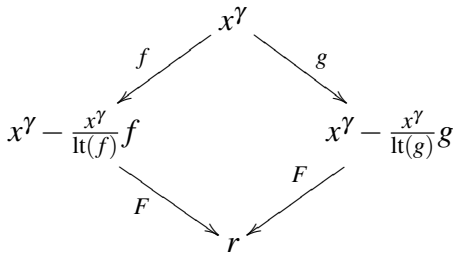
$$x^\delta = \mathrm{ppcm}(x^\alpha \mathrm{lm}(f), x^\beta \mathrm{lm}(g)) = \mathrm{ppcm}(\mathrm{lm}(x^\alpha f), \mathrm{lm}(x^\beta g)).$$

Soit $\mu \in \mathbb{N}^n$ tel que $x^\delta = x^\mu x^\gamma$. Alors, on vérifie facilement que $S(x^\alpha f, x^\beta g) = x^\mu S(f,g)$ et que la paire critique associée à $S(x^\alpha f, x^\beta g)$ correspond à la multiplication par x^μ de celle associée à $S(f,g)$:



On en déduit **i)** et **ii)**.

Pour **iii)**, supposons que



Alors, il existe $u'_1, \ldots, u'_s$ et $u''_1, \ldots, u''_s$ tels que

- $x^\gamma - \frac{x^\gamma}{\mathrm{lt}(f)} f = u'_1 f_1 + \ldots + u'_s f_s + r$,
- $x^\gamma - \frac{x^\gamma}{\mathrm{lt}(g)} g = u''_1 f_1 + \ldots + u''_s f_s + r$,
- pour tout $u'_i \neq 0$, $\mathrm{multideg}(u'_i f_i) \leq \mathrm{multideg}\left(x^\gamma - \frac{x^\gamma}{\mathrm{lt}(f)} f\right) < \gamma$,
- pour tout $u''_i \neq 0$, $\mathrm{multideg}(u''_i f_i) \leq \mathrm{multideg}\left(x^\gamma - \frac{x^\gamma}{\mathrm{lt}(g)} g\right) < \gamma$.

D'où,

$$S(f,g) = (x^\gamma - \frac{x^\gamma}{\mathrm{lt}\,(g)} g) - (x^\gamma - \frac{x^\gamma}{\mathrm{lt}\,(f)} f) = (u''_1 - u'_1) f_1 + \ldots + (u''_s - u'_s) f_s$$

avec pour tout $(u''_i - u'_i) \neq 0$,

$$\mathrm{multideg}((u''_i - u'_i) f_i) < \gamma.$$

□

V.3 Théorème (Critère de Buchberger). — Soit $G = \{g_1, \ldots, g_t\}$ une base d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$. Les assertions suivantes sont équivalentes :

i) G est une base de Gröbner de I ;

ii) pour tout couple (i, j), avec $i \neq j$,

$$S(g_i, g_j) \xrightarrow{G} 0;$$

iii) pour tout couple (i, j), avec $i \neq j$, la paire critique associée à $S(g_i, g_j)$ est confluente.

Preuve. Si G est une base de Gröbner de I, comme tout S-polynôme $S(g_i, g_j)$ est dans I, d'après la proposition IV.10, on a $S(g_i, g_j) \xrightarrow{G} 0$. De plus, la relation de réduction $\xrightarrow{G}$ est confluente par la remarque IV.4.1, et donc en particulier les paires critiques le sont.

Supposons réciproquement que l'assertion **ii)** ou l'assertion **iii)** est vérifiée. Soit $G = \{g_1, \ldots, g_t\}$ une base de I. Pour montrer que G est une base de Gröbner de I, il suffit de vérifier que

$$\langle \mathrm{lt}\,(I) \rangle = \langle \mathrm{lt}\,(g_1), \ldots, \mathrm{lt}\,(g_s) \rangle .$$

Considérons donc un polynôme non nul $f \in I$ et montrons que $\mathrm{lt}\,(f) \in \langle \mathrm{lt}\,(g_1), \ldots, \mathrm{lt}\,(g_s) \rangle$. Il existe une décomposition

$$f = h_1 g_1 + \ldots + h_t g_t, \tag{V.4}$$

où les h_i sont des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$. Posons

$$\delta = \max\{\text{multideg}(h_1 g_1),\ \ldots\ ,\text{multideg}(h_t g_t)\}. \tag{V.5}$$

D'après la proposition III.10, on a $\text{multideg}(f) \leq \delta$.

Il existe a priori plusieurs décompositions de f sous la forme (V.4). Pour chaque décomposition, on a un $\delta \in \mathbb{N}^n$, comme défini en (V.5). On considère une décomposition de f telle que δ soit minimal ; il est possible de faire un tel choix du fait qu'un ordre monomial est un bon ordre.

Si $\text{multideg}(f) = \delta$, c'est-à-dire, il existe un $i \in [\![1,s]\!]$, tel que $\text{multideg}(f) = \text{multideg}(h_i g_i)$, alors $\text{lt}(f)$ est divisible par $\text{lt}(g_i)$. Par suite,

$$\text{lt}(f) \in \langle \text{lt}(g_1), \ldots, \text{lt}(g_s) \rangle .$$

Reste à montrer que $\text{multideg}(f) = \delta$. Pour cela, procédons par l'absurde et supposons que $\text{multideg}(f) < \delta$. En posant $m(i) = \text{multideg}(h_i g_i)$, on a une décomposition

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i.$$

Soit

$$f = \sum_{m(i)=\delta} \text{lt}(h_i)\, g_i + \sum_{m(i)=\delta} (h_i - \text{lt}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \tag{V.6}$$

Or, si $m(i) = \delta$, alors $\text{multideg}((h_i - \text{lt}(h_i))g_i) < \delta$ et si $m(i) < \delta$, alors $\text{multideg}(h_i g_i) < \delta$. Les deux dernières sommes dans (V.6) sont ainsi de multidegrés strictement inférieurs à δ. Comme par hypothèse $\text{multideg}(f) < \delta$, on a alors nécessairement

$$\text{multideg}\left(\sum_{m(i)=\delta} \text{lt}(h_i)\, g_i \right) < \delta.$$

En posant, $\text{lt}(h_i) = c_i x^{\alpha(i)}$, avec $c_i \in \mathbb{K}$, on a

$$\sum_{m(i)=\delta} \text{lt}(h_i)\, g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i.$$

Comme pour tout i tel que $m(i) = \delta$, on a $\text{multideg}(\text{lt}(h_i)\, g_i) = \delta$, la somme $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ satisfait aux hypothèses de la proposition V.1, cette somme se décompose alors en une combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(x^{\alpha(i)} g_i, x^{\alpha(k)} g_k)$:

$$\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k), \tag{V.7}$$

où $c_{jk} \in \mathbb{K}$.

Si $S(g_j, g_k) \xrightarrow{G} 0$ pour tous $j \neq k$, alors on a également $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) \xrightarrow{G} 0$ pour tous $j \neq k$, par la proposition V.2. Comme ces derniers S-polynômes sont de multidegrés strictement inférieurs à δ, ils s'écrivent sous la forme

$$S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) = \sum_{i=1}^{t} u_{ijk} g_i, \tag{V.8}$$

tels que $\text{multideg}(u_{ijk} g_i) < \delta$ pour tout $u_{ijk} \neq 0$. Si toutes les paires critiques associées aux $S(g_j, g_k)$ sont confluentes, alors, par la proposition V.2, il en est de même pour les paires cri-

tiques associées aux $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$ et ces derniers S-polynômes se décomposent comme en (V.8).

Dans les deux cas, on en déduit en utilisant les équations (V.6) et (V.7) que f admet une décomposition de la forme

$$f = \sum_{i=1}^{t} u_i g_i$$

avec $\text{multideg}(u_i g_i) < \delta$ pour tout $u_i \neq 0$. Ceci contredit l'hypothèse sur la minimalité de δ, par suite, $\text{multideg}(f) = \delta$, ce qui termine la preuve du théorème. □

On déduit de ce critère les caractérisations suivantes des bases de Gröbner.

V.4 Théorème. — Soit $G = \{g_1, \ldots, g_t\}$ une base d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$. Alors les assertions suivantes sont équivalentes :

i) G est une base de Gröbner de I ;

ii) pour tout polynôme $f \in I$,

$$f \in I, \text{ si, et seulement si, } f \xrightarrow{G} 0;$$

iii) la relation de réduction $\xrightarrow{G}$ est confluente.

Preuve. On a déjà vu que **i)** implique **ii)** et **iii)** (proposition IV.10 et remarque IV.4.1). Réciproquement, si on suppose **ii)**, alors tous les S-polynômes se réduisent en 0 modulo G, et si on suppose **iii)**, alors toutes les paires critiques sont confluentes. Dans les deux cas, on conclut par le théorème V.3. □

V.2.6. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x,y,z]$ avec $f_1 = y - z^2$ et $f_2 = x - z^3$. Alors $G = \{f_1, f_2\}$ est une base de Gröbner pour l'ordre lexicographique avec $z < y < x$. En effet, on calcule de S-polynôme

$$\begin{aligned} S(f_1, f_2) &= \frac{yx}{y}(y - z^2) - \frac{yx}{x}(x - z^3), \\ &= xy - xz^2 - xy + yz^3, \\ &= -xz^2 + yz^3, \end{aligned}$$

où $\text{ppcm}(\text{lm}(f_1), \text{lm}(f_2)) = \text{ppcm}(y,x) = yx$. Par ailleurs, la division de $S(f_1, f_2)$ par G donne

$$S(f_1, f_2) = z^3(y - z^2) - z^2(x - z^3) + 0.$$

Par suite $S(f_1, f_2) \xrightarrow{G} 0$ et donc G est une base de Gröbner d'après le théorème V.3.

Exercice 95. — Montrer que l'ensemble G de l'exemple V.2.6 ne forme pas une base de Gröbner pour l'ordre lexicographique avec l'ordre alphabétique $x < y < z$.

Exercice 96. — Montrer que $\{y - x^2, z - x^3\}$ n'est pas une base de Gröbner pour l'ordre lexicographique induit par $z < y < x$.

Exercice 97. — L'ensemble $\{x^2-y, x^3-z\}$ est-il une base de Gröbner pour un ordre lexicographique ?

FIGURE V.1.: Bruno Buchberger (1942-)

Bruno Buchberger est un mathématicien autrichien né en 1942. Il introduit la théorie des bases de Gröbner dans sa thèse soutenue en 1965. Il nomme ces bases ainsi en l'honneur de son directeur de thèse Wolfgang Gröbner. Il donne un algorithme, appelé algorithme de Buchberger, qui calcule les bases de Gröbner.

§ 3 L'algorithme de Buchberger

D'après la proposition IV.8, tout idéal non nul de $\mathbb{K}[x_1,\ldots,x_n]$ admet une base de Gröbner. La preuve donnée n'est pas constructive ; elle n'indique pas le moyen de construire une base de Gröbner. L'algorithme de Buchberger construit une base de Gröbner d'un idéal à partir d'une base de cet idéal.

V.3.1. Exemple.— Considérons l'idéal $I = \langle f_1, f_2\rangle$ de $\mathbb{R}[x,y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$. Nous avons vu en V.1.1, que pour l'ordre lexicographique gradué, l'ensemble $F = \{f_1, f_2\}$ n'est pas une base de Gröbner. On peut le montrer en utilisant le critère de Buchberger, on calcule le S-polynôme

$$\begin{aligned} S(f_1,f_2) &= \frac{x^3y}{x^3}(x^3-2xy) - \frac{x^3y}{x^2y}(x^2y-2y^2+x), \\ &= -x^2. \end{aligned}$$

Comme $-x^2$ n'est pas divisible par $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$, la forme normale de $S(f_1,f_2)$ est x^2 :

$$S(f_1,f_2) \xrightarrow{F} -x^2$$

et d'après le critère de Buchberger, F n'est pas une base de Gröbner de I.

V.3.2. L'algorithme de Buchberger.— L'idée de Buchberger est de compléter la base F de I en résolvant toute les obstructions, pour obtenir une base de Gröbner. Les relations rajoutées

doivent rester redondantes, cela revient à compléter avec des polynômes de I. Dans l'exemple V.3.1, l'obstruction à ce que $\{f_1, f_2\}$ soit une base de Gröbner est que le reste de la division

$$S(f_1, f_2) \xrightarrow{f_1, f_2} -x^2$$

est non nul. Comme $S(f_1, f_2) = -x^2 \in I$, on peut inclure ce reste comme générateur et considérer l'ensemble générateur $F' = \{f_1, f_2, f_3\}$ avec $f_3 = -x^2$. On a alors

$$S(f_1, f_2) \xrightarrow{F'} 0.$$

Testons le critère de Buchberger avec les nouveaux S-polynômes $S(f_1, f_3)$ et $S(f_2, f_3)$. On a

$$S(f_1, f_3) = \frac{x^3}{x^3}(x^3 - 2xy) - \frac{x^3}{-x^2}(-x^2) = -2xy.$$

Donc

$$S(f_1, f_3) \xrightarrow{F'} -2xy.$$

On rajoute alors le polynôme $f_4 = -2xy$ comme générateur et on considère l'ensemble $f'' = \{f_1, f_2, f_3, f_4\}$. On a alors

$$S(f_1, f_2) \xrightarrow{F''} 0, \quad S(f_1, f_3) \xrightarrow{F''} 0.$$

On a

$$S(f_1, f_4) = \frac{x^3 y}{x^3}(x^3 - 2xy) - \frac{x^3 y}{-2xy}(-2xy) = -2xy^2 = y f_4.$$

Ainsi $S(f_1, f_4) \xrightarrow{F''} 0$. On

$$S(f_2, f_3) = \frac{x^2 y}{x^2 y}(x^2 y - 2y^2 + x) - \frac{x^2 y}{-x^2}(-x^2) = -2y^2 + x.$$

On rajoute alors le polynôme $f_5 = -2y^2 + x$. En posant $G = \{f_1, f_2, f_3, f_4, f_5\}$, on a

$$S(f_i, f_j) \xrightarrow{G} 0,$$

pour tout $i, j \in [\![1, 5]\!]$. D'après le critère de Buchberger, G est une base de Gröbner de I.

V.5 Théorème. — Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal non nul de $\mathbb{K}[x_1, \ldots, x_n]$, avec $f_i \neq 0$, pour $i \in [\![1, s]\!]$. L'algorithme de Buchberger construit une base de Gröbner de I en un nombre fini d'étapes.

Preuve. Montrons que l'algorithme termine. Par l'absurde, supposons que l'algorithme ne termine pas. Dans l'affectation $G := G \cup \{r\}$, l'ensemble G se construit progressivement par ajout de polynômes, on a ainsi une suite strictement croissante

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \ldots$$

avec $G_i := G_{i-1} \cup \{r\}$, où r est un polynôme de I, tel que $S(f, g) \xrightarrow{G_{i-1}} r$, où f et g sont deux

polynômes de G_{i-1}. Le polynôme r est en forme normale relativement à la division par rapport à G_{i-1}, d'où $\mathrm{lt}(r) \notin \mathrm{lt}(G_{i-1})$. Par suite

$$\mathrm{lt}(G_1) \subsetneq \mathrm{lt}(G_2) \subsetneq \mathrm{lt}(G_3) \subsetneq \dots$$

forme une suite strictement croissante d'idéaux, qui est en contradiction avec la propriété des suites croissantes d'idéaux de $\mathbb{K}[x_1,\dots,x_n]$, théorème IV.6 . Ainsi, l'algorithme termine.

Montrons que l'ensemble G obtenu est une base de Gröbner de I. On a $F \subseteq G \subset I$, donc G forme un ensemble de générateurs pour l'idéal I. Par ailleurs, par construction, pour tous $g_i, g_k \in G$, on a $S(g_i,g_k) \xrightarrow{G} 0$. D'après le critère de Buchberger, G forme une base de Gröbner de I. □

V.3.3. Algorithme de Buchberger.—

ENTRÉE : $F = \{f_1,\dots,f_s\}$ une base de I, avec $f_i \neq 0$, pour $i \in [\![1,s]\!]$.
SORTIE : une base de Gröbner G de I avec $F \subset G$.
INITIALISATION : $G := F$
$\mathscr{G} := \{\ \{f_i,f_j\} \mid f_i,f_j \in G \text{ et } f_i \neq f_j\}$
TANT QUE : $\mathscr{G} \neq \emptyset$ **FAIRE**
prendre $\{f,g\} \in \mathscr{G}$
$\mathscr{G} := \mathscr{G} - \{\{f,g\}\}$
$S(f,g) \xrightarrow{G} r$, où r est en forme normale
SI $r \neq 0$ **ALORS**
$\mathscr{G} := \mathscr{G} \cup \{\{f,r\} \mid \text{pour tout } f \in G\}$
$G := G \cup \{r\}$

V.3.4. Exemple.—

On exécute l'algorithme de Buchberger sur les polynômes $f_1 = xy - x$ et $f_2 = -y + x^2$ de $\mathbb{Q}[x,y]$, en considérant l'ordre lexicographique avec $x < y$.

INITIALISATION : $G := \{f_1,f_2\}$, $\mathscr{G} := \{\{f_1,f_2\}\}$
première passage de la boucle **TANT QUE :**
$\mathscr{G} := \emptyset$
$S(f_1,f_2) \xrightarrow{G} x^3 - x$
comme $r \neq 0$, on pose $f_3 := x - x$
$\mathscr{G} := \{\{f_1,f_3\},\{f_2,f_3\}\}$
$G := \{f_1,f_2,f_3\}$
second passage de la boucle **TANT QUE :**
$\mathscr{G} := \{\{f_2,f_3\}\}$
$S(f_1,f_3) \xrightarrow{G} 0$
troisième passage de la boucle **TANT QUE :**
$\mathscr{G} := \emptyset$
$S(f_2,f_3) \xrightarrow{G} 0$
Arrêt de la boucle **TANT QUE :** , car $\mathscr{G} = \emptyset$.

D'après le théorème V.5, l'ensemble $\{f_1, f_2, f_3\}$ forme une base de Gröbner de l'idéal $I = \langle f_1, f_2 \rangle$.

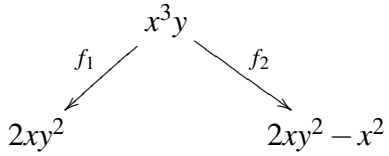
V.3.5. Complétion des paires critiques.— On peut également compléter progressivement les paires critiques associées aux S-polynômes et ainsi satisfaire le second critère. Reprenons la construction de la base de Gröbner dans l'exemple V.3.1. On souhaite construire une base de Gröbner pour l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x,y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$.

Étape 1. On fixe un ordre, par exemple l'ordre lexicographique gradué.

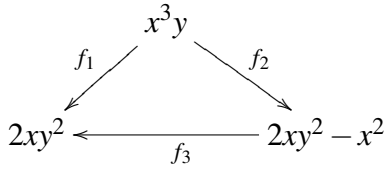
Étape 2. On oriente les relations par rapport à cet ordre

$$x^3 \xrightarrow{f_1} 2xy, \qquad x^2y \xrightarrow{f_2} 2y^2 - x.$$

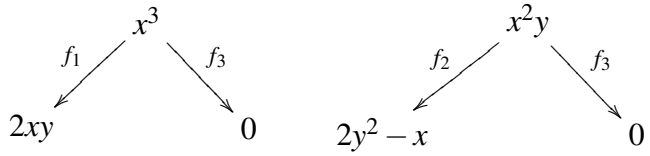
Étape 3. On calcule les paires critiques. Ici, il n'y a qu'une paire critique formée par f_1 et f_2 :



Étape 4. On rajoute la règle $x^2 \xrightarrow{f_3} 0$, pour obtenir un diagramme confluent :



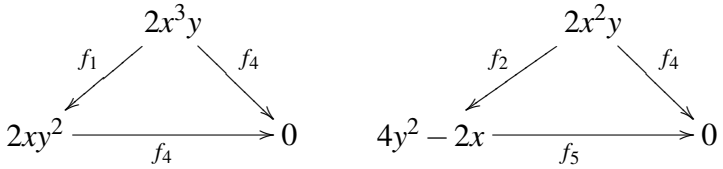
Étape 5. On examine les nouvelles paires critiques :

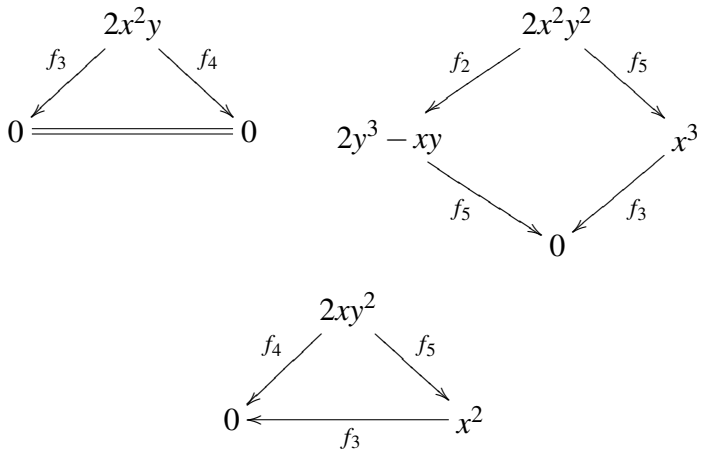


Étape 6. Pour compléter ces diagrammes, on rajoute les règles

$$2xy \xrightarrow{f_4} 0, \qquad 2y^2 \xrightarrow{f_5} x.$$

Étape 7. On examine les nouvelles paires critiques





Il n'y a plus d'autre paire critique, par suite $G = \{f_1, f_2, f_3, f_4, f_5\}$ est une base de Gröbner de I.

Exercice 98. — Pour les idéaux suivants, construire une base de Gröbner en utilisant l'ordre lexicographique, puis l'ordre lexicographique gradué.

1. $I = \langle x^2y - 1, xy^2 - x \rangle$,
2. $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3 \rangle$,
3. $I = \langle x - z^4, y - z^5 \rangle$.

V.3.6. Remarque.— En pratique, certaines paires critiques sont nécessairement confluentes et, dans certaines situations, quand l'on complète la base par un polynôme, on peut supprimer un polynôme précédent. Ceci permet de diminuer le nombre de calculs. Pour cela, on utilisera les propriétés suivantes :

V.6 Proposition. — Soit $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$ ($s \geq 2$).

i) Si $\text{ppcm}(\text{lm}(f_1), \text{lm}(f_2)) = \text{lm}(f_1)\text{lm}(f_2)$ (c.à.d. si $\text{lm}(f_1)$ et $\text{lm}(f_2)$ sont premiers entre eux), alors la paire critique associée à $S(f_1, f_2)$ est confluente modulo $\{f_1, f_2\}$ et

$$S(f_1, f_2) \overset{\{f_1, f_2\}}{\longrightarrow} 0.$$

ii) si $\text{lm}(f_2)$ divise $\text{lm}(f_1)$ et si h est un réduit sous forme normale de $S(f_1, f_2)$ ou une complétion de la paire critique associée modulo F, alors

$$\langle f_1, f_2, \ldots, f_s \rangle = \langle h, f_2, \ldots, f_s \rangle .$$

Exercice 99. — 1. Montrer la proposition V.6.
2. On munit $\mathbb{Q}[x, y, z]$ de l'ordre lexicographique induit par $x > y > z$. Soient $f_1 = xy - y + z$, $f_2 = x^2yz + y^2$ et l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y, z]$. En utilisant la proposition V.6, déterminer une base de Gröbner de I constituée de trois polynômes.

CHAPITRE
VI

Premières applications des bases de Gröbner

Sommaire

Les bases de Gröbner permettent de résoudre algorithmiquement de nombreux problèmes portant sur les idéaux d'anneaux de polynômes. Voici les principaux problèmes que l'on peut aborder en utilisant les bases de Gröbner et que nous allons présenter dans ce chapitre :

i) problème de l'appartenance à un idéal,

ii) problème de la résolution d'équations polynomiales,

iii) problème d'impliciter une présentation paramétrée.

§ 1 Description d'un idéal et appartenance à un idéal

VI.1.1. Problème de la description d'un idéal.—

- Est-ce que tout idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ possède un nombre fini de générateurs ? Autrement dit, existe-t-il une famille de polynômes $f_1,\ldots,f_s$ tels que $I=\langle f_1,\ldots,f_s\rangle$?
- Existe-t-il une famille génératrice « plus intéressante » que les autres ?

Une réponse à la première question est donnée par le théorème de la base de Hilbert, théorème IV.5. Dans ce chapitre, nous allons voir que pour certains problèmes des familles de générateurs sont plus intéressantes que d'autres.

VI.1.2. Problème de l'appartenance à un idéal.—

Étant donné un idéal $I = \langle f_1, \ldots, f_s \rangle$ et un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$, déterminer si $f \in I$.

L'algorithme de division appliquée avec une base de Gröbner permet de résoudre le problème de l'appartenance à un idéal ; on procède en deux étapes :

- la première étape consiste à calculer une base de Gröbner $G = \{g_1, \ldots, g_t\}$ de I avec l'algorithme de Buchberger, théorème V.5 (après avoir choisi un ordre monomial) ;
- la deuxième étape calcule la division de f par G. D'après la proposition IV.10, un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ est un élément de I, si, et seulement si, le reste de la division de f par G est égal à 0 :

$$f \in I, \quad \text{si, et seulement si,} \quad f \xrightarrow{G} 0.$$

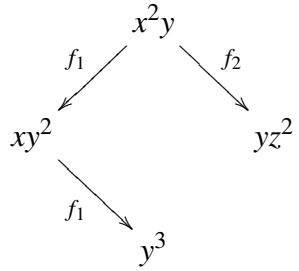
VI.1.3. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y, z]$, avec

$$f_1 = xy - y^2, \qquad f_2 = x^2 - z^2.$$

Soit $f = 2x^3y - xyz^2 - y^2z^2$, a-t-on $f \in I$? Considérons l'ordre lexicographique gradué, avec $z < y < x$, on a les réductions

$$xy \xrightarrow{f_1} y^2, \qquad x^2 \xrightarrow{f_2} z^2.$$

L'ensemble $\{f_1, f_2\}$ n'est pas une base de Gröbner de I, car la paire critique



n'est pas confluente. Pour obtenir une base de Gröbner, il suffit de compléter cette paire critique, car il n'apparaît pas d'autre paire critique non confluente. L'ensemble $G = \{f_1, f_2, f_3\}$, avec $f_3 = y^3 - yz^2$, est une base de Gröbner de I.

Pour tester l'appartenance de f à I, il suffit alors de diviser f par G, on a

$$f = 2xyf_1 + z^2 f_2.$$

Le reste de cette division est nul, ainsi $f \in I$. Cela revient à réduire le polynôme f par f_1 et f_2 et tester si la forme normale obtenue est nulle :

$$2x^3y - xyz^2 - y^2z^2 \xrightarrow{f_1} 2x^2y^2 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2xy^3 - xyz^2 - y^2z^2$$

$$\xrightarrow{f_1} 2y^4 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2y^4 - y^2z^2 - y^2z^2 \xrightarrow{f_3} 2y^2z^2 - 2y^2z^2 = 0.$$

L'ordre d'application des réductions n'a pas d'influence sur le résultat, car G étant une base de Gröbner, le système est confluent.

Ainsi, tout polynôme f tel que $\mathrm{lt}(f)$ n'est pas dans l'idéal $\langle \mathrm{lt}(G) \rangle = \langle xy, x^2, y^3 \rangle$ n'est pas dans I. Par exemple, le polynôme $f = zy - y^2$ n'est pas dans I, car il est en forme normale par réduction par G.

On peut utiliser Sage pour calculer la base de Gröbner G :

```
sage: A.<x,y,z> = PolynomialRing(RationalField(), 3, order='deglex')
sage: f1 = x*y-y^2
sage: f2 = x^2-z^2
sage: I = (f1, f2)*A
sage: G = I.groebner_basis()
sage: print G
        [y^3 - y*z^2, x^2 - z^2, x*y - y^2]
```

§ 2 Résolution d'équations polynomiales

VI.2.1. Problème de la résolution d'équations polynomiales.—

Étant donnés des polynômes $f_1,\dots,f_s$ de $\mathbb{K}[x_1,\dots,x_n]$, trouver les solutions dans $\mathbb{K}^n$ du système d'équations polynomiales

$$\left|\begin{array}{l} f_1(x_1,\dots,x_n)=0 \\ \qquad\vdots \\ f_s(x_1,\dots,x_n)=0 \end{array}\right.$$

D'après la proposition IV.7, pour tout idéal I de $\mathbb{K}[x_1,\dots,x_n]$,

$$\mathbf{V}(I)=\{(a_1,\dots,a_n)\in\mathbb{K}^n \mid f(a_1,\dots,a_n)=0 \text{ pour tout } f\in I\}.$$

est un ensemble algébrique affine. Si l'idéal I est défini par $I=\langle f_1,\dots,f_s\rangle$, alors $\mathbf{V}(I)=\mathbf{V}(f_1,\dots,f_s)$. On peut ainsi décrire $\mathbf{V}(I)$ à partir de toute base de I, en particulier avec une base de Gröbner calculée avec l'ordre lexicographique.

VI.2.2. Exemple.— On considère le système d'équations

$$\left|\begin{array}{rl} x^2+y^2+z^2 &= 1 \\ x^2+z^2 &= y \\ x &= z \end{array}\right.$$

dans $\mathbb{C}^3$. Ces équations déterminent l'idéal

$$I=\left\langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\right\rangle.$$

L'objectif est de décrire l'ensemble algébrique affine $\mathbf{V}(I)$. On calcule une base de Gröbner $G=\{g_1,g_2,g_3\}$ de l'idéal I en utilisant l'ordre lexicographique induit par l'ordre alphabétique $z<y<x$:

$$g_1=x-z,\quad g_2=-y+2z^2,\quad g_3=z^4+\frac{1}{2}z^2-\frac{1}{4}.$$

On a $\mathbf{V}(I)=\mathbf{V}(g_1,g_2,g_3)$. L'équation $g_3=0$ est de degré 4 en z, ses racines sont

$$z=\pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}.$$

Des équations $g_1=0$ et $g_2=0$, on déduit alors les valeurs de x et de y.

VI.2.3. Exemple : méthode des extrema liés de Lagrange sous une contrainte.— La méthode des extrema liés de Lagrange consiste à trouver les points extrema locaux d'une fonction

$p \longmapsto f(p)$ de classe C^1 sur un ouvert U de $\mathbb{R}^n$, lorsque le point p est asujetti aux contraintes exprimées sous la forme

$$h_1(p) = 0\,, \quad \ldots \quad , h_k(p) = 0.$$

Considérons le cas d'une seule contrainte $h(p) = 0$, où h est une fonction de classe C^1 définie sur l'ouvert U et telle que le gradient $\mathrm{grad}_p(h)$ de h au point p est non nul si $h(p) = 0$.

La méthode de Lagrange montre que la fonction f présente un extremum local en un point p, si les vecteurs gradients $\mathrm{grad}_p(f)$ et $\mathrm{grad}_p(h)$ son colinéaires. C'est-à-dire s'il existe un réel λ tel que

$$\mathrm{grad}_p(f) = \lambda \mathrm{grad}_p(h). \tag{VI.1}$$

Rappelons que le gradient de f est le vecteur défini par

$$\mathrm{grad}(f) = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}\right).$$

Les extrema p satisfont ainsi le système d'équations

$$\left|\begin{array}{rl} \frac{\partial f}{\partial x}(p) & = \lambda \frac{\partial h}{\partial x}(p) \\ \frac{\partial f}{\partial y}(p) & = \lambda \frac{\partial h}{\partial y}(p) \\ \frac{\partial f}{\partial z}(p) & = \lambda \frac{\partial h}{\partial z}(p) \\ h(p) & = 0 \end{array}\right.$$

Par exemple, on cherche les extrema de la fonction

$$f(x,y,z) = x^3 + 2xyz - z^2.$$

soumis à la contrainte $h(x,y,z) = x^2 + y^2 + z^2 - 1 = 0$. L'équation (VI.1) avec la contrainte $h(x,y,z) = 0$ donne ainsi un système de quatre équations

$$\left|\begin{array}{rl} 3x^2 + 2yz & = 2x\lambda \\ 2xz & = 2y\lambda \\ 2xy - 2z & = 2z\lambda \\ x^2 + y^2 + z^2 & = 1 \end{array}\right.$$

dont les solutions forment un ensemble algébrique affine. Posons

$$f_1 = 3x^2 + 2yz - 2x\lambda\,, \quad f_2 = 2xz - 2y\lambda\,,$$

$$f_3 = 2xy - 2z - 2z\lambda\,, \quad f_4 = x^2 + y^2 + z^2 - 1.$$

On construit une base de Gröbner de l'idéal $I = \langle f_1, f_2, f_3, f_4 \rangle$ de $\mathbb{R}[x,y,z,\lambda]$, avec l'ordre lexi-

cographique donné par $\lambda > x > y > z$. On obtient

$$\begin{aligned}
g_1 &= \lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2,\\
g_2 &= x^2 + y^2 + z^2 - 1,\\
g_3 &= xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z,\\
g_4 &= xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z,\\
g_5 &= y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z,\\
g_6 &= y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z,\\
g_7 &= yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2,\\
g_8 &= z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z.
\end{aligned}$$

Le polynôme g_8 ne dépend que de l'indéterminée z. Les solutions de l'équation $g_8(z) = 0$ sont

$$z = \pm\frac{1}{16}\sqrt{2}\sqrt{11}, \quad z = \pm\frac{2}{3}, \quad z = \pm 1, \quad z = 0.$$

Avec ces différentes valeurs de z, on peut obtenir les valeurs de x et y dans les autres équations :

$$\begin{aligned}
&z = 0,\ y = 0,\ x = 1; \quad z = 0,\ y = 0,\ x = -1;\\
&z = 0,\ y = 1,\ x = 0; \quad z = 0,\ y = -1,\ x = 0;\\
&z = 1,\ y = 0,\ x = 0; \quad z = -1,\ y = 0,\ x = 0;\\
&z = \frac{2}{3},\ y = \frac{1}{3},\ x = -\frac{2}{3}; \quad z = -\frac{2}{3},\ y = -\frac{1}{3},\ x = -\frac{2}{3};\\
&z = \frac{\sqrt{11}}{8\sqrt{2}},\ y = \frac{-3\sqrt{11}}{8\sqrt{2}},\ x = -\frac{3}{8}; \quad z = -\frac{\sqrt{11}}{8\sqrt{2}},\ y = \frac{3\sqrt{11}}{8\sqrt{2}},\ x = -\frac{3}{8}.
\end{aligned}$$

Le choix de l'ordre lexicographique avec l'ordre $\lambda > x > y > z$ permet d'éliminer des indéterminées dans les équations. L'indéterminée λ est éliminée en premier, puis x, ...

§ 3 Une méthode d'élimination

Les exemples vus dans la section précédente mettent en évidence le procédé d'élimination qui peut apparaître lorsque l'on calcule une base de Gröbner avec l'ordre lexicographique

VI.3.1. Exemple.— On considère le système d'équations

$$\left|\begin{array}{ll} x^2 + y + z &= 1,\\ x + y^2 + z &= 1,\\ x + y + z^2 &= 1. \end{array}\right. \tag{VI.2}$$

Soit I l'idéal de $\mathbb{R}[x,y,z]$ défini par ces équations :

$$I = \left\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 \right\rangle.$$

On calcule une base de Gröbner G de I pour l'ordre lexicographique induit par $z < y < x$. On a $G = \{g_1, g_2, g_3, g_4\}$, avec

$$\begin{aligned} g_1 &= x+y+z^2-1, \\ g_2 &= y^2-y-z^2+z, \\ g_3 &= 2yz^2+z^4-z^2, \\ g_4 &= z^6-4z^4+4z^3-z^2. \end{aligned}$$

Le système (VI.2) possède les mêmes solutions que le système

$$\left| \begin{array}{rl} x+y+z^2-1 &= 0, \\ y^2-y-z^2+z &= 0, \\ 2yz^2+z^4-z^2 &= 0, \\ z^6-4z^4+4z^3-z^2 &= 0. \end{array} \right. \tag{VI.3}$$

On remarque que le polynôme g_4 est d'une seule indéterminée :

$$g_4 \in I \cap \mathbb{R}[z].$$

Le polynôme g_4 se factorise en

$$g_4 = z^2(z-1)^2(z^2+2z-1).$$

Les racines du polynôme g_4 sont les valeurs de z, ainsi

$$0, \quad 1, \quad -1-\sqrt{2}, \quad -1+\sqrt{2}.$$

En substituant ces valeurs dans les polynômes g_2 et g_3, on obtient les valeurs de l'indéterminée y. Ensuite en substituant les valeurs de y et z dans le polynôme g_1, on obtient les valeurs de x. Le système d'équations (VI.2) admet ainsi cinq solutions :

$$(1,0,0), \quad (0,1,0), \quad (0,0,1),$$

$$(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}), \quad (-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}).$$

Pour résoudre ce système, nous avons procédé en deux étapes :

- une étape d'*élimination* qui a produit une équation $g_4 = 0$ d'une seule indéterminée z, obtenue après éliminitation des indéterminées x et y,
- une étape d'*extension*, après résolution de l'équation $g_4 = 0$, on étend ces solutions aux autres équations, pour déterminer les valeurs des autres indéterminées.

VI.3.2. Idéal d'élimination.— Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Le k - ième *idéal d'élimination* I_k est l'idéal de $\mathbb{K}[x_{k+1}, \ldots, x_n]$ défini par

$$I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

Les éléments de I_k sont des *conséquences* du système d'équations

$$f_1 = \ldots = f_s = 0,$$

après élimination des indéterminées $x_1, \ldots, x_k$.

Noter que $I_0 = I$ et que les idéaux d'élimination dépendent de l'ordre des indéterminées. Le résultat suivant montre comment extraire d'une base de Gröbner de I une base de Gröbner de I_k.

VI.1 Théorème (Théorème d'élimination). — Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et soit G une base de Gröbner de I, pour l'ordre lexicographique induit par l'ordre alphabétique donné par $x_n < \ldots < x_2 < x_1$. Alors, pour tout $k \in [\![0, n]\!]$, l'ensemble

$$G_k = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$$

est une base de Gröbner de l'idéal d'élimination I_k.

Preuve. Fixons $k \in [\![1, n]\!]$. On a $G_k \subset I_k$, par définition G_k est une base de Gröbner de I_k si

$$\langle \mathrm{lt}(G_k) \rangle = \langle \mathrm{lt}(I_k) \rangle .$$

L'inclusion $\langle \mathrm{lt}(G_k) \rangle \subset \langle \mathrm{lt}(I_k) \rangle$ est immédiate. Montrons l'inclusion réciproque. Il suffit de montrer que pour tout polynôme f de I_k, le terme dominant $\mathrm{lt}(f)$ est divisible par un $\mathrm{lt}(g)$, où $g \in G_k$.

Soit donc $f \in I_k$. Comme G est une base de Gröbner de I et que $I_k \subset I$, alors $\mathrm{lt}(f)$ est divisible par $\mathrm{lt}(g)$, où $g \in G$. Le polynôme f est dans I_k, il ne possède donc que des indéterminées $x_{k+1}, \ldots, x_n$. Comme $\mathrm{lt}(f) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$, alors $\mathrm{lt}(g) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$.

D'après l'ordre lexicographique choisi, tout monôme de $\mathbb{K}[x_1, \ldots, x_n] \setminus \mathbb{K}[x_{k+1}, \ldots, x_n$ est plus grand que tout monôme de $\mathbb{K}[x_{k+1}, \ldots, x_n]$, de $\mathrm{lt}(g) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$, on déduit que g est un polynôme de $\mathbb{K}[x_{k+1}, \ldots, x_n]$; ainsi $g \in G_k$. □

VI.3.3. Exemple.— Reprenons l'exemple VI.3.1. Le premier idéal d'élimination est

$$I_1 = I \cap \mathbb{R}[y, z] = \left\langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2 \right\rangle$$

et le deuxième est

$$I_2 = I \cap \mathbb{R}[z] = \left\langle z^6 - 4z^4 + 4z^3 - z^2 \right\rangle .$$

Du théorème d'élimination VI.1, on déduit que tout polynôme qui élimine les indéterminées x et y est un multiple du polynôme $g_4 = z^6 - 4z^4 + 4z^3 - z^2$.

§ 4 Problème d'impliciter une présentation paramétrée

VI.4.1. Problème d'impliciter une présentation paramétrée.— *Étant donné un paramétrage*

$$x_i = f_i(t_1, \ldots, t_m), \quad i \in [\![1, n]\!], \quad f_i \in \mathbb{K}[t_1, \ldots, t_m],$$

d'un ensemble algébrique affine $\mathbf{V}$ *de* $\mathbb{K}^n$*, déterminer des polynômes* $g_1,\ldots,g_s$ *de* $\mathbb{K}[x_1,\ldots,x_n]$*, tels que*

$$\mathbf{V} = \mathbf{V}(g_1,\ldots,g_s).$$

Considérons l'ensemble algébrique affine de $\mathbb{K}^{n+m}$ défini par le système d'équations suivant

$$\left|\begin{array}{rl} x_1 - f_1(t_1,\ldots,t_m) & = 0 \\ & \vdots \\ x_n - f_n(t_1,\ldots,t_m) & = 0 \end{array}\right.$$

en les indéterminées $x_1,\ldots,x_n,t_1,\ldots,t_m$. L'objectif est d'éliminer les indéterminées $t_1,\ldots,t_m$ dans ces équations. On utilise pour cela les bases de Gröbner, comme méthode d'élimination, avec l'ordre lexicographique sur $\mathbb{K}[x_1,\ldots,x_n,t_1,\ldots,t_m]$ avec l'ordre alphabétique suivant

$$t_1 > \ldots > t_m > x_1 > \ldots > x_n.$$

Le calcul d'une base de Gröbner de l'idéal $I = \langle x_1 - f_1,\ldots,x_n - f_n\rangle$ avec cet ordre permettra d'obtenir une base de polynômes où les indéterminées $t_1,\ldots,t_m$ ont été éliminées.

VI.4.2. Exemple.— Considérons la courbe paramétrée $\mathscr{C}$ dans $\mathbb{C}^3$ définie par les équations suivantes

$$\left|\begin{array}{rl} x & = t^4, \\ y & = t^3, \\ z & = t^2. \end{array}\right. \tag{VI.4}$$

Considérons l'ordre lexicographique sur $\mathbb{C}[t,x,y,z]$ avec $z < y < x < t$. On calcule une base de Gröbner G de l'idéal

$$I = \left\langle t^4 - x,\, t^3 - y,\, t^2 - z\right\rangle$$

On obtient

$$G = \{t^2 - z,\, ty - z^2,\, tz - y,\, x - z^2,\, y^2 - z^3\}.$$

Ainsi

$$I = \left\langle t^2 - z,\, ty - z^2,\, tz - y,\, x - z^2,\, y^2 - z^3\right\rangle.$$

L'ensemble algébrique affine

$$\mathbf{V}(x - z^2,\, y^2 - z^3) = \mathbf{V}(I \cap \mathbb{C}[x,y,z])$$

est-il le plus petit contenant la courbe paramétrée $\mathscr{C}$?

VI.4.3. Théorème de l'implicitation.— Considérons une paramétrisation polynomiale

$$\begin{array}{l} x_1 = f_1(t_1,\ldots,t_m) \\ \quad\vdots \\ x_n = f_n(t_1,\ldots,t_m) \end{array} \tag{VI.5}$$

où $f_1,\ldots,f_n \in \mathbb{K}[t_1,\ldots,t_m]$. On peut associer une fonction

$$F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$$

définie par

$$F(t_1,\dots,t_m) = (f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

Ainsi $F(\mathbb{K}^m)$ est le sous-ensemble de $\mathbb{K}^n$ paramétrisé par les équations VI.5.

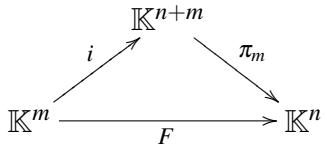
En général, $F(\mathbb{K}^m)$ n'est pas un ensemble algébrique affine. L'objectif est construire le plus petit ensemble algébrique affine de $\mathbb{K}^n$ contenant l'ensemble $F(\mathbb{K}^m)$. On considère pour cela l'ensemble algébrique affine

$$\mathbf{V} = \mathbf{V}(x_1 - f_1,\dots,x_n - f_n) \subset \mathbb{K}^{n+m}.$$

Les points de $\mathbf{V}$ s'écrivent

$$(t_1,\dots,t_m,f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

L'ensemble $\mathbf{V}$ est ainsi le graphe de la fonction F. On considère les applications i et π_m



définies par

$$i(t_1,\dots,t_m) = (t_1,\dots,t_m,f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

$$\pi_m(t_1,\dots,t_m,x_1,\dots,x_n) = (x_1,\dots,x_n).$$

On a $F = \pi_m \circ i$. Comme $i(\mathbb{K}^m) = \mathbf{V}$, on a

$$F(\mathbb{K}^m) = \pi_m(\mathbf{V}).$$

Ainsi, l'image de la paramétrisation est la projection de son graphe sur $\mathbb{K}^n$. Le théorème suivant construit le plus petit ensemble algébrique affine contenant $F(\mathbb{K}^n)$.

VI.2 Théorème (admis).— Soit $\mathbb{K}$ un corps infini. Soit $F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$ une application définie par une paramétrisation polynomiale

$$x_i = f_i(t_1,\dots,t_m), \quad i \in [\![1,n]\!], \quad f_i \in \mathbb{K}[t_1,\dots,t_m].$$

Soit I l'idéal de $\mathbb{K}[t_1,\dots,t_m,x_1,\dots,x_n]$ défini par

$$I = \langle x_1 - f_1,\dots,x_n - f_n \rangle.$$

Soit $I_m = I \cap \mathbb{K}[x_1,\dots,x_n]$ le m-ième idéal d'intersection de I. Alors $\mathbf{V}(I_m)$ est le plus petit sous-ensemble algébrique affine de $\mathbb{K}^n$ contenant le sous-ensemble paramétré $F(\mathbb{K}^m)$.

VI.4.4. Algorithme pour rendre implicite une présentation paramétrée.—

ENTRÉE : $x_i = f_i(t_1,\dots,t_m), \quad i \in [\![1,n]\!], \quad f_i \in \mathbb{K}[t_1,\dots,t_m]$.

Considérer l'idéal $I = \langle x_1 - f_1,\dots,x_n - f_n \rangle$.

Calculer une base de Gröbner G de I avec un ordre lexicographique où chaque t_i est plus grand que chaque x_i.

D'après le théorème VI.1, $G \cap \mathbb{K}[x_1,\ldots,x_n]$ est une base de Gröbner de I_m.

SORTIE : $\mathbf{V}(G \cap \mathbb{K}[x_1,\ldots,x_n])$, qui est, d'après le théorème VI.2, le plus petit ensemble algébrique qui contient la paramétrisation.

VI.4.5. Exemple.— La cubique tordue est l'ensemble algébrique affine de $\mathbb{R}^3$ défini par $\mathbf{V} = \mathbf{V}(y-x^2, z-x^3)$, c'est l'intersection des deux surfaces de $\mathbb{R}^3$:

$$y = x^2, \quad z = x^3.$$

La surface tangente à la courbe $\mathbf{V}$ est obtenue comme la réunion des droites tangentes à la courbe.

Pour définir cette surface, on considère la description paramétrique de la courbe $\mathbf{V}$:

$$\left| \begin{array}{ll} x & = t \\ y & = t^2 \\ z & = t^3 \end{array} \right. \tag{VI.6}$$

Tout réel t défini un point $c(t) = (t, t^2, t^3)$ de la courbe. Le vecteur tangent en t à la courbe est $c'(t) = (1, 2t, 3t^2)$. La droite tangente à la courbe en t est paramétrée par

$$c(t) + uc'(t) = (t+u, t^2+2tu, t^3+3t^2u).$$

La surface tangente de la cubique tordue est ainsi paramétrée par

$$\left| \begin{array}{ll} x & = t+u, \\ y & = t^2+2tu, \\ z & = t^3+3t^2u. \end{array} \right. \tag{VI.7}$$

On calcule une base de Gröbner G de l'idéal

$$I = \left\langle t+u-x, t^2+2tu-y, t^3+3t^2u-z \right\rangle.$$

avec l'ordre lexicographique induit par l'ordre alphabétique $t > u > x > y > z$. On a $G = \{g_1,\ldots,g_7\}$ avec

$$\begin{aligned}
g_1 &= t+u-x, \\
g_2 &= u^2-x^2+y, \\
g_3 &= ux^2-uy-x^3+\frac{3}{2}xy-\frac{1}{2}z, \\
g_4 &= uxy-uz-x^2y-xz+2y^2, \\
g_5 &= uxz-uy^2+x^2z-\frac{1}{2}xy^2-\frac{1}{2}yz, \\
g_6 &= uy^3-uz^2-2x^2yz+\frac{1}{2}xy^3-xz^2+\frac{5}{2}y^2z, \\
g_7 &= x^3z-\frac{3}{4}x^2y^2-\frac{3}{2}xyz+y^3+\frac{1}{4}z^2.
\end{aligned}$$

D'après le théorème d'élimination VI.1, on a

$$I_2 = I \cap \mathbb{R}[x,y,z] = \langle g_7 \rangle.$$

D'après le théorème d'implicitation VI.2, $\mathbf{V}(g_7)$ est le plus petit ensemble algébrique affine

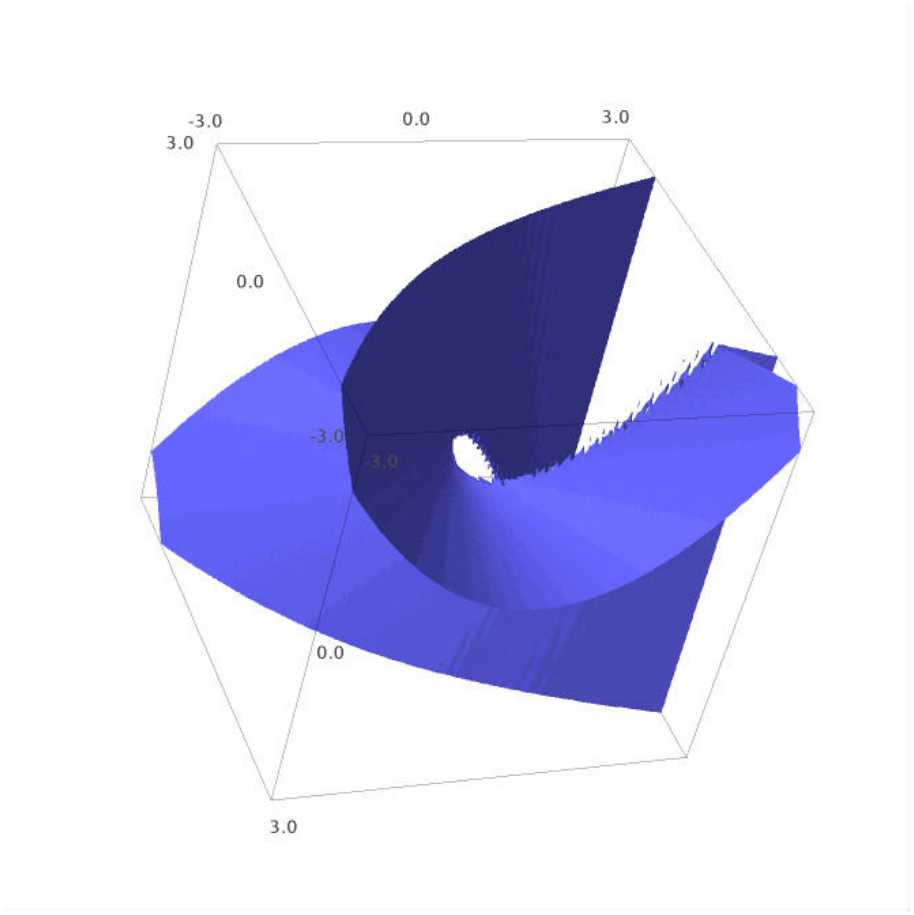
contenant la surface tangente.

Le code Sage pour calculer la base de Gröbner G :

```
sage: A.<t,u,x,y,z> = PolynomialRing(RationalField(), 5, order='lex')
sage: f1 = t + u - x
sage: f2 = t^2 + 2*t*u - y
sage: f3 = t^3 + 3*t^2*u - z
sage: I = (f1,f2,f3)*A
sage: G = I.groebner_basis()
sage: G
[t + u - x, u^2 - x^2 + y, u*x^2 - u*y - x^3 + 3/2*x*y - 1/2*z, u*x*y -
u*z - x^2*y - x*z + 2*y^2, u*x*z - u*y^2 + x^2*z - 1/2*x*y^2 - 1/2*y*z,
u*y^3 - u*z^2 - 2*x^2*y*z + 1/2*x*y^3 - x*z^2 + 5/2*y^2*z, x^3*z -
3/4*x^2*y^2 - 3/2*x*y*z + y^3 + 1/4*z^2]
```

Pour tracer la surface :

```
sage: var('x,y,z')
sage: h = lambda x, y , z:x^3*z - 3/4*x^2*y^2 - 3/2*x*y*z + y^3 + 1/4*z^2
sage: f = implicit_plot3d(h, (x,-3,3), (y, -3,3), (z, -3,3),
                                        plot_points=100, adaptative = True)
sage: f
```



CHAPITRE
VII

Applications des bases de Gröbner à la géométrie élémentaire

Sommaire

Dans cette partie on illustre l'utilisation des bases de Gröbner pour retrouver de manière effective des théorèmes de géométrie élémentaire.

§ 1 Traduction algébrique de problèmes de géométrie

VII.1.1. Droite de Gauss-Newton.— On considère un quadrilatère convexe $ABCD$ sans côtés parallèles et on note E le point d'intersection de (AB) avec (CD) et F le point d'intersection de (AD) avec (BC). Soient I, J et K les milieux respectifs des trois diagonales $[AC]$, $[BD]$ et $[EF]$ de ce *quadrilatère complet*. Alors les trois points I, J et K sont alignés.

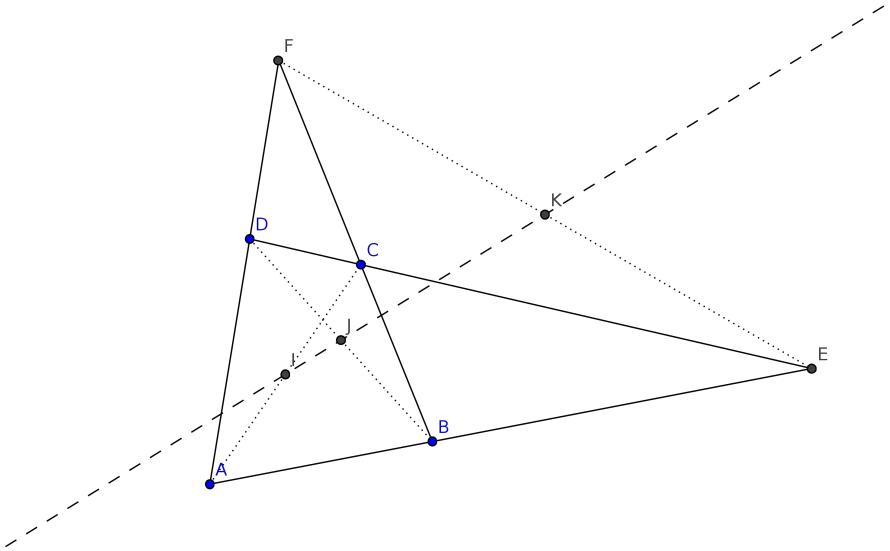


FIGURE VII.1.: Droite de Gauss-Newton

On peut retrouver ce résultat en traduisant les hypothèses géométriques par des relations polynomiales : pour cela, on considère les coordonnées des points A, B, C, D, F, I, J, K dans la plan euclidien. Sans perdre de généralités, on peut supposer que A est à l'origine et B sur l'axe des abscisses. On obtient ainsi

$$\begin{array}{llllll} A=(0,0), & B=(x_0,0), & C=(x_1,x_2), & D=(x_3,x_4), & E=(x_5,0), \\ F=(x_6,x_7), & I=(x_8,x_9), & J=(x_{10},x_{11}) & K=(x_{12},x_{13}). & & \end{array}$$

On traduit les hypothèses géométriques en terme d'équations polynomiales :

– $E \in (AB) \cap (CD)$ se traduit par $\begin{vmatrix} x_5-x_1 & x_3-x_1 \\ -x_2 & x_4-x_2 \end{vmatrix} = 0$, c'est-à-dire par

$$-x_1x_4+x_2x_3-x_2x_5+x_4x_5=0$$

(ici comme on a pris A, B et E sur l'axe des abscisses, l'hypothèse $E \in (AB)$ est déjà vérifiée).

– $F \in (AD) \cap (BC)$ se traduit par $\begin{vmatrix} x_6 & x_3 \\ x_7 & x_4 \end{vmatrix} = 0$ et $\begin{vmatrix} x_6-x_0 & x_1-x_0 \\ -x_7 & x_2 \end{vmatrix} = 0$, c'est-à-dire par

$$-x_3x_7+x_4x_6=0 \text{ et } -x_0x_2+x_0x_7-x_1x_7+x_2x_6=0.$$

– I est le milieu de $[AC]$ se traduit par

$$2x_8-x_1=0 \text{ et } 2x_9-x_2=0.$$

– J est le milieu de $[BD]$ se traduit par

$$2x_{10}-x_0-x_3=0 \text{ et } 2x_{11}-x_4=0.$$

– K est le milieu de $[EF]$ se traduit par

$$2x_{12}-x_5-x_6=0 \text{ et } 2x_{13}-x_7=0.$$

La conclusion, les trois points I, J et K sont alignés, est équivalente à

$\begin{vmatrix} x_{10}-x_8 & x_{12}-x_8 \\ x_{11}-x_9 & x_{13}-x_9 \end{vmatrix} = 0$ c'est-à-dire à

$$x_8x_{11} - x_8x_{13} - x_9x_{10} + x_9x_{12} + x_{10}x_{13} - x_{11}x_{12} = 0.$$

On se place dans l'anneau $\mathbb{R}[x_0, x_1, \ldots, x_{13}]$ et on pose

$$\begin{aligned}
f_1 &= -x_1x_4 + x_2x_3 - x_2x_5 + x_4x_5, & f_2 &= -x_3x_7 + x_4x_6, \\
f_3 &= -x_0x_2 + x_0x_7 - x_1x_7 + x_2x_6, & f_4 &= 2x_8 - x_1, \\
f_5 &= 2x_9 - x_2, & f_6 &= 2x_{10} - x_0 - x_3, \\
f_7 &= 2x_{11} - x_4 = 0, & f_8 &= 2x_{12} - x_5 - x_6, \\
f_9 &= 2x_{13} - x_7, & f &= x_8x_{11} - x_8x_{13} - x_9x_{10} + x_9x_{12} + x_{10}x_{13} - x_{11}x_{12}.
\end{aligned}$$

On peut alors vérifier en calculant une base de Gröbner (ou directement avec Sage) que $f \in \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9 \rangle$.

On en déduit que $f = 0$ est conséquence du système $f_1 = f_2 = f_3 = f_4 = f_5 = f_6 = f_7 = f_8 = f_9 = 0$.

Le code Sage pour vérifier que $f \in \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9 \rangle$:

```
sage: R= PolynomialRing(QQ, 'x',14)
sage: x= R.gens()
sage: f1 = (x[4]-x[2])*(x[5]-x[1])+x[2]*(x[3]-x[1])
sage: f2 = x[4]*x[6]-x[3]*x[7]
sage: f3 = x[2]*(x[6]-x[0])-(x[1]-x[0])*x[7]
sage: f4 = 2*x[8]-x[1]
sage: f5 = 2*x[9]-x[2]
sage: f6 = 2*x[10] - x[3]-x[0]
sage: f7 = 2*x[11] - x[4]
sage: f8 = 2*x[12] - x[5]-x[6]
sage: f9 = 2*x[13] -x[7]
sage: f = (x[10]-x[8])*(x[13]-x[9]) -(x[11]-x[9])*(x[12]-x[8])
sage: I = (f1,f2,f3,f4,f5,f6,f7,f8,f9)*R
sage: f in I
True
```

En utilisant l'ordre lexicographique et le théorème d'élimination, on peut retrouver directement la propriété de colinéarité des points I, J, K :

```
sage: R= PolynomialRing(QQ, 'x',14, order ='lex')
sage: x= R.gens()
sage: f1 = (x[4]-x[2])*(x[5]-x[1])+x[2]*(x[3]-x[1])
sage: f2 = x[4]*x[6]-x[3]*x[7]
sage: f3 = x[2]*(x[6]-x[0])-(x[1]-x[0])*x[7]
sage: f4 = 2*x[8]-x[1]
sage: f5 = 2*x[9]-x[2]
sage: f6 = 2*x[10] - x[3]-x[0]
sage: f7 = 2*x[11] - x[4]
sage: f8 = 2*x[12] - x[5]-x[6]
sage: f9 = 2*x[13] -x[7]
sage: I = (f1,f2,f3,f4,f5,f6,f7,f8,f9)*R
sage: G = I.groebner_basis()
sage: print G
[x0 + x3 - 2*x10, x1 - 2*x8, x2 - 2*x9, x3*x9 + x6*x9 - x6*x11 -
2*x8*x13 - 2*x9*x10 + 2*x10*x13, x3*x13 - x6*x11, x4 - 2*x11, x5 + x6 -
2*x12, x6*x8*x9*x13 - 1/2*x6*x8*x13^2 + 1/2*x6*x9^2*x10 -
1/2*x6*x9^2*x12 - x6*x9*x10*x13 + 1/2*x6*x10*x13^2 - x8^2*x13^2 -
x8*x9*x10*x13 + x8*x10*x13^2 + x8*x12*x13^2 + x9*x10*x12*x13 -
x10*x12*x13^2, x6*x9*x11 + x6*x9*x13 - x6*x11*x13 - 2*x8*x13^2 -
2*x9*x10*x13 + 2*x10*x13^2, x7 - 2*x13, x8*x11 - x8*x13 - x9*x10 +
x9*x12 + x10*x13 - x11*x12]
```

VII.1.2. Remarque.— Pour les calculs avec Sage ci-dessus, on se limite à l'anneau des polynômes à coefficients rationnels, car les hypothèses et la conclusion sont à coefficients rationnels

et tous calculs intermédiaires (divisions, réductions, calcul de bases de Gröbner) ne font également intervenir que des des polynômes à coefficients rationnels.

Exercice 100. — En traduisant les hypothèses géométriques dans le repère affine $(A, \overrightarrow{AB}, \overrightarrow{AD})$, retrouver le résultat sur la droite de Gauss-Newton.

VII.1 Proposition. — Soit A, B, C, D, E, F six points distincts du plan euclidien orienté. Les énoncés géométriques suivants s'expriment par des équations polynomiales :

1. les droites (AB) et (CD) sont parallèles ;
2. les droites (AB) et (CD) sont perpendiculaires ;
3. les points A, B et C sont alignés ;
4. les distances AB et CD sont égales ;
5. le point C appartient au cercle de centre A et de rayon AB ;
6. le point C est le milieu du segment $[AB]$;
7. les angles orientés $(\widehat{\overrightarrow{AB}, \overrightarrow{AC}})$ et $(\widehat{\overrightarrow{DE}, \overrightarrow{DF}})$ sont égaux modulo π ;
8. la droite (BD) est la bissectrice de l'angle $\widehat{ABC}$;
9. le point C appartient à la médiatrice de $[AB]$.

Exercice 101. — Montrer la proposition VII.1. Pour le point 7 rappelons que

$$\det(\overrightarrow{AB}, \overrightarrow{AC}) = AB \times AC \times \sin(\widehat{\overrightarrow{AB}, \overrightarrow{AC}}) \text{ et } \overrightarrow{AB} \cdot \overrightarrow{AC} = AB \times AC \times \cos(\widehat{\overrightarrow{AB}, \overrightarrow{AC}})$$

Exercice 102. — Soit ABC un triangle. Traduire en termes d'équations polynomiales les théorèmes de géométrie suivants :

1. Les trois hauteurs de ABC se coupent en unique point, appelé l'orthocentre de ABC.
2. Les trois médianes de ABC se coupent en unique point, appelé le centre de gravité de ABC.
3. Le centre du cercle circonscrit, l'orthocentre et le centre gravité du triangle ABC sont alignés. (La droite contenant ces trois points est appelée droite d'Euler.)

§ 2 Conséquences d'un système d'équations algébriques et radical d'un idéal

VII.2.1. Conséquences d'un système d'équations algébriques.— Dans la partie précédente, on a étudié un théorème de géométrie dont les hypothèses et les conclusions peuvent être traduites en termes de systèmes d'équations polynomiales. De manière abstraite, la question est de résoudre le problème suivant :

Étant donnés des polynômes $f_1, \ldots, f_s, g$ de $\mathbb{K}[x_1, \ldots, x_n]$, est-ce que

$$g(x_1, \ldots, x_n) = 0 \textit{ est conséquence du système } \left| \begin{array}{c} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{array} \right. ?$$

Définition VII.2. — Soit $f_1, \ldots, f_s, g$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. On dit que l'équation $g = 0$ est une *conséquence* du système d'équations $f_1 = \ldots = f_s = 0$ si $g(a_1, \ldots, a_n) = 0$ pour tout $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$, autrement dit si

$$g \in I(\mathbf{V}(f_1, \ldots, f_s)).$$

VII.2.2. Radical d'un idéal.—

VII.3 Proposition. — Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. L'ensemble $\sqrt{I}$ suivant, appelé *radical* de I,

$$\sqrt{I} := \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f^m \in I \text{ pour un entier } m\}$$

est un idéal contenant I.

Exercice 103. — 1. Montrer la proposition précédente.

2. Donner un exemple d'idéal strictement inclus dans son radical.

VII.4 Proposition. — Soit $f_1, \ldots, f_s, g$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$.
Si $g \in \sqrt{\langle f_1, \ldots, f_s \rangle}$ alors l'équation $g = 0$ est une conséquence du système d'équations $f_1 = \ldots = f_s = 0$.

Exercice 104. — 1. Montrer la proposition précédente.

2. Donner un exemple de deux polynômes f et g de $\mathbb{R}[x, y]$ tel que $g = 0$ est conséquence de $f = 0$ mais $g \notin \sqrt{\langle f \rangle}$.

Dans le cas du corps $\mathbb{C}$ (et plus généralement d'un corps algébriquement clos), les deux notions sont équivalentes par le théorème des zéros de Hilbert :

VII.5 Théorème (admis !). — Soit $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$ alors

$$I(\mathbf{V}(f_1, \ldots, f_s)) = \sqrt{\langle f_1, \ldots, f_s \rangle}.$$

Autrement dit, pour tout polynôme $g \in \mathbb{C}[x_1, \ldots, x_n]$, l'équation $g = 0$ est conséquence du système $f_1 = \ldots = f_s = 0$ si et seulement si $g \in \sqrt{\langle f_1, \ldots, f_s \rangle}$.

Exercice 105. — Soit $f_1, \ldots, f_s \in \mathbb{R}[x_1, \ldots, x_n]$. On note $\mathbf{V}_{\mathbb{C}}(f_1, \ldots, f_s)$ l'ensemble algébrique affine formé des points de $\mathbb{C}^n$ satisfaisant le système $f_1 = \ldots = f_s = 0$. Soit $g \in \mathbb{R}[x_1, \ldots, x_n]$. Montrer que

$$g \in \sqrt{\langle f_1, \ldots, f_s \rangle} \subseteq \mathbb{R}[x_1, \ldots, x_n]$$

si et seulement si

$$g \in I(\mathbf{V}_{\mathbb{C}}(f_1, \ldots, f_s)) \subseteq \mathbb{C}[x_1, \ldots, x_n].$$

VII.2.3. Problème de l'appartenance au radical d'un idéal.— La théorème suivant donne un critère pour déterminer si un polynôme appartient au radical d'un idéal :

VII.6 Théorème (admis !). — Soit $f_1,\dots,f_s,g \in \mathbb{K}[x_1,\dots,x_n]$. Alors $g \in \sqrt{\langle f_1,\dots,f_s\rangle}$ si et seulement si

$$1 \in \langle f_1,\dots,f_s,1-yg\rangle \subseteq K[x_1,\dots,x_n,y].$$

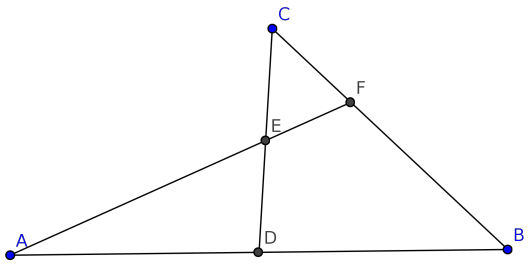
On peut donc répondre à ce problème en calculant une base de Gröbner de l'idéal $\langle f_1,\dots,f_s,1-yg\rangle$.

Exercice 106. — Soit $f_1,\dots,f_s,g \in \mathbb{K}[x_1,\dots,x_n]$ et $I = \langle f_1,\dots,f_s,1-yg\rangle \subseteq K[x_1,\dots,x_n,y]$. Soit G une base de Gröbner de I pour un ordre monomial fixé.

Montrer que $g \in \sqrt{\langle f_1,\dots,f_s\rangle}$ si et seulement si G contient un polynôme constant.

§ 3 Hypothèses implicites de généricité dans les théorèmes de géométrie

VII.3.1. Exemple.— Soit A, B et C trois points du plan affine. Soit D le milieu de $[AB]$ et E le milieu de $[CD]$. Si on note F le point d'intersection des droites (AE) et (BC), on a $FB = 2FC$.



Sans perte de généralité, on peut supposer que D est l'origine du plan et A et B sont sur l'axe des abscisses. Ainsi, on peut choisir les coordonnées suivantes pour les points de ce problème :

$$A = (-x_0,0),\quad B = (x_0,0),\quad C = (x_1,x_2),\quad D = (0,0),\quad E = (x_3,x_4),\quad F = (x_5,x_6).$$

Ce choix particulier de coordonnées assure que D est le milieu de $[AB]$. Traduisons en termes algébriques les autres hypothèses :

– E est le milieu de $[CD]$ se traduit par

$$2x_3 - x_1 = 0 \text{ et } 2x_4 - x_2 = 0.$$

– F est le point d'intersection des droites (AE) et (BC) se traduit par $\begin{vmatrix} x_5+x_0 & x_3+x_0 \\ x_6 & x_4 \end{vmatrix} = 0$ et $\begin{vmatrix} x_5-x_0 & x_1-x_0 \\ x_6 & x_2 \end{vmatrix} = 0$, c'est-à-dire par

$$x_0x_4 - x_0x_6 - x_3x_6 + x_4x_5 = 0 \text{ et } -x_0x_2 + x_0x_6 - x_1x_6 + x_2x_5 = 0.$$

Comme $F \in [BC]$, la conclusion $FB = 2FC$ est équivalente à

$$3x_5 - 2x_1 - x_0 = 0 \text{ et } 3x_6 - 2x_2 = 0.$$

Considérons maintenant les polynômes de $\mathbb{R}[x_0,x_1,x_2,x_3,x_4,x_5,x_6]$ suivants : $f_1 = 2x_3 - x_1$, $f_2 = 2x_4 - x_2$, $f_3 = x_0x_4 - x_0x_6 - x_3x_6 + x_4x_5$, $f_4 = -x_0x_2 + x_0x_6 - x_1x_6 + x_2x_5$, $g_1 = 3x_5 - 2x_1 - x_0$ et $g_2 = 3x_6 - 2x_2$.

Soit $I = \langle f_1, f_2, f_3, f_4 \rangle$. Alors $g_1 \notin I$ et $g_2 \notin I$:

```
sage: R.<x0,x1,x2,x3,x4,x5,x6>= PolynomialRing(QQ, 'x0,x1,x2,x3,x4,x5,x6')
sage: f1 = 2*x3-x1
sage: f2 = 2*x4-x2
sage: f3 = (x5+x0)*x4 -(x3+x0)*x6
sage: f4 = (x5-x0)*x2 - (x1-x0)*x6
sage: g1 = 3*x5-2*x1-x0
sage: g2 = 3*x6-2*x2
sage: I = (f1,f2,f3,f4)*R
sage: g1 in I, g2 in I
(False, False)
```

Mais, en fait g_1 et g_2 n'appartiennent pas non plus au radical $\sqrt{I}$:

```
sage: R.<x0,x1,x2,x3,x4,x5,x6,y>= PolynomialRing(QQ, 'x0,x1,x2,x3,x4,x5,x6,y')
sage: f1 = 2*x3-x1
sage: f2 = 2*x4-x2
sage: f3 = (x5+x0)*x4 -(x3+x0)*x6
sage: f4 = (x5-x0)*x2 - (x1-x0)*x6
sage: g1 = 3*x5-2*x1-x0
sage: g2 = 3*x6-2*x2
sage: h1 = 1-y*g1
sage: h2 = 1-y*g2
sage: I1 = (f1,f2,f3,f4,h1)*R
sage: I2 = (f1,f2,f3,f4,h2)*R
sage: 1 in I1, 1 in I2
(False, False)
```

Cela signifie que les équations $g_1 = 0$ et $g_2 = 0$ ne sont pas conséquences du système $f_1 = f_2 = f_3 = f_4 = 0$ au-dessus du corps des complexes. Dans la traduction ci-dessus on omet de traduire l'hypothèse implicite de généricité : les points A, B et C ne sont pas colinéaires ; c'est-à-dire l'hypothèse $x_0x_2 \neq 0$.

Pour inclure l'inéquation $x_0x_2 \neq 0$ parmi les hypothèses, on considère une nouvelle variable t et l'équation $1 - x_0x_2t = 0$. Posons $f_5 = 1 - x_0x_2t$ et $J = \langle f_1, f_2, f_3, f_4, f_5 \rangle \subseteq \mathbb{R}[x_0,x_1,x_2,x_3,x_4,x_5,x_6,t]$. Alors, on vérifie que g_1 et g_2 appartiennent à J :

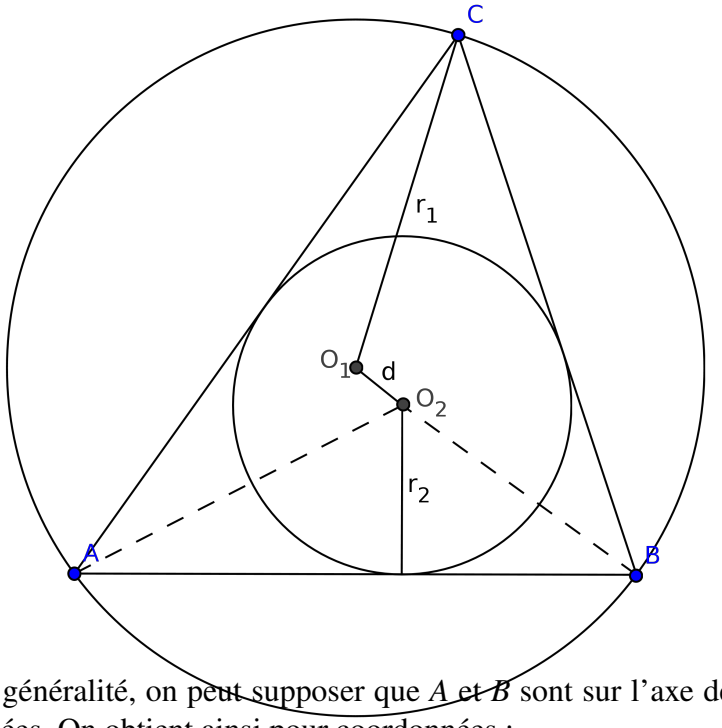
```
sage: R.<t,x0,x1,x2,x3,x4,x5,x6>= PolynomialRing(RR, 't,x0,x1,x2,x3,x4,x5,x6')
sage: f1 = 2*x3-x1
sage: f2 = 2*x4-x2
sage: f3 = (x5+x0)*x4 -(x3+x0)*x6
sage: f4 = (x5-x0)*x2 - (x1-x0)*x6
sage: f5 = 1-t*x0*x2
sage: g1 = 3*x5-2*x1-x0
sage: g2 = 3*x6-2*x2
sage: I = (f1,f2,f3,f4,f5)*R
sage: g1 in I,g2 in I
(True, True)
```

Exercice 107. — Dans cet exemple, il n'est pas question d'angles. On peut donc considérer le repère affine $(D, \overrightarrow{DB}, \overrightarrow{DC})$. Retrouver ainsi le résultat.

Exercice 108. — Reprendre l'exercice 102 et vérifier à l'aide du logiciel Sage que les conclusions sont des conséquences des hypothèses après ajout éventuel d'hypothèses de généricité.

§ 4 Découvrir ou redécouvrir des théorèmes de géométrie

VII.4.1. Théorème de Poncelet.— Dans cette partie, nous retrouvons en utilisant les bases de Gröbner, un résultat de Poncelet qui établit une relation entre les rayons des cercles inscrits et circonscrits d'un triangle et la distance entre les deux centres de ces cercles. Soit ABC un triangle, O_1 le centre du cercle circonscrit de rayon r_1 et O_2 le centre du cercle inscrit de rayon r_2. Notons d la distance O_1O_2.



Sans perte de généralité, on peut supposer que A et B sont sur l'axe des abscisses et O_2 sur l'axe des ordonnées. On obtient ainsi pour coordonnées :

$$A(x_1,0),\quad B(x_2,0)\quad O_2(0,r_2)\quad C(x_3,x_4)\quad O_1(x_5,x_6).$$

L'hypothèse "(AO_2) est la bissectrice de $(\overrightarrow{AB},\overrightarrow{AC})$" s'exprime par l'équation

$$\begin{vmatrix} \overrightarrow{AB}\cdot\overrightarrow{AO_2} & \overrightarrow{AC}\cdot\overrightarrow{AO_2} \\ -\det(\overrightarrow{AB},\overrightarrow{AO_2}) & \det(\overrightarrow{AC},\overrightarrow{AO_2}) \end{vmatrix} = 0.$$

Après calculs, on obtient

$$(x_2-x_1)((r_2^2-x_1^2)x_4-2x_1r_2(x_3-x_1))=0.$$

De la même façon, on obtient pour l'hypothèse "(BO_2) est la bissectrice de $(\overrightarrow{BA},\overrightarrow{BC})$" l'équation

$$(x_2-x_1)((r_2^2-x_2^2)x_4-2x_2r_2(x_3-x_2))=0.$$

Le fait que O_1 soit à l'intersection des médiatrices des segments $[AB]$ et $[BC]$ correspond aux égalités suivantes

$$\overrightarrow{AB}\cdot\overrightarrow{AO_1}=\overrightarrow{BA}\cdot\overrightarrow{BO_1} \text{ et } \overrightarrow{BC}\cdot\overrightarrow{BO_1}=\overrightarrow{CB}\cdot\overrightarrow{CO_1}.$$

Après calculs, on obtient

$$(x_2-x_1)(2x_5-x_2-x_1)=0 \text{ et } 2x_4x_6+2x_3x_5-2x_2x_5-x_4^2-x_3^2+x_2^2=0.$$

Pour d, r_1, on obtient les équations suivantes :

$$d^2-(x_6-r_2)^2-x_5^2=0,$$
$$r_1^2-x_6^2-(x_5-x_1)^2=0$$

Comme on ne considère pas le cas dégénéré où $A=B$, on suppose que $x_2-x_1\neq 0$ et on pose alors

$$\begin{aligned}
f_1&=(r_2^2-x_1^2)x_4-2x_1r_2(x_3-x_1),\\
f_2&=(r_2^2-x_2^2)x_4-2x_2r_2(x_3-x_2),\\
f_3&=2x_5-x_2-x_1,\\
f_4&=2x_4x_6+2x_3x_5-2x_2x_5-x_4^2-x_3^2+x_2^2,\\
f_5&=d^2-(x_6-r_2)^2-x_5^2,\\
f_6&=r_1^2-x_6^2-(x_5-x_1)^2.
\end{aligned}$$

Soit l'idéal $I=\langle f_1,\ldots,f_6\rangle\subseteq\mathbb{R}[d,r_1,r_2,x_1,\ldots,x_6]$. À l'aide de Sage(), on calcule une base de Gröbner correspondant à l'ordre lexicographique (inverse) associé à l'ordre alphabétique $d<r_1<r_2<x_1<\ldots<x_6$. Cette base comporte 97 polynômes et l'idéal d'élimination $I\cap\mathbb{R}[d,r_1,r_2]$ est trivial d'après le code Sage() ci-dessous

```
sage: R.<d,r1,r2,x1,x2,x3,x4,x5,x6> =
PolynomialRing(QQ,'d,r1,r2,x1,x2,x3,x4,x5,x6',order ='invlex')
sage: f1 = (r2^2-x1^2)*x4-2*x1*r2*(x3-x1)
sage: f2 = (r2^2-x2^2)*x4-2*x2*r2*(x3-x2)
sage: f3 = 2*x5-x2-x1
sage: f4 = 2*x4*x6+2*x3*x5-2*x2*x5-x4^2-x3^2+x2^2
sage: f5 = d^2-(x6-r2)^2-x5^2
sage: f6 = r1^2-x6^2-(x5-x1)^2
sage: I = (f1,f2,f3,f4,f5,f6)*R
sage: G = I.groebner_basis()
Polynomial Sequence with 97 Polynomials in 9 Variables
sage : G[96].factor()
(1/4) * r2 * x1 * (-2*r1*r2 - r1^2 + d^2) * (-2*r1*r2 + r1^2 - d^2) *
(-x1^2 - r2^2 - 2*r1*r2 - r1^2 + d^2) * (-x1^2 - r2^2 + 2*r1*r2 - r1^2 +
d^2) * (r2^2*x1^2 + r2^4 - 2*r1^2*r2^2 - 2*d^2*r2^2 + r1^4 - 2*d^2*r1^2
+ d^4)
```

On ne trouve pas ainsi une relation entre r_1, r_2 et d. Il faut éliminer pour cela le cas dégénéré et supposer que les points A, B et C ne sont pas colinéaires, ce qui est équivalent à $x_2-x_1\neq 0$ et $x_4\neq 0$.

On considère alors l'idéal $J=\langle f_1,\ldots,f_6,1-(x_2-x_1)s,1-x_4t\rangle\subseteq\mathbb{R}[d,s,t,r_1,r_2,x_1,\ldots,x_7]$. L'idéal d'élimination $J\cap\mathbb{R}[d,s,t]$ contient le polynôme

$$g=(d^2-r_1^2+2r_1r_2)(d^2-r_1^2-2r_1r_2)$$

d'après le code Sage() ci-dessous

```
sage: R.<d,r1,r2,s,t,x1,x2,x3,x4,x5,x6> =
PolynomialRing(QQ, 'd,r1,r2,s,t,x1,x2,x3,x4,x5,x6',order ='invlex')
sage: f1 = (r2^2-x1^2)*x4-2*x1*r2*(x3-x1)
sage: f2 = (r2^2-x2^2)*x4-2*x2*r2*(x3-x2)
sage: f3 = 2*x5-x2-x1
sage: f4 = 2*x4*x6+2*x3*x5-2*x2*x5-x4^2-x3^2+x2^2
sage: f5 = d^2-(x6-r2)^2-x5^2
sage: f6 = r1^2-x6^2-(x5-x1)^2
sage: f7 = 1-(x2-x1)*s
sage: f8 = 1-x4*t
sage: I = (f1,f2,f3,f4,f5,f6,f7,f8)*R
sage: G = I.groebner_basis()
sage: G.parent()
Category of sequences in Multivariate Polynomial Ring in d, r1, r2,
s, t, x1, x2, x3, x4, x5, x6 over Rational Field
```

```
sage : len(G)
18
sage: G[17].factor()
(1/4) * (2*r1*r2 - r1^2 + d^2) * (2*r1*r2 + r1^2 - d^2)
```

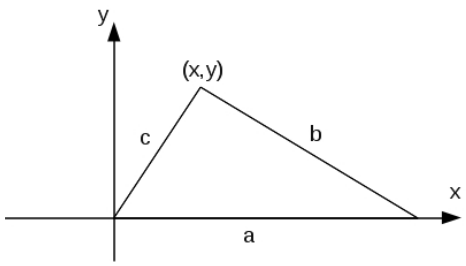
Comme $d < r_1$, on en déduit l'équation

$$r_1^2 - 2r_1r_2 = d^2.$$

VII.4.2. La formule de Héron.— La formule de Héron permet d'exprimer l'aire s d'un triangle quelconque en fonction des longueurs a, b et c de ses trois côtés :

$$s^2 = \frac{1}{16}(a+b+c)(a+b-c)(a-b+c)(-a+b+c).$$

Cette formule peut être obtenue par méthode d'élimination des indéterminées. Considérons le triangle suivant



Exercice 109. — Établir les relations suivantes :

$$b^2 = (a-x)^2 + y^2, \quad c^2 = x^2 + y^2, \quad 2s = ay.$$

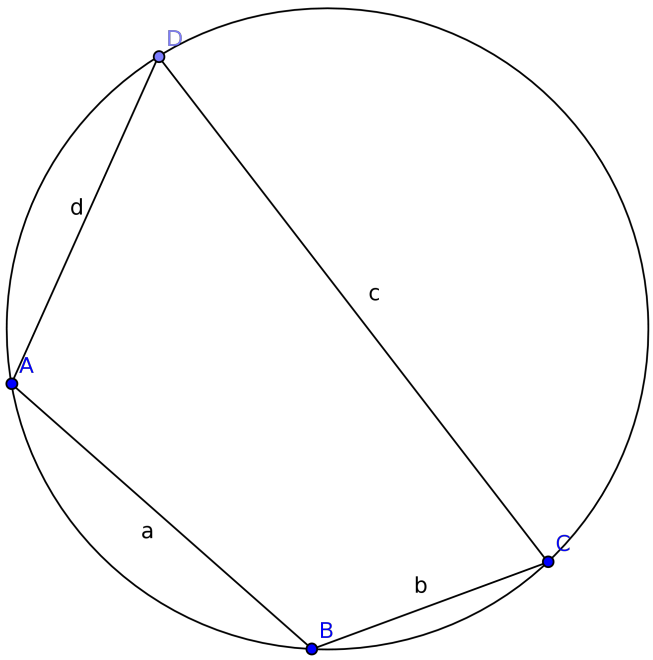
Considérons l'idéal I de $\mathbb{R}[x,y,a,b,c,s]$ engendré par les équations précédentes :

$$I = \left\langle b^2 - (a-x)^2 - y^2, c^2 - x^2 - y^2, 2s - ay \right\rangle$$

Exercice 110. —

1. Décrire le deuxième idéal d'élimination $I \cap \mathbb{R}[a,b,c,s]$.
2. En déduire la formule de Héron.
3. On pose $p = (a+b+c)/2$ le demi périmètre du triangle. Vérifier que la formule de Héron est équivalente à
$$s^2 = p(p-a)(p-b)(p-c).$$

VII.4.3. Formule de Brahmagupta.— La formule de Héron se généralise aux quadrilatères convexes inscriptibles, quadrilatères dont les sommets sont sur un même cercle.



Pour un tel quadrilatère dont les cotés sont de longueurs a, b, c et d, si l'on note $p = (a+b+c+d)/2$ le demi-périmètre du quadrilatère et s sa surface, on a alors la formule de Brahmagupta suivante :

$$s^2 = (p-a)(p-b)(p-c)(p-d).$$

(Si deux points sont confondus, on retrouve la formule de Héron.)

Exercice 111. —

1. En prenant pour origine le centre du cercle et pour coordonnées $A(x_1,x_2)$, $B(x_3,x_4)$, $C(x_5,x_6)$, $D(x_7,x_8)$, traduire les hypothèses par des équations algébriques. On vérifiera en particulier que l'aire "orientée" s satisfait l'équation suivante :

$$x_5x_8 - x_1x_8 - x_6x_7 + x_2x_7 + x_3x_6 - x_4x_5 + x_1x_4 - x_2x_3 - 2s = 0.$$

2. Soit I l'idéal correspondant à ces équations. En utilisant Sage, vérifier que l'idéal d'élimination $I \cap \mathbb{R}[a,b,c,d,s]$ est engendré par la polynôme $g = g_1g_2$ où

$$g_1 = 16s^2 + d^4 - 2c^2d^2 - 2b^2d^2 - 2a^2d^2 - 8abcd + c^4 - 2b^2c^2 - 2a^2c^2 + b^4 - 2a^2b^2 + a^4$$

et

$$g_2 = 16s^2 + d^4 - 2c^2d^2 - 2b^2d^2 - 2a^2d^2 + 8abcd + c^4 - 2b^2c^2 - 2a^2c^2 + b^4 - 2a^2b^2 + a^4.$$

3. Il suit que les hypothèses entraînent que $g_1 = 0$ ou $g_2 = 0$. Vérifier que $g_1 = 0$ correspond à la formule de Brahmagupta.

CHAPITRE
VIII

D'autres applications des bases de Gröbner

Sommaire

Cette dernière partie porte sur l'étude d'applications de la méthode l'élimination. On s'intéressera notamment à deux applications géométriques : la recherche de points singuliers d'une courbe, le calcul de l'enveloppe d'une famille de courbes. Ces deux problèmes fournissent des systèmes d'équations polynomiales que l'on peut résoudre par élimination en utilisant les bases de Gröbner. Enfin, on présente une application originale en robotique.

§ 1 Applications de l'élimination

VIII.1.1. Résolution de systèmes d'équations polynomiales.—

Exercice 112. — En utilisant le théorème d'élimination, déterminer les solutions réelles et complexes des systèmes d'équations polynomiales suivants :

$$\left|\begin{array}{rl} x^2+2y^2-y-2z &= 0\\ x^2-8y^2+10z &= 1\\ x^2-7yz &= 0 \end{array}\right. \qquad \left|\begin{array}{rl} x^2+y^2+z^2-2x &= 0\\ x^3-yz-x &= 0\\ x-y+2z &= 0 \end{array}\right.$$

Exercice 113. — Résoudre en fonction de a le système d'équations polynomiales suivant :

$$\left|\begin{array}{rl} x^2+y+z &= a\\ x+y^2+z &= a\\ x+y+z^2 &= a \end{array}\right.$$

VIII.1.2. La surface d'Enneper.— La surface d'Enneper est une surface de $\mathbb{R}^3$ définie par le paramétrage suivant :

$$\left|\begin{array}{ll} x & = 3u + 3uv^2 - u^3 \\ y & = 3v + 3u^2v - v^3 \\ z & = 3u^2 - 3v^2 \end{array}\right.$$

Donner une formulation implicite de de cette surface.

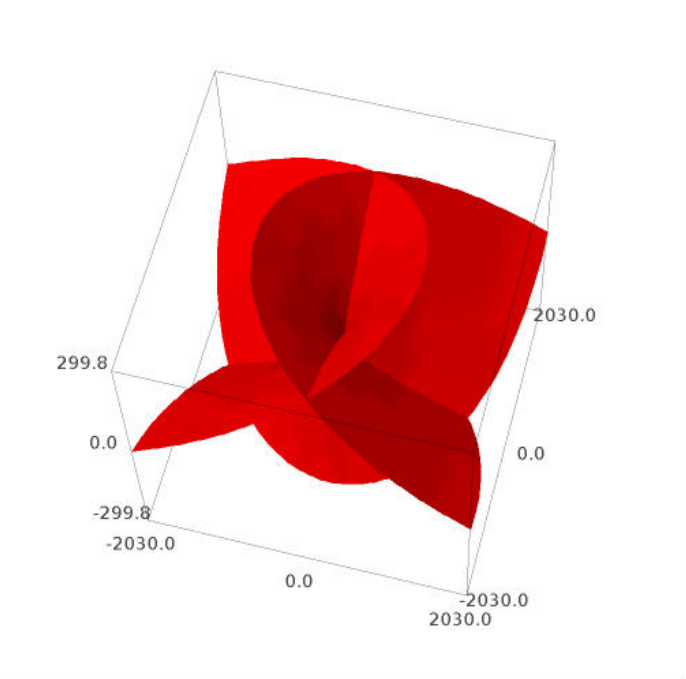


FIGURE VIII.1.: Surface d'Enneper.

§ 2 Recherche de points singuliers

VIII.2.1. Points singuliers.— Soit f un polynôme de $\mathbb{K}[x,y]$ et soit $\mathscr{C} = \mathbf{V}(f)$ la courbe de $\mathbb{K}^2$ définie par f, *i.e.*, $\mathscr{C}$ est formée de l'ensemble des points (x,y) de $\mathbb{K}^2$ vérifiant

$$f(x,y) = 0.$$

Rappelons que le gradient de la fonction f est le vecteur défini par

$$\mathrm{grad}(f) = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right).$$

Un point (a,b) de $\mathscr{C}$ est dit *singulier* si $\mathrm{grad}(f)(a,b) = 0$. Sinon, lorsque $\mathrm{grad}(f)(a,b)$ est non nul, on dit que le point (a,b) est *régulier*.

VIII.2.2. Tangente à une courbe.— Étant donné un point (a,b) de la courbe $\mathscr{C}$, une droite D passant par (a,b) est définie paramétriquement par

$$\left|\begin{array}{ll} x & = a + ct \\ y & = b + dt \end{array}\right.$$

La droite passe par le point (a,b) pour $t=0$ et le vecteur (c,d) est parallèle à la droite D. L'ensemble des droites passant par (a,b) est obtenu en faisant varier le vecteur (c,d). Posons

$$g(t) = f(a+ct, b+dt).$$

Comme $(a,b) \in \mathscr{C}$, 0 est une racine du polynôme g. On a

$$g'(t) = \frac{\partial f}{\partial x}(a+ct,b+dt).c + \frac{\partial f}{\partial y}(a+ct,b+dt).d.$$

d'où

$$g'(0) = \frac{\partial f}{\partial x}(a,b).c + \frac{\partial f}{\partial y}(a,b).d.$$

Si $\text{grad}(f)(a,b) = 0$, alors $g'(0) = 0$. Si $\text{grad}(f)(a,b)$ est non nul, on a alors $g'(0) = 0$ si, et seulement si,

$$\frac{\partial f}{\partial x}(a,b).c + \frac{\partial f}{\partial y}(a,b).d = 0.$$

Lorsque (a,b) est un point régulier de $\mathscr{C}$, la courbe $\mathscr{C}$ admet une tangente en (a,b) ; c'est la droite affine passant par (a,b) et dirigée par le vecteur (c,d), orthogonal au vecteur $\text{grad}(f)(a,b)$.

VIII.2.3. Calcul des points singuliers.— Un point singulier (a,b) de $\mathscr{C}$ vérifie

$$\frac{\partial f}{\partial x}(a,b) = 0 \quad \text{et} \quad \frac{\partial f}{\partial y}(a,b) = 0,$$

de plus, comme c'est une point de la courbe, on a

$$f(a,b) = 0.$$

Les points singuliers de $\mathscr{C}$ sont ainsi les solutions du système d'équations polynomiales

$$\left| \begin{array}{rl} f & = 0 \\ \frac{\partial f}{\partial x} & = 0 \\ \frac{\partial f}{\partial y} & = 0 \end{array} \right.$$

VIII.2.4. Exemple.— Considérons la cubique cuspidale $\mathscr{C} = \mathbf{V}(y^2 - x^3)$

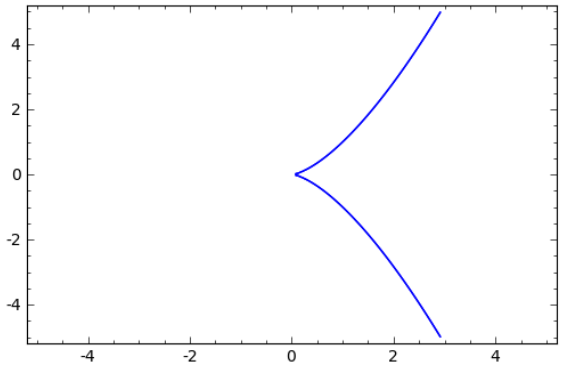


FIGURE VIII.2.: Cubique cuspidale $y^2 = x^3$.

Les points singuliers de $\mathscr{C}$ sont les solutions du système :

$$\left|\begin{array}{rl} y^2-x^3 & =0 \\ -3x^2 & =0 \\ 2y & =0 \end{array}\right.$$

Il est immédiat que la courbe $\mathscr{C}$ n'admet qu'un seul point singulier, le point $(0,0)$.

Exercice 114. —

1. Tracer la courbe de $\mathbb{R}^2$ définie par l'équation

$$y^2 = x^2(1+x).$$

2. Déterminer l'ensemble de ses points singuliers.

Exercice 115. —

1. On considère la courbe de $\mathbb{R}^2$ définie par

$$y^2 = cx^2 - x^3,$$

où c est une constante réelle. Faire un tracé de cette courbe pour $c = 2$. Déterminer l'ensemble des points singuliers de cette courbe.

2. Montrer que le cercle

$$x^2 + y^2 = a^2,$$

ne possède pas de point singulier.

Exercice 116. — L'astroïde est la courbe de $\mathbb{R}^2$ d'équation

$$(x^2+y^2-1)^3 + 27x^2y^2 = 0.$$

Faire un tracé de l'astroïde, puis calculer l'ensemble de ses points singuliers.

Exercice 117. — Tracer, puis calculer les points singuliers de la *sextique de Cayley*, d'équation

$$4(x^2+y^2-x)^3 = 27(x^2+y^2)^2.$$

§ 3 Calcul de l'enveloppe d'une famille de courbes

VIII.3.1. Famille de courbes.— Soit F un polynôme de $\mathbb{R}[x,y,t]$. Un réel t étant fixé, on notera $\mathbf{V}(F_t)$ l'ensemble algébrique affine de $\mathbb{R}^2$ défini par les solutions de l'équation

$$F(x,y,t) = 0.$$

On appelle *famille de courbes* engendrée par F l'ensemble des $\mathbf{V}(F_t)$, lorsque t parcourt $\mathbb{R}$.

VIII.3.2. Exemple.— Soit $F = (x-t)^2 + (y-t^2)^2 - 4$. Pour $t \in \mathbb{R}$ fixé, F défini un cercle de $\mathbb{R}^2$ d'équation

$$(x-t)^2 + (y-t^2)^2 = 4.$$

Voici un tracé de quelques cercles de cette famille :

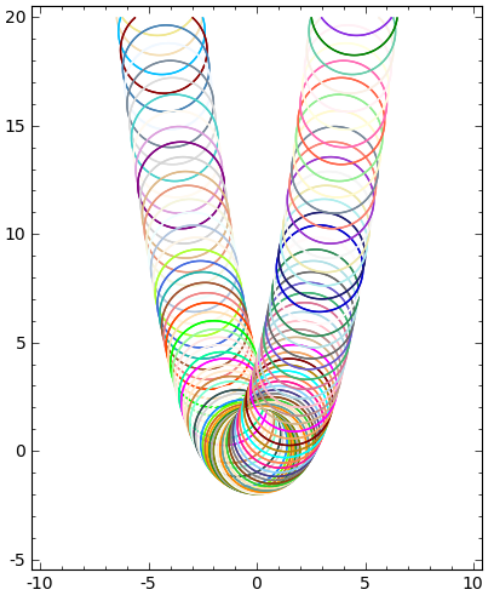


FIGURE VIII.3.: Famille de cercles.

Exercice 118. — On considère la parabole de $\mathbb{R}^2$ défini par

$$(x-t)^2 - y + t = 0,$$

où t est un paramètre réel. Tracer une famille de telles paraboles.

VIII.3.3. Enveloppe de courbes.— Soit $\mathbf{V}(F_t)$ une famille de courbes dans $\mathbb{R}^2$. L'*enveloppe* de la famille $\mathbf{V}(F_t)$ peut se décrire intuitivement comme la courbe qui est tangente à toutes les courbes de la famille. La discussion sur cette notion géométrique dépasse le cadre de ce cours. Formellement, on définira l'enveloppe de la famille $\mathbf{V}(F_t)$ comme l'ensemble des points (x,y) de $\mathbb{R}^2$ vérifiant, pour tout réel t, les équations suivantes

$$\left| \begin{array}{rl} F(x,y,t) & = 0 \\ \frac{\partial F}{\partial t}(x,y,t) & = 0 \end{array} \right.$$

VIII.3.4. Exemple.— Reprenons l'exemple VIII.3.2. Si $F = (x-t)^2 + (y-t^2)^2 - 4$, l'enveloppe de la famille $\mathbf{V}(F_t)$ est définie par les équations

$$\left| \begin{array}{rl} (x-t)^2 + (y-t^2)^2 - 4 & = 0 \\ 4t^3 - 4ty + 2t - 2x & = 0 \end{array} \right.$$

On calcule une base de Gröbner de l'idéal $I = \left\langle F, \frac{\partial F}{\partial t} \right\rangle$, avec l'ordre lexicographique induit par $y < x < t$. On obtient $G = \{g_1, g_2, g_3, g_4, g_5\}$, avec

$$\begin{aligned}
g_1 &= t^2 + \frac{32}{135}txy^2 + \frac{8}{27}txy + \frac{26}{135}tx - \frac{16}{135}x^4 - \frac{16}{135}x^2y^2 + \frac{8}{135}x^2y + \frac{37}{45}x^2 \\
&\quad - \frac{16}{135}y^3 + \frac{32}{135}y^2 + \frac{64}{135}y - \frac{128}{135} \\
g_2 &= tx^2 - \frac{2}{9}ty^3 + \frac{7}{6}ty^2 - \frac{3}{8}ty - \frac{697}{288}t - \frac{1}{9}x^5 - \frac{1}{9}x^3y^2 + \frac{7}{18}x^3y + \frac{29}{48}x^3 + \frac{1}{3}xy^3 \\
&\quad - \frac{1}{9}xy^2 - \frac{161}{144}xy - \frac{23}{288}x \\
g_3 &= txy^3 + \frac{3}{4}txy^2 + \frac{3}{16}txy - \frac{431}{64}tx - \frac{1}{2}x^4y + \frac{1}{4}x^4 - \frac{1}{2}x^2y^3 + \frac{1}{2}x^2y^2 + \frac{107}{32}x^2y \\
&\quad + \frac{159}{64}x^2 - \frac{1}{2}y^4 + \frac{5}{4}y^3 + \frac{183}{32}y^2 - 5y - \frac{119}{8} \\
g_4 &= ty^4 - \frac{7}{2}ty^3 - 3ty^2 - \frac{241}{32}ty + \frac{7327}{256}t + \frac{1}{2}x^5y + \frac{7}{8}x^5 + \frac{1}{2}x^3y^3 - \frac{7}{8}x^3y^2 - \frac{185}{32}x^3y \\
&\quad - \frac{1473}{128}x^3 - \frac{3}{2}xy^4 - \frac{17}{8}xy^3 - \frac{99}{32}xy^2 + \frac{1461}{128}xy + \frac{6929}{256}x \\
g_5 &= x^6 + x^4y^2 - \frac{5}{2}x^4y - \frac{191}{16}x^4 - 2x^2y^3 - 6x^2y^2 + \frac{15}{8}x^2y + 43x^2 + y^4 - \frac{17}{2}y^3 + \frac{225}{16}y^2 + 34y - \frac{289}{4}.
\end{aligned}$$

D'après le théorème d'élimination, le premier idéal d'élimination $I \cap \mathbb{R}[x,y]$ est engendré par le polynôme g_5. Par suite, l'enveloppe est contenue dans l'ensemble algébrique affine $\mathbf{V}(g_5)$.

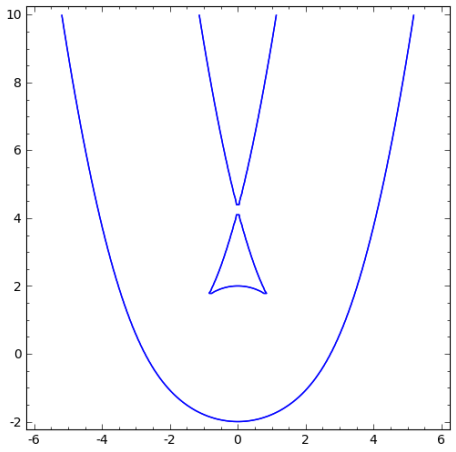


FIGURE VIII.4.: Enveloppe de la famille $(x-t)^2 + (y-t^2)^2 = 4$.

Exercice 119. — Calculer l'enveloppe de la famille de parabole de l'exercice 118.

Exercice 120. — Pour les familles de courbes suivantes, faire un tracé de quelques éléments de la famille, calculer l'enveloppe de la famille, puis tracer cette enveloppe.

1. $(x-t)^2 + y^2 = \frac{1}{2}t^2$, $t \in \mathbb{R}$,
2. $(x-t)^2 + (y-t^2)^2 = t^2$, $t \in \mathbb{R}$.

VIII.3.5. Remarque.— Notre définition sur les enveloppes reste bien intuitive. En effet, considérons la famille $\mathscr{C}$ composée des cercles de rayon 1 et dont le centre se trouve sur l'axe des abscisses x.

Exercice 121. — Déterminer l'enveloppe de la famille $\mathscr{C}$.

Exercice 122. —

1. Déterminer l'enveloppe de la famille de courbes définie par l'équation

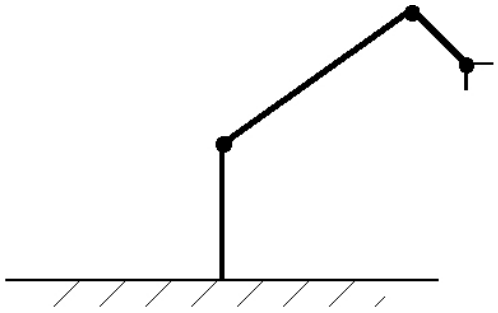
$$(x-t^3)^2+y^2=1.$$

2. Tracer cette enveloppe et comparer avec le résultat de l'exercice précédent.

§ 4 Une application en robotique

L'objectif est d'étudier les configurations géométriques d'un bras robotisé. Pour cette étude, nous allons faire quelques hypothèses simplificatrices sur les éléments constitutifs du bras. Même en considérant une version idéalisée, il est possible de présenter cette problématique importante en robotique.

On s'intéresse au problème de la réalisation des mouvements et de la description de l'espace des mouvements possibles d'un bras robotisé de la forme

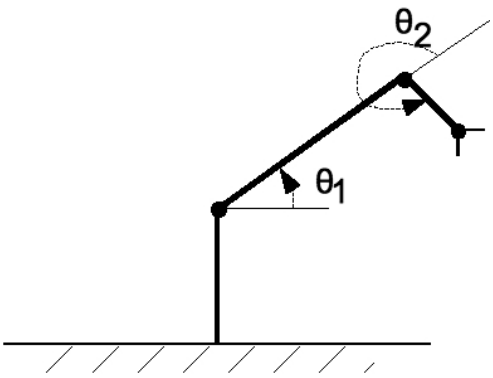


VIII.4.1. Modélisation géométrique d'un robot.— On considère des robots planaires, dont l'évolution est dans le plan, ou spatiaux, dont l'évolution est dans l'espace. Les bras robotisés que nous considérons possèdent deux extrémités :

- la première est fixée au socle et supporte le bras du robot ;
- l'autre extrémité est la partie terminale, appelé *main*, qui réalise la tâche du robot : perçage, vissage, peinture, ...

Un robot est ainsi vu comme une réunion de segments et de joints ; on considère des joints de deux types :

- les *rotules* qui permettent de faire une rotation d'un segment relativement à un autre (dans le cas planaire, on suppose que les mouvements se déroulent dans un même plan). La rotation entre deux segments est repérée par son angle θ, ainsi l'ensemble des positions d'une rotule est paramétré par S^1 ;



– les *joints prismatiques* qui permettent de réaliser une translation à partir d'un segment via un bras télescopique. La position d'un tel joint est paramétrée par un intervalle de $\mathbb{R}$.

L'ensemble des positions des joints d'un bras composé de r rotules et de p joints prismatiques est paramétré par

$$J = S^1 \times \ldots \times S^1 \times I_1 \times \ldots \times I_p,$$

avec r produits S^1 et où I_k est l'ensemble des positions du k-ème joint prismatique. L'ensemble J est appelé l'*espace des joints* du robot.

On repère la main du robot, à un instant donné, par un point (x_1, x_2) de $\mathbb{R}^2$. Ainsi l'ensemble des positions de la main du robot décrit une partie U de $\mathbb{R}^2$. À chaque point de U, on peut associer un vecteur unité u décrivant l'orientation de la main. En notant V l'ensemble des vecteurs unités associés à l'orientation de la main, le produit cartésien $C = U \times V$ est appelé l'*espace de configuration* de la main du robot. Ainsi, on peut déterminer toutes les positions de la main du robot à l'aide d'une application

$$f : J \longrightarrow C$$

reliant la position de la main avec celle de l'ensemble des joints.

On peut alors formuler deux problèmes classiques en robotique :
– ***problème du mouvement avant :*** peut-on donner une description explicite de f ?
– ***problème cinématique inverse :*** si $c \in C$, peut-on décrire $f^{-1}(c)$?

VIII.4.2. Le problème du mouvement avant (cas planaire).— On considère que le premier segment du bras du robot est fixé à un socle. Soit (x_1, y_1) les coordonnées du premier joint du bras. On associe au joint i un système de coordonnées $\beta_{i+1} = (x_{i+1}, y_{i+1})$
– dont l'origine est placée au joint i,
– l'axe positif des x_{i+1} est situé dans le prolongement du segment $i+1$,
– l'axe des y_{i+1} est normal à l'axe des x_{i+1}.

Ainsi, pour tout $i \geq 2$, les coordonnées (x_i, y_i) du joint i sont $(l_i, 0)$, où l_i est la longueur du segment i.

On veut écrire le système de coordonnées β_{i+1} en fonction de β_i. Notons θ_i l'angle entre les axes x_i et x_{i+1} (mesuré dans le sens trigonométrique usuel). Soit q un point de $\mathbb{R}^2$, on note

$$[q]_{\beta_{i+1}} = \begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix}, \quad [q]_{\beta_i} = \begin{bmatrix} a_i \\ b_i \end{bmatrix}$$

ses coordonnées dans les systèmes β_{i+1} et β_i respectivement. On a

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix} \begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} + \begin{bmatrix} l_i \\ 0 \end{bmatrix}.$$

En utilisant une représentation affine du plan dans $\mathbb{R}^3$, on a

$$\begin{bmatrix} a_i \\ b_i \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i & l_i \\ \sin\theta_i & \cos\theta_i & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{bmatrix}.$$

En posant

$$\mathbf{A}_i = \begin{bmatrix} \cos\theta_i & -\sin\theta_i & l_i \\ \sin\theta_i & \cos\theta_i & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

on a ainsi

$$\begin{bmatrix} a_i \\ b_i \\ 1 \end{bmatrix} = \mathbf{A}_i \begin{bmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{bmatrix}.$$

Pour un robot formé de k rotules, on aura

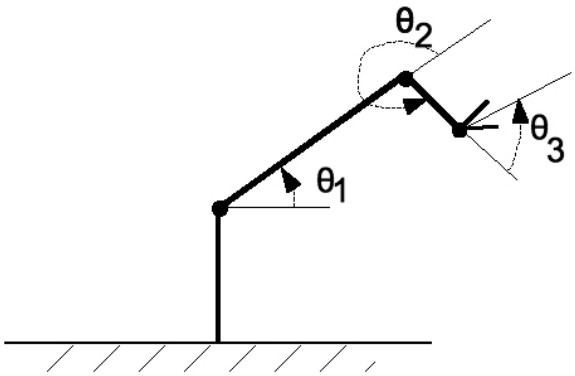
$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \mathbf{A}_1\mathbf{A}_2\ldots\mathbf{A}_k \begin{bmatrix} x_{k+1} \\ y_{k+1} \\ 1 \end{bmatrix},$$

où $\beta_1 = (x_1, y_1)$ est le système de coordonnées initial.

Comme la main est attachée au dernier joint, on obtient les coordonnées de la main dans le sytème β_1 en posant $x_k = y_k = 0$, d'où

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \mathbf{A}_1\mathbf{A}_2\ldots\mathbf{A}_k \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

VIII.4.3. Exemple.— On considère un bras avec trois rotules :



On a

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta_1 & -\sin\theta_1 & 0 \\ \sin\theta_1 & \cos\theta_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_2 \\ y_2 \\ 1 \end{bmatrix}.$$

Ici l'origine de $\beta_2 = (x_2, y_2)$ est placée au premier joint. On a

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta_1 & -\sin\theta_1 & 0 \\ \sin\theta_1 & \cos\theta_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\theta_2 & -\sin\theta_2 & l_2 \\ \sin\theta_2 & \cos\theta_2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\theta_3 & -\sin\theta_3 & l_3 \\ \sin\theta_3 & \cos\theta_3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_4 \\ y_4 \\ 1 \end{bmatrix}.$$

Soit

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos(\theta_1+\theta_2+\theta_3) & -\sin(\theta_1+\theta_2+\theta_3) & l_3\cos(\theta_1+\theta_2)+l_2\cos(\theta_1) \\ \sin(\theta_1+\theta_2+\theta_3) & \cos(\theta_1+\theta_2+\theta_3) & l_3\sin(\theta_1+\theta_2)+l_2\sin(\theta_1) \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_4 \\ y_4 \\ 1 \end{bmatrix}.$$

Les coordonnées (x_4, y_4) de la main sont $(0,0)$ dans le système de coordonnées du dernier joint, on a donc

$$\begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} l_3\cos(\theta_1+\theta_2)+l_2\cos(\theta_1) \\ l_3\sin(\theta_1+\theta_2)+l_2\sin(\theta_1) \\ 1 \end{bmatrix}$$

VIII.4.4. Problème cinématique inverse (cas planaire).— Étant donné une position (a,b) de $\mathbb{R}^2$ et une orientation, on souhaite déterminer s'il est possible ou non de placer la main du robot à cette position et dans cette orientation. On peut procéder de la façon suivante.

Posons $c_i = \cos(\theta_i)$ et $s_i = \sin(\theta_i)$. On a la condition $c_i^2 + s_i^2 = 1$. On peut alors écrire l'image de $f : J \longrightarrow C$ comme une fonction polynomiale

$$f = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix},$$

où f_1 et f_2 sont des polynômes en c_i et s_i, et f_3 un polynôme en θ_i, pour $i \in [\![1,n]\!]$. Le problème revient alors à chercher les solutions du système d'équations polynomiales :

$$\left|\begin{array}{rl} f(c_1,\ldots,c_n,s_1,\ldots,s_n,l_1,\ldots,l_n) &= a \\ g(c_1,\ldots,c_n,s_1,\ldots,s_n,l_1,\ldots,l_n) &= b \\ c_1^2+s_1^2 &= 1, \\ \vdots & \\ c_n^2+s_n^2 &= 1. \end{array}\right.$$

On calcule pour cela une base de Gröbner du système relativement à l'ordre lexicographique induit par l'ordre alphabétique suivant :

$$s_1 < c_1 < \ldots < s_n < c_n.$$

Les réels $a, b, l_1, \ldots, l_n$ sont des paramètres du système, on calcule la base de Gröbner dans l'anneau $\mathbb{R}(a,b,l_1,\ldots,l_n)[c_1,\ldots,c_n,s_1,\ldots,s_n]$. En pratique, on fixera les l_i pour calculer les solutions du système.

VIII.4.5. Exemple.— Reprenons l'exemple VIII.4.3. En utilisant les formule trigonométrique

$$\cos(\theta_1+\theta_2) = \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 = c_1c_2 - s_1s_2,$$
$$\sin(\theta_1+\theta_2) = \sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1 = s_1c_2 + s_2c_1.$$

On a

$$f = \begin{bmatrix} l_3(c_1c_2-s_1s_2)+l_2c_1 \\ l_3(s_1c_2+s_2c_1)+l_2s_1 \\ \theta_1+\theta_2+\theta_3 \end{bmatrix}$$

Les configurations possible du robot pour que la main atteigne la position (a,b) de $\mathbb{R}^2$ sont données par les solutions du systèmes suivant

$$\left|\begin{array}{rl} l_3(c_1c_2-s_1s_2)+l_2c_1 & =a \\ l_3(s_1c_2+s_2c_1)+l_2s_1 & =b \\ c_1^2+s_1^2 & =1 \\ c_2^2+s_2^2 & =1 \end{array}\right.$$

Exercice 123. —

1. Calculer dans $\mathbb{Q}(a,b,l_2,l_3)[c_2,s_2,c_1,s_1]$ une base de Gröbner de l'idéal engendré par les équations du système précédent, pour l'ordre lexicographique induit par $s_1 < c_1 < s_2 < c_2$.
2. En déduire les solutions s_1, s_2, c_1, c_2 de ce système en fonction des paramètres a, b, l_2 et l_3.

Exercice 124. — Étudier les configurations d'un bras robotisé plan constitué de quatre rotules.

ANNEXE
A

Prise en main du système de calcul Sage

Sommaire

§ 1 Prise en main de l'environnement de calcul SAGE

L'objectif de cette annexe est de découvrir le système de calcul Sage, en particulier sa syntaxe, ses mécanismes d'affectation et d'évaluation. Dans ce cours, nous utilisons Sage pour le calcul polynomial, nous présentons ici les principales opérations de Sage pour la manipulation de polynômes.

A.1.1. Le système de calcul Sage.— Sage est un système de calcul formel et numérique dont le développement a débuté en 2005 à l'université de Washington [1]. Sage est construit au dessus de systèmes libres déjà existants tels que MAXIMA et SYMPY pour le calcul symbolique, GAP pour la théorie des groupes, PARI pour la théorie des nombres, SINGULAR pour l'algèbre commutative, SCYPY pour le calcul numérique, R pour les statistiques. Sage a pour objectif de fournir une alternative libre aux systèmes propriétaires tels que MAPLE, MAGMA, MATLAB.

Un point fort, outre la mise en commun des potentialités de tous ces systèmes, est l'utilisation, au lieu d'une multitude de langages spécifiques, d'un langage informatique universel Python [2] comme langage fédérateur. Ainsi les structures mathématiques sont implémentées dans un cadre catégorique et orienté objets avec des méthodes pour les objets structurés et des méthodes pour leurs éléments. Les classes ainsi définies sont regroupées dans des modules Python.

1. http://www.sagemath.org/
2. http://www.python.org/

Il existe plusieurs façons d'utiliser Sage : en « ligne de commande » , en écrivant des programmes interprétés ou compilés en Sage, en écrivant des scrits Python qui font appels à la bibliothèque Sage. Nous utiliserons ici Sage par l'intermédiaire d'une « interface graphique » permettant d'éditer des « feuilles de travail » .

A.1.2. Connexion au serveur Sage.— La connection au serveur Sage passe par une identification via la page à l'adresse `http://sage-math.univ-lyon1.fr`. Saisir cette url dans votre navigateur web, puis saisir votre login référérencé par l'annuaire ldap de l'UCBL. Après cette première identification, vous êtes connecté à un serveur Sage qui demande une identification : saisir le même login et le mot de passe associé. Vous accédez ainsi à une interface de gestion de « feuilles de travail » .

A.1.3. Première feuille de travail.— Pour ouvir une nouvelle feuille de travail, cliquer sur le lien New Worksheet. La feuille présente différentes fonctionnalités, en particulier :

- une zone de menus : File, Action, Data, sage, permettant de gérer la feuille de travail, en particulier une entrée du menu File permet d'enregister la feuille de travail dans un fichier (le serveur Sage de l'UCBL étant en phase expérimentale, il est conseillé d'enregistrer ses feuilles de travail à l'issue de la séance),
- trois boutons Save, Save & quit, Discard & quit, permettant d'enregistrer la feuille de travail et de quitter la feuille de travail en l'enregistrant ou non.
- des cellules pour la saisie des commandes.

Dans un premier temps, nous n'utiliserons pas les autres fonctionnalités disponibles.

A.1.4. Les cellules.— Les cellules permettent de saisir les instructions. Pour évaluer l'ensemble des instructions saisies dans une cellule, on peut cliquer sur le lien evaluate au-dessous de la cellule ou bien utiliser le racourci clavier `<MAJ><ENTREE>`.

Exercice 125. — Saisir l'expression suivante puis l'évaluer.

```
sage: 2+2
```

Il est possible d'évaluer séquentiellement toutes les cellules de la feuille de travail avec l'entrée Evaluate All du menu Action.

Pour insérer une cellule (entre deux cellules), cliquer sur la ligne bleu au-dessus ou au-dessous de la cellule ou bien faire `<CTRL><ENTREE>` au clavier. Pour supprimer une cellule, vider la cellule de son contenu puis `<DELETE>`.

A.1.5. Aide en ligne et complétion dynamique.— Une aide en ligne est disponible pour les commandes et les méthodes. Cette aide en ligne permet aussi d'obtenir une description des classes. Pour obtenir de l'aide sur une méthode ou une classe on exécute l'instruction `nomMethode?` ou `nomClasse?`.

Exercice 126. — Tester les instructions suivantes :

```
sage: cos?
sage: RationalField?
sage: PolynomialRing?
```

Pour écrire le nom d'une méthode ou d'une classe, on peut utiliser la complétion dynamique en utilisant la touche `<TAB>`.

§ 2 Variables et expressions

A.2.1. L'affectation.— Pour affecter à une *variable* une valeur, on utilise le symbole =, par exemple

```
sage: x = 2 + 2
sage: x
          4
sage: x = cos(pi/12)
sage: x
          1/12*(sqrt(3) + 3)*sqrt(6)
```

L'affectation d'une variable n'affiche pas la valeur de la variable sur la sortie standard. Tester :

```
sage: x = sqrt(2)
...   y = 3
...   y
          3

sage: y
...   print x
...   y
          sqrt(2)
          3
```

Pour un affichage plus visuel on peut utiliser la fonction `show(-)`. Saisir l'instruction suivante :

```
sage: show(x)
```

Pour afficher la valeur de variable `x` avec une approximation avec 20 chiffres décimaux :

```
sage: x.n(digits=20)
```

Il est possible de saisir des instructions sur plusieurs lignes, pour passer à la ligne, utiliser la touche <ENTRÉE> :

```
sage : x=2
...    y=x
...    print y
...    z=3 ; t = z+y ; z = z+t
...    print z
2
8
```

Pour réinitialiser les variables, on peut utiliser la méthode `reset()` :

```
sage : x=2
...    print x
...    reset()
...    print x
2
x
```

A.2.2. Expressions symboliques.— Sage permet de manipuler des expressions symboliques. La commande `var` permet de déclarer des variables symboliques.

Exercice 127. — Saisir les instructions suivantes puis les évaluer.

```
sage : var('x,y')
...    z = cos(x)^2 + sin(y)^2
...    print z
...    z = z(x=y)
...    print z
...    z.simplify_trig()
```

La méthode `subs.expr()`, ou la syntaxe `expression(variable = valeur)`, permet de substituer des valeurs dans une expression symbolique :

```
sage : var('x,y')
...    z = cos(x)^2 + sin(y)^2
...    print z.subs_expr(x==pi/2)
...    print z(y=pi/2)
```

A.2.3. Fonctions.— On peut définir des fonctions de la façon suivante :

```
sage : reset()
...    var('x,y')
...    f(x,y) = x/sin(x) + sqrt(y)
...    f
```

Dans Sage, toute expression mathématique est un objet. Un objet possède des attributs définissant sa structure et des méthodes permettant de modifier sa structure ou de communiquer avec lui. En particulier, les fonctions sont des objets :

```
sage : f.parent()
```

qui possèdent des méthodes d'accès, par exemple :

```
sage : f.show()
...    f.limit(x=0).show()
...    f.diff(x).show()
```

Pour définir une fonction avec Sage, on peut aussi utiliser la commande `def`. Par exemple, pour la fonction

$$x \longmapsto x^2$$

on peut procéder de la façon suivante :

```
sage: def carre(x):
...       return x^2
sage: carre(3)
9
sage: A = Matrix([[1,1],[1,1]])
sage: carre(A)
[2 2]
[2 2]
```

On peut définir des fonctions de plusieurs variables de la même façon. Par exemple, pour la fonction

$$(x,y) \longmapsto \cos^2(x) + \sin^2(y)$$

```
sage: def fonc(x,y):
          return cos(x)^2 + sin(y)^2
sage: fonc(pi/3,pi/2)
5/4
```

A.2.4. Remarque.— Tous les types d'objets ne possèdent pas la méthode `show()`. Tester la méthode `show()` sur une matrice :

```
sage: A = Matrix([[1,2],[3,5]])
...   A.show()
```

Tester ensuite la fonction `show(-)` :

```
sage: show(A)
```

§ 3 Les polynômes à une indéterminée

A.3.1. Anneaux de polynômes à une indéterminée.— Pour construire un anneau de polynômes, on utilise le constructeur `PolynomialRing`. L'anneau $R = A[x]$ des polynômes à une indéterminée x à coefficients dans un anneau ou corps A peut se spécifier par les expressions équivalentes suivantes :

```
R.<x> = A[],   R.<x> = PolynomialRing(A),
R = A['x'],   R = PolynomialRing(A, 'x').
```

Par exemple, on utilise `ZZ['x']`, `QQ['x']`, `RR['x']` et `Integers(n)['x']` pour construire les anneaux $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ et $\mathbb{Z}/n\mathbb{Z}[x]$.

Pour accéder à l'anneau de base A, on utilise la méthode `R.base_ring()`. On peut obtenir l'indéterminée avec la méthode `R.gen()` ou `R.0`.

A.3.2. Exemple.— Pour construire $\mathbb{Q}[x]$:

```
sage: R = PolynomialRing(QQ, 'x')
```

L'argument 'x' de `PolynomialRing` est une chaîne de caractères qui représente le nom de l'indéterminée de l'anneau ou du corps. On peut écrire aussi

```
sage: R = QQ['x']
sage: R
        Univariate Polynomial Ring in x over Rational Field
```

Pour récupérer l'indéterminée (avec le même nom) :

```
sage: x = R.gen()
```

La variable Python x représente alors le polynôme x de $\mathbb{Q}[x]$:

```
sage: x.parent()
Univariate Polynomial Ring in x over Rational Field
```

Ainsi, le polynôme x de $\mathbb{Q}[x]$ est différent du polynôme x de $\mathbb{R}[x]$ et du polynôme t de $\mathbb{Q}[t]$.

A.3.3. Construction de polynômes.— Un polynôme de $A[x]$ se définit simplement comme une expression algébrique en l'indéterminée x :

```
sage: R = QQ['x']
sage: f = 2*x^2 - 3*x +1
sage: f.parent()
        Univariate Polynomial Ring in x over Rational Field
```

Pour changer d'anneau de base de $A[x]$ en $B[x]$, on utilise la méthode `f.change_ring(B)`. Pour changer le nom de l'indéterminée, on utilise la méthode `change_variable_name` :

```
sage: g = f.change_variable_name('y')
sage: g
        2*y^2 - 3*y + 1
sage: h = g.change_ring(RR)
sage: h.parent()
        Univariate Polynomial Ring in y over Real Field with 53 bits of
            precision
```

A.3.4. Remarque.— Les instructions `R = A['x']` et `R.<x> = A[ ]` ne sont pas tout à fait équivalentes : dans le premier cas, il faut affecter l'indéterminée `R.gen()` à une variable `x` avant de construire des polynômes ; dans le second cas, ce n'est pas nécessaire.

Tester les instructions suivantes :

```
sage: reset()
      R.<x>= QQ[]
      f = 2*x^2-3*x+1
      print f.parent()
      print f
      show(f)
      f.subs(2)
```

```
sage: reset()
      R = QQ['x']
      f = 2*x^2 - 3*x +1
      print f.parent()
      print f
      show(f)
      f.subs(2)
```

```
sage: reset()
      y = R.gen()
      g = 2*y^2-3*y+1
      print g.parent()
      print g
      show(g)
      g.subs(2)
```

A.3.5. Opérations d'accès sur les polynômes d'une seule indéterminée.— Les principales opérations d'accès permettent d'obtenir

- l'indéterminée x : `f.variable_name()`,
- le coefficient de x^k : `f[k]`,
- le coefficient dominant : `f.leading_coefficient()`,
- le degré : `f.degree()`,
- la liste des coefficients : `f.coeffs()`,
- la liste des coefficients non nuls : `f.coefficients()`.

A.3.6. Opérations arithmétiques élémentaires.— Les opérations arithmétiques élémentaires s'écrivent naturellement : l'addition `f + g`, la soustraction `f - g`, la multiplication `f * g` et la puissance `f^k`.

Il existe plusieurs syntaxes pour la substitution dans un polynôme `f` de l'indéterminée par une valeur a. On peut utiliser `f(a)` ou la méthode `subs` : `f.subs(a)`. Par exemple :

```
sage: reset()
      R.<x>= QQ[]
sage: f = x^2 + 3*x +1
sage: f(sqrt(3))
        (sqrt(3) + 3)*sqrt(3) + 1
sage: f(sqrt(3)).expand()
    3*sqrt(3)+4
sage: A = Matrix([[0,1],[1,0]])
sage: f(A)
        [2 3]
        [3 2]
```

Pour calculer la dérivée d'un polynôme, on a la méthode `f.derivative()` ou `diff(f)`. La méthode `random_element()` génère un polynôme au hasard.

```
sage: f = R.random_element(degree=6)
sage: f
                2*x^6 + 11*x^5 + 1/4*x^3 + 1/3*x^2 + 2*x - 2
sage: f.subs(x^3)
        2*x^18 + 11*x^15 + 1/4*x^9 + 1/3*x^6 + 2*x^3 - 2
sage: f.subs(2)
        1456/3
sage: f.derivative()
        12*x^5 + 55*x^4 + 3/4*x^2 + 2/3*x + 2
```

A.3.8. Arithmétique euclidienne.— L'anneau $\mathbb{K}[x]$ étant euclidien, les méthodes de division sont simples :

- le test de divisibilité de f par g : `g.divides(f)`,
- pour obtenir la multiplicité d'un diviseur g de f : `k = f.valuation(g)`,
- pour calculer la division euclidienne dans $\mathbb{K}[x]$, où $\mathbb{K}$ est un corps, $f = qg + r$:

```
sage: q, r = f.quo_rem(g)
sage: q = f//g
sage: r = f%g
```

- pour calculer le plus grand commun diviseur (pgcd) de polynômes de $\mathbb{K}[x]$, où $\mathbb{K}$ est un corps, on utilise la méthode `gcd` : `f.gcd(g)`, `gcd([f1, f2, f3])` :

```
sage: reset()
      R.<x> = QQ[]
sage: f = 15*(x^12 - 3*x^5)*(x^2 -1)
sage: f.gcd(f.derivative())
      x^4
```

- pour calculer le plus petit commun multiple : `p.lcm(q)`, `lcm([p1, p2, p3])` :

```
sage: f = x^5 -1
sage: g = x + 1
sage: f.lcm(g)
      x^6 + x^5 - x - 1
```

– la méthode `xgcd` permet de calculer une relation de Bézout :

$$g = \text{pgcd}(f_1, f_2) = u_1 f_1 + u_2 f_2, \quad \text{où} \quad g, u_1, u_2, f_1, f_2 \in \mathbb{K}[x].$$

La syntaxe est la suivante `g, u1, u2 = f1.xgcd(f2)` ou `xgcd(f1, f2)`. Par exemple,

```
sage: f1 = x^7 - 1
sage: f2 = x^3 - 1
sage: f1.xgcd(f2)
```

Exercice 128. — On considère les polynômes

$$f_1 = x^7 - 3x^5 + 2x^4 - x^2 + 1, \quad f_2 = x^8 + 2x^6 - 3x^3 - x + 5.$$

1. Déterminer le degré, le coefficient dominant et la liste des coefficients du produit $f_1 f_2$.
2. Calculer la division euclidienne de f_2 par f_1.
3. Calculer le pgcd de f_1 et f_2.
4. Calculer $f_1(1)$.

A.3.9. Racines d'un polynôme.— Il existe plusieurs méthodes pour calculer les racines d'un polynôme. La méthode `roots` d'un polynôme retourne les racines du polynôme dans son anneau de base, sous la forme d'une liste de couples (racine, multiplicité) :

```
sage: reset()
      R.<x> = QQ[]
sage: f = (x-1)*(x^2-1)*(x^2+1)*(x^2 - 5)
sage: f.roots(QQ)
     [(-1, 1), (1, 2)]
```

Il est possible de spécifier le domaine, par exemple pour obtenir les racines réelles, puis les racines complexes :

```
sage: f.roots(RR)
     [(-2.23606797749979, 1), (-1.00000000000000, 1),
       (1.00000000000000, 2), (2.23606797749979, 1)]
sage: f.roots(CC)
     [(-2.23606797749979, 1), (-1.00000000000000, 1),
      (1.00000000000000, 2), (2.23606797749979, 1),
      (-5.44339946922833e-36 - 1.00000000000000*I, 1),
      (-5.44339946922833e-36 + 1.00000000000000*I, 1)]
```

A.3.10. Idéaux de $A[x]$.— Les idéaux d'anneaux de polynômes sont des objets construits à partir de la méthode `ideal` :

```
sage: reset()
      R.<x> = QQ[]
      I = R.ideal(x^2 + 1)
sage: I
        Principal ideal (x^2 + 1) of Univariate Polynomial Ring in x over
        Rational Field
```

ou bien avec la syntaxe suivante, pour construire l'idéal I de $\mathbb{Q}[x]$ engendré par les deux polynômes $f_1 = x^2 - 1$ et $f_2 = x^3 - x^2 + x - 1$:

```
sage: I = (x^2 - 1, x^3 - x^2 + x - 1)*R
sage: I
        Principal ideal (x - 1) of Univariate Polynomial Ring in x
        over Rational Field
```

Pour réduire un polynôme modulo un idéal :

```
sage: I = R.ideal((x^2 - 1)*(x+1))
sage: g = I.reduce(x^4 + 1) ; g
        2*x^2
```

Exercice 129. — Soit I l'idéal de $\mathbb{Q}[x]$ engendré par les polynômes

$$f_1 = x^6 - 1, \quad f_2 = x^4 + 2x^3 + 2x^2 - 2x - 3.$$

1. Déterminer un générateur g de I tel que $I = \langle g \rangle$.
2. Montrer que le polynôme $f = x^4 + 2x^2 - 3$ est dans I.
3. Décomposer f en une combinaison algébrique de f_1 et f_2.

§ 4 Polynômes à plusieurs indéterminées

Sage permet de calculer avec les polynômes à plusieurs indéterminées. La différence fondamentale avec le cas à une seule indéterminée est que l'anneau $\mathbb{K}[x_1, \ldots, x_n]$ n'est pas principal, cf. exercice 59 du chapitre III. Pour l'arithmétique euclidienne dans ces anneaux, les bases de Gröbner sont alors un outils précieux.

A.4.1. Anneaux de polynômes à plusieurs indéterminées.— Pour construire l'anneau des polynômes à plusieurs indéterminées, on utilise le constructeur `PolynomialRing`. Pour construire l'anneau $A[x,y]$, on utilise `PolynomialRing(A, 'x,y')` ou `A['x,y']`. Par exemple, pour l'anneau $\mathbb{Q}[x,y,z]$:

```
sage: R = PolynomialRing(QQ, 'x,y,z')
sage: x, y, z = R.gens()
```

On peut aussi utiliser la syntaxe équivalente : `R.<x,y,z> = QQ[]`.

A.4.2. Construction d'anneaux de polynômes.— Il est possible de construire des indéterminées d'un même nom indicé par des entiers naturels, comme par exemple $x_0, x_1, \ldots, x_n$ ou $y_0, y_1, \ldots, y_k$. Pour construire l'anneau $A[x_0, \ldots, x_{n-1}]$, on utilise le constructeur `PolynomialRing(A, 'x', n)`.

Par exemple pour construire l'anneau $\mathbb{Q}[x_0, x_1, x_2, x_3, x_4, x_5]$:

```
sage: R = PolynomialRing(QQ, 'x', 5)
sage: x = R.gens()
sage: sum(x[i] for i in xrange(5))
        x0 + x1 + x2 + x3 + x4
```

La méthode `R.gens()` retourne le n-uplet des indéterminées. On peut aussi obtenir le 1er, 2e, ... générateur avec `R.0`, `R.1`, ...

Pour l'évaluation, il faut donner une valeur à chacune des indéterminées ou préciser les indéterminées à substituer :

```
sage: R.<x,y,z> = QQ[]
sage: f = 2*x^2*y*z^2 + 3*x*y^2*z - 4*z^2
sage: f(1,0,2)
        -16
sage: g = f.subs(x=1, z=y^2-1) ; g
        2*y^5 - y^4 - 4*y^3 + 5*y^2 + 2*y - 4
sage: g.parent()
        Multivariate Polynomial Ring in x, y, z over Rational Field
```

Avec le constructeur `PolynomialRing`, on peut spécifier un ordre monomial sur un anneau de polynômes à plusieurs indéterminées :

```
sage: R.<x,y,z> = PolynomialRing(QQ, 'x,y,z', order='lex')
sage: x > y^2
        True
sage: x^2 *y* z > x * y
        True
sage: x^2 *y* z > x^3 * y
        False
```

Dans cet exemple, on a spécifié l'ordre lexicographique, `lex`, induit par $z < y < x$. On peut spécifier l'ordre lexicographique "inverse", `invlex`, induit par $x < y < z$.

```
sage: R.<x,y,z> = PolynomialRing(QQ, 'x,y,z', order='invlex')
sage: x * y > z
        False
sage: x^2 *y* z > x * y
        True
sage: x^2 *y* z > x^3 * y
        True
```

Il existe également l'ordre lexicographique gradué, `deglex` (voir définition à la partie III.4.9).

```
sage: R.<x,y,z> = PolynomialRing(QQ, 'x,y,z', order='deglex')
sage: z^3 > x^2
        True
sage: x^2 *y* z > x * y * z^2
        True
sage: x^2 *y* z > x^3 * y
        False
```

L'ordre spécifié par défaut est l'ordre `degrevlex` :

```
sage: R.<x,y,z> = QQ[]
sage: R.term_order()
        Degree reverse lexicographic term order
```

La définition de cet ordre se trouve sur la page `http://www.sagemath.org/doc/reference/sage/rings/polynomial/term_order.html`.

A.4.3. Méthodes d'accès.— Les principales opérations d'accès permettent d'obtenir

- le support : `f.exponents()`,
- les coefficients non nuls `f.coefficients()`,
- le degré total : `f.degree()`,
- le degré en x : `f.degree(x)`,
- le terme dominant : `f.lt()`,
- le coefficient dominant : `f.lc()`,
- le monôme dominant : `f.lm()`.

```
sage: R.<x,y,z> = QQ[]
sage: f = 2*x^2*y*z^2 + 3*x*y^2*z - 4*z^2
sage: print f.degree() , f.degree(x)
        5 2
```

On peut utiliser l'opérateur crochet `[ ]` pour extraire des coefficients, il accepte comme paramètre un monôme ou son *exposant* :

```
sage: f[2,1,2] , f[1,2,1], f[0,0,2]
        (2, 3, -4)
sage: f[x^2*y*z^2]
        2
```

Exercice 130. — Soit $f = 5x^2y^3z^2 + 3xy^2z + 4z^2 - 2xy + zy + z$ un polynôme de $\mathbb{Q}[x,y,z]$.

1. Avec Sage, donner le terme dominant, le coefficient dominant et le monôme dominant de f pour l'ordre lexicographique et pour l'ordre lexicographique gradué.
2. Donner le degré total de f,
3. Écrire f comme un polynôme en x.

A.4.4. Opérations arithmétiques sur le polynômes.— Pour les polynômes à plusieurs indéterminées, les opérations arithmétiques +, -, * s'utilisent comme dans le cas d'une seule indéterminée. Comme $\mathbb{K}[x_1,\ldots,x_n]$ n'est pas principal, les méthodes basées sur la division euclidienne des polynômes ne fonctionnent pas dans ce cas. En particulier, il ne faut pas utiliser les commandes `f//g` et `f%g` qui ne tiennent pas compte de l'ordre monomial spécifié. Pour obtenir le reste de la division de f par g suivant l'ordre monomial spécifié, vous pouvez utiliser la méthode `f.mod(g)`.

Exercice 131. — Soient $f = x^3y^3 + 2y^2$, $f_1 = 2xy^2 + 3x + 4y^2$ et $f_2 = y^2 - 2y - 2$ des polynômes de $\mathbb{Q}[x,y]$. En utilisant l'ordre lexicographique induit par $y < x$, calculer le reste de la division de f par f_1 puis par f_2. Calculer ensuite le reste de la division de f par f_2, puis f_1.

Exercice 132. — Soit $f = x^2y^2 - w^2$, $f_1 = x - y^2w$, $f_2 = y - zw$, $f_3 = z - w^3$ et $f_4 = w^3 - w$ des polynômes de $\mathbb{Q}[x,y,z,w]$. En utilisant l'ordre lexicographique induit par $w < z < y < x$, calculer le reste de la division de f par f_1, f_2, f_3, f_4 dans cet ordre. Faire le même calcul avec l'ordre f_4, f_3, f_2, f_1. Faire les mêmes calculs avec $f = x^2y^2 + w^3$.

A.4.5. Calcul de bases de Gröbner.— La méthode `I.groebner_basis()` retourne une base de Gröbner réduite de l'idéal I. Une base est de Gröbner G d'un idéal I est dite *réduite* si

i) $\mathrm{lc}(g) = 1$, pour tout $g \in G$,

ii) pour tout $g \in G$, aucun monôme de p est dans l'idéal $\langle \mathrm{lt}(G - \{g\})\rangle$.

On peut montrer, un ordre monomial étant fixé, que tout idéal non nul possède une unique base de Gröbner réduite.

```
sage: R.<x,y,z> = PolynomialRing(RationalField(), 3, order='deglex')
sage: f1 = x*y-y^2
sage: f2 = x^2-z^2
sage: I = (f1, f2)*R
sage: G = I.groebner_basis()
sage: print G
        [y^3 - y*z^2, x^2 - z^2, x*y - y^2]
```

Avec l'argument `toy:buchberger`, la base de l'idéal est complétée en une base de Gröbner sans être réduite :

```
sage: R.<x,y,z> = PolynomialRing(RationalField(), 3, order='deglex')
sage: f1 = x^2 + y^2 - 1
sage: f2 = x^2 + z^2 - 1
sage: I = (f1, f2)*R
sage: G = I.groebner_basis()
sage: H = I.groebner_basis('toy:buchberger')
sage : print G
        [x^2 + z^2 - 1, y^2 - z^2]
sage: print H
        [x^2 + y^2 - 1, x^2 + z^2 - 1, y^2 - z^2]
```

Exercice 133. — Pour les idéaux suivants, construire une base de Gröbner en utilisant l'ordre lexicographique, puis l'ordre lexicographique gradué.

1. $I = \langle x^2y - 1, xy^2 - x \rangle$,
2. $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3 \rangle$,
3. $I = \langle x - z^4, y - z^5 \rangle$.

Exercice 134. — Montrer que les polynômes f_1 et f_2 de l'exercice 131 ne forment pas une base de Gröbner de l'idéal qu'ils engendrent pour l'ordre lexicographique induit par $y < x$.

Exercice 135. — Montrer que les polynômes f_1, f_2, f_3, f_4 de l'exercice 132 ne forment pas une base de Gröbner de l'idéal qu'ils engendrent pour l'ordre lexicographique induit par $z < y < x < w$. Existe-t-il un ordre lexicographique pour lequel cette famille forme une base de Gröbner ?

Exercice 136. — Calculer les S-polynômes des couples (f_1, f_2) de polynômes de $\mathbb{Q}[x,y,z]$ suivants avec l'ordre lexicographique et l'ordre lexicographique gradué induits par $z < y < x$:

1. $f_1 = 3x^2yz - y^3z^3$, $f_2 = xy^2 + z^2$,
2. $f_1 = 3x^2yz - xy^3$, $f_2 = xy^2 + z^2$,
3. $f_1 = 3x^2y - yz$, $f_2 = xy^2 + z^4$.

A.4.6. Problème de l'appartenance à un idéal.—

Exercice 137. — Soit I l'idéal de $\mathbb{Q}[x,y,z]$ défini par

$$I = \langle y - x^3, x^2y - z \rangle .$$

1. Calculer une base de Gröbner de I pour l'ordre lexicographique induit par $z < y < x$.
2. Le polynôme $f = xy^3 - z^2 + y^5 - z^3$ appartient-il à I ?

Exercice 138. — Les polynôme $x^3 + 1$ et $x^3 - 1$ s'écrivent-ils comme combinaison algébrique des polynômes $x + y + z$, $xy + yz + zx$ et $xyz - 1$?

Exercice 139. — On considère dans $\mathbb{Q}[x,y,z]$ les idéaux

$$I = \langle x^2 + z, xy + y^2 + z, xz - y^3 - 2yz, y^4 + 3y^2z + z^2 \rangle ,$$
$$J = \langle x^2 + z, xy + y^2 + z, x^3 - yz \rangle .$$

A-t-on $I \subset J$, $J \subset I$ ou $I = J$?

A.4.7. Résolution de systèmes d'équations polynomiales.—

Exercice 140. — Soit $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x,y]$ engendré par les polynômes

$$\begin{aligned} f_1 &= x^2 + 2y^2 - 1, \\ f_2 &= x^2 + xy + y^2 - 1. \end{aligned}$$

1. Déterminer une famille de générateurs de l'idéal $I \cap \mathbb{R}[x]$ et de l'idéal $I \cap \mathbb{R}[y]$.
2. Déterminer les solutions du système d'équations suivant

$$\left| \begin{array}{ll} f_1(x,y) & = 0, \\ f_2(x,y) & = 0. \end{array} \right.$$

Exercice 141. — Pour $a = 1,2,3$, déterminer toutes les solutions dans $\mathbb{Q}$ du système

$$\left| \begin{array}{rl} x^2 + 2y^2 & = a, \\ x^2 + xy + y^2 & = a. \end{array} \right.$$

Exercice 142. — Déterminer une base des idéaux d'élimination I_1 et I_2 pour l'idéal I engendré par les équations

$$\left| \begin{array}{rl} x^2 + y^2 + z^2 & = 4, \\ x^2 + 2y^2 & = 5, \\ xz & = 1. \end{array} \right.$$

Déterminer les solutions dans $\mathbb{Q}^3$ de ce système.

Exercice 143. — On considère les équations

$$\left| \begin{array}{rl} t^2 + x^2 + y^2 + z^2 & = 0, \\ t^2 + 2x^2 - xy - z^2 & = 0, \\ t + y^3 - z^3 & = 0. \end{array} \right.$$

Soit I l'idéal engendré par ces équations.

1. Calculer une base de Gröbner de I pour l'ordre lexicographique induit par $z < y < x < t$.
2. Calculer une base de Gröbner de l'idéal $I \cap \mathbb{Q}[x,y,z]$.
3. Calculer une base de Gröbner de $I \cap \mathbb{Q}[x,y,z]$ avec l'ordre monomial `degrevlex`.

A.4.8. Recherche d'extrema et de points critiques.—

Exercice 144. — Déterminer les extrema de la fonction réelle

$$f = x^2 + y^2 + xy,$$

soumis à la contrainte $x^2 + 2y^2 = 1$.

Exercice 145. — Montrer que la fonction réelle

$$f = (x^2 + y^2)(x^2 + y^2 - 1)z + z^3 + x + y$$

ne possède pas de point critique.

Bibliographie

[1] William W. Adams, Philippe Loustaunau, *An introduction to Gröbner bases*, American mathematical society, (1994)

[2] Bruno Buchberger, Franz Winker, *Ideals, Varieties and Algorithms*, Cambridge University Press (1998)

[3] David Cox, John Little, Donal O'Shea, *Ideals, Varieties and Algorithms*, Third Edition, Springer (2007)

[4] Daniel Perrin, *Géométrie algébrique. Une introduction*, InterEditions et CNRS Editions (1995), Chapitre I : Ensembles algébriques affines

Index