UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LES BASES DE GROEBNER ET LES ORDRES MONOMIAUX

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES

PAR

LAURENCE MARCOTTE

AVRIL 2008

REMERCIEMENTS

Ce mémoire n'aurait pas été possible sans l'apport indéfectible de Pierre Bouchard, professeur titulaire de mathématiques à l'Université du Québec à Montréal et directeur de ce mémoire.

Sa grande disponibilité, sa rigueur, son souci du détail ainsi que ses encouragements m'ont énormément aidé tout au long de ce travail.

Que ce mémoire lui soit le modeste témoignage de ma reconnaissance envers son savoir, son enseignement et son amour des mathématiques.

Je tiens aussi à exprimer ma profonde gratitude envers mes parents pour le soutien qu'ils m'ont apporté au fil des ans dans la poursuite de mes études et pour m'avoir permis de devenir tout ce que je suis aujourd'hui.

TABLE DES MATIÈRES

RÉSUMÉ

Ce mémoire se veut une étude détaillée de ce que sont les bases de Groebner, de la manière dont on les calcule et dans quels cas elles sont utiles et utilisées.

Un éventail de définitions, de théorèmes, de lemmes et de propositions sont énoncés et démontrés afin que les lecteurs, lectrices, intéressé(e)s, puissent avoir les ressources nécessaires leur permettant de comprendre vraiment ce que sont les bases de Groebner.

Ce travail propose également une définition précise de ce que sont les ordres monomiaux et élabore une formulation claire de leur classification.

Ce mémoire donne, en plus, une description des algorithmes sous forme de procédures, programmés en utilisant le logiciel Maple 10 qui sont mis en annexe.

Tous les algorithmes, décrits en pseudo-code, ont été programmés de manière naïve, c'est-à-dire, sans astuce de programmation afin d'en réduire le temps d'exécution ou l'espace mémoire occupé. Cela afin de faire voir aux lecteurs, lectrices, intéressé(e)s, comment se font les calculs.

Mots clés : Anneau, idéal, base de Groebner, module, ordre monomial, ordre monoïdal.

INTRODUCTION

La théorie des bases de Groebner pour les anneaux de polynômes à plusieurs indéterminées, telle que nous allons la voir dans ce mémoire a été développée en 1965 en Autriche.

Le père de cette théorie est Bruno Buchberger, il a donné à ces bases le nom de son directeur d'études, Wolfgang Groebner.

Les bases de Groebner sont employées par les mathématiciens et les informaticiens comme outils pour une multitude d'applications dans lesquelles les méthodes de géométrie algébrique algorithmique jouent un rôle important.

À titre d'applications d'algèbre commutative, notons le calcul de l'intersection entre deux idéaux ou l'appartenance d'un polynôme à un idéal donné.

À titre d'applications plus concrètes, soulignons le problème du pavage des polyominos ou celui des robots parallèles.

Le temps d'exécution et la mémoire utilisée par un ordinateur pour construire une base de Groebner dépendent essentiellement de l'ordre des variables et de l'ordre des monômes dans les polynômes impliqués.

Les bases de Groebner peuvent être facilement calculées avec des logiciels de calcul symbolique, tels Mathematica, Maple, Singular, Macaulay et CoCoA.

Dans ce mémoire, nous avons fait appel, pour nos calculs et algorithmes, au logiciel Maple, version 10.

Ce travail est décrit en deux grandes parties comportant plusieurs volets.

Dans un premier temps, il est question d'algèbre commutative.

Après avoir fait un rappel de notions élémentaires, nous expliquons ce que sont les bases de Groebner et définissons les ordres monomiaux.

Ensuite, nous présentons quelques applications de bases de Groebner et nous expliquons, grâce à des algorithmes détaillés et des exemples approfondis, comment les construire.

Les références, exemples et notations sont principalement tirés des ouvrages (Cox, 1996) et (Cox, 1998).

Dans un deuxième temps, il est question d'ordres monomiaux.

Nous élaborons la manière de décrire ces ordres, entre autres, par des matrices dont les éléments sont tous positifs.

Ensuite, nous faisons leur classification, en nous basant sur le travail de deux auteurs, soient Volker Weispfenning (Allemagne) et Lorenzo Robbiano (Italie), s'étant penchés sur le sujet.

Ce mémoire a été conçu dans une perspective à la fois mathématique et informatique : bien que la théorie des bases de Groebner soit née des mathématiques pures, sa compréhension et son utilisation s'expliquent aisément dans le domaine informatique, via les outils mentionnés ci-haut.

Ce travail sera utile dans la découverte et l'apprentissage des bases de Groebner et permettra de connaître des situations mathématiques dans lesquelles elles sont essentielles.

Ce travail représente, également, un endroit où l'on retrouvera le contenu détaillé et expliqué des articles de Weispfenning et de Robbiano sur la classification des ordres monomiaux.

Première partie
Bases de Groebner, rappels d'algèbre commutative et applications

CHAPITRE I

RAPPELS D'ALGÈBRE COMMUTATIVE

Convention : Dans cette première partie, à moins d'avis contraire, A désignera un anneau de polynômes à un nombre fini d'indéterminées sur un corps commutatif.

1 Idéaux

Définition 1.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Un idéal I de A est un sous-ensemble ($I \subset A$) ayant les propriétés suivantes :

- $0 \in I$,
- $(x \in I \text{ et } y \in I) \Rightarrow (x + y \in I)$,
- $(a \in A \text{ et } x \in I) \Rightarrow (ax \in I)$.

Lemme 1.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient $f_1, \cdots, f_s$ des éléments de A.*

L'ensemble

$$\langle f_1, \cdots, f_s \rangle = \{h_1 f_1 + \cdots + h_s f_s \mid h_i \in A\}$$

est un idéal de A et on l'appellera l'idéal engendré par $f_1, \cdots, f_s$.

Démonstration. Voir (Cox, 1996) page 29. □

En général, dans un idéal de A, il y a une infinité d'éléments, mais on verra plus loin

qu'un idéal de A a toujours un nombre fini de générateurs [1].

1.1 Idéaux premiers

Définition 1.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Un idéal I de A est dit idéal premier si et seulement si il satisfait les deux conditions suivantes.

1. *I est un idéal propre de A, c'est-à-dire que $I \neq A$.*
2. *Si $f \in A$, $g \in A$ et $(f \cdot g) \in I$, alors ou bien $f \in I$ ou bien $g \in I$.*

1.2 Idéaux maximaux

Définition 1.3. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Un idéal I de A est dit idéal maximal si $I \neq A$ et si tout idéal J de A, contenant I, est tel que $J = I$ ou bien $J = A$.

Lemme 1.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Tout idéal I de A, de la forme $I = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$ est un idéal maximal, avec $a_1, \cdots, a_n \in k$.

Démonstration. Voir (Cox, 1996) page 198. □

Proposition 1.1. *Dans un anneau commutatif, un idéal maximal est nécessairement un idéal premier.*

Démonstration. Voir (Cox, 1996) page 199. □

[1] Voir la section sur le théorème de base de Hilbert.

1.3 Idéaux monomiaux

Définition 1.4. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Un idéal I de A est dit idéal monomial s'il existe un sous ensemble $E \subset \mathbb{Z}^n_{\geq 0}$, possiblement infini, tel que l'idéal I est composé de tous les polynômes qui sont des sommes finies de la forme

$$\sum_{e \in E} h_e x^e,$$

où $h_e \in A$.

Dans ce cas, nous notons $I = \langle x^e \mid e \in E \rangle$.

2 Variétés

Une variété algébrique est un sous-ensemble de k^n, où

$$k^n = \{(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in k\},$$

défini par des équations algébriques, avec k un corps commutatif.

Un des objets de la géométrie algébrique est le classement des différentes variétés algébriques. Dans ce classement, la notion d'idéal premier entre en jeu.

Définition 2.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Une variété V sur k est l'ensemble des zéros communs dans k^n d'un nombre fini d'éléments $f_1, \cdots, f_s$ de A.

$$V(f_1, \cdots, f_s) = \{(a_1, \cdots, a_n) \in k^n \mid f_i(a_1, \cdots, a_n) = 0, \text{ pour } i = 1, \cdots, s\}.$$

Une variété est donc l'ensemble de toutes les solutions du système d'équations

$$f_1(x_1, \cdots, x_n) = \cdots = f_s(x_1, \cdots, x_n) = 0.$$

2.1 Variétés irréductibles

Définition 2.2. *Une variété $V \subset k^n$ est dite irréductible si, V écrite sous la forme $V = V_1 \cup V_2$, pour V_1, V_2 des variétés, est telle que ou bien $V_1 = V$ ou bien $V_2 = V$.*

Exemple 2.1. Soit $A = k[x, y, z]$, où k est un corps commutatif.

Prenons $f_1 = x^2 + y^2 + z^2 - 4$ et $f_2 = z - 1$, avec $f_1, f_2 \in A$.

On a que $V(f_1, f_2)$ est le cercle de rayon $\sqrt{3}$ et de centre $(0, 0, \sqrt{3})$ parallèle au plan xy.

CHAPITRE II

MINIMUM NÉCESSAIRE SUR LES ORDRES MONOMIAUX

1 Ordres monomiaux

Définition 1.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Un ordre monomial sur A est une relation $>$ sur $\mathbb{Z}_{\geq 0}^n = \mathbb{N}^n$, ou de manière équivalente, une relation $>$ sur l'ensemble des monômes x^α de A, avec $\alpha \in \mathbb{Z}_{\geq 0}^n$, satisfaisant les trois conditions suivantes :

1. *$>$ est un ordre total sur $\mathbb{Z}_{\geq 0}^n$.*
2. *Si $\alpha > \beta$, alors $\alpha + \gamma > \beta + \gamma$, avec $\beta, \gamma \in \mathbb{Z}_{\geq 0}^n$.*
3. *$>$ est un bon ordre sur $\mathbb{Z}_{\geq 0}^n$.*

   Cette dernière condition veut dire que tout sous-ensemble non vide de $\mathbb{Z}_{\geq 0}^n$ possède un plus petit élément pour $>$.

Notons $\mathbb{T}^n$ l'ensemble des monômes x^α de A.

À titre d'exemple, notons que l'ordre numérique connu

$$\cdots > n+1 > n > \cdots > 2 > 1 > 0,$$

avec $n \in \mathbb{N}$, satisfait les trois conditions précédentes, c'est donc un ordre monomial.

Il existe plusieurs ordres monomiaux, mais pour les besoins de ce mémoire, nous ne verrons en détail que trois d'entre eux. Ces ordre seront définis sur les monômes, mais par abus de langage, nous les utiliseront aussi sur les termes.

1.1 Ordre lexicographique

Définition 1.2. *Soient* $\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.

Nous dirons que $\alpha >_{\text{lex}} \beta$ *si, dans le vecteur différence* $(\alpha - \beta) \in \mathbb{Z}^n_{\geq 0}$, *la coordonnée non nulle la plus à gauche est positive.*

Si $\alpha >_{\text{lex}} \beta$, *alors nous pourrons dire que* $x^\alpha >_{\text{lex}} x^\beta$.

Exemple 1.1. Soit $A = k[x, y, z]$, où k est un corps commutatif.

Prenons le polynôme $f = 4xy^2 + 2y^3z^4$ de A. Le premier terme de f est $4xy^2$ avec $\alpha = (1, 2, 0)$ et le deuxième terme de f est $2y^3z^4$ avec $\beta = (0, 3, 4)$.

On obtient donc le vecteur différence $(\alpha - \beta) = (1, -1, -4)$. Puisque sa coordonnée non nulle la plus à gauche est positive, on a que $\alpha >_{\text{lex}} \beta$. C'est donc dire que $4xy^2 >_{\text{lex}} 2y^3z^4$.

1.2 Ordre lexicographique avec priorité au degré

Définition 1.3. *Soient* $\alpha = (\alpha_1, \cdots, \alpha_n)$, $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.

Nous dirons que $\alpha >_{\text{grlex}} \beta$ *si* $|\alpha| > |\beta|$ *ou alors si* $|\alpha| = |\beta|$ *et* $\alpha >_{\text{lex}} \beta$, *où*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i \quad et \quad |\beta| = \sum_{i=1}^{n} \beta_i.$$

Si $\alpha >_{\text{grlex}} \beta$, *alors nous pourrons dire que* $x^\alpha >_{\text{grlex}} x^\beta$.

Exemple 1.2. Soit $A = k[x, y, z]$, où k est un corps commutatif.

Prenons le même polynôme $f = 4xy^2 + 2y^3z^4$ de A que dans l'exemple précédent. Le premier terme de f est $4xy^2$ avec $|\alpha| = 3$ et le deuxième terme de f est $2y^3z^4$ avec $|\beta| = 7$.

On obtient que $|\beta| > |\alpha|$ et donc $\beta >_{\text{grlex}} \alpha$. C'est donc dire que $2y^3z^4 >_{\text{grlex}} 4xy^2$.

1.3 Ordre lexicographique inversé avec priorité au degré

Définition 1.4. *Soient* $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.

Nous dirons que $\boldsymbol{\alpha} >_{\text{grevlex}} \boldsymbol{\beta}$ *si* $|\boldsymbol{\alpha}| > |\boldsymbol{\beta}|$ *ou alors si* $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}|$ *et que dans le vecteur différence* $(\boldsymbol{\alpha} - \boldsymbol{\beta}) \in \mathbb{Z}^n_{\geq 0}$, *la coordonnée non nulle la plus à droite est négative, où*

$$|\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i \quad et \quad |\boldsymbol{\beta}| = \sum_{i=1}^{n} \beta_i.$$

Si $\boldsymbol{\alpha} >_{\text{grevlex}} \boldsymbol{\beta}$, *alors nous pourrons dire que* $x^{\boldsymbol{\alpha}} >_{\text{grevlex}} x^{\boldsymbol{\beta}}$.

Exemple 1.3. Soit $A = k[x, y, z]$, où k est un corps commutatif.

Prenons le polynôme $g = 2xy^5z^2 - x^4yz^3$ de A. Le premier terme de g est $2xy^5z^2$ avec $\boldsymbol{\alpha} = (1, 5, 2)$, $|\boldsymbol{\alpha}| = 8$ et le deuxième terme de g est $-x^4yz^3$ avec $\boldsymbol{\beta} = (4, 1, 3)$, $|\boldsymbol{\beta}| = 8$.

On doit donc examiner le vecteur différence $(\boldsymbol{\alpha} - \boldsymbol{\beta}) = (-3, 4, -1)$. Puisque sa coordonnée non nulle la plus à droite est négative, on a que $\boldsymbol{\alpha} >_{\text{grevlex}} \boldsymbol{\beta}$. C'est donc dire que $2xy^5z^2 >_{\text{grevlex}} -x^4yz^3$.

2 Terme, coefficient et monôme dominant

Définition 2.1. *Soit* $A = k[x_1, \cdots, x_n]$, *où* k *est un corps commutatif et soient* $f = a_d\mathbf{x}^d + a_{d-1}\mathbf{x}^{d-1} + \cdots + a_1\mathbf{x} + a_0$ *un polynôme de* A, *où* $a_i \in k, a_d \neq 0$, *pour* $i = 1, \cdots, n$ *et* t *est un ordre monomial sur* A.

Soit d *le degré du polynôme.*

Nous dirons que $a_d\mathbf{x}^d$ *est le terme dominant de* f, *selon* t *et nous le noterons* $\text{LT}(f)$ *(pour leading term).*

Nous dirons aussi que a_d *est le coefficient dominant de* f, *selon* t *et nous le noterons* $\text{LC}(f)$ *(pour leading coefficient).*

Finalement, nous dirons que $\mathbf{x}^d$ *est le monôme dominant de* f, *selon* t *et nous le noterons* $\text{LM}(f)$ *(pour leading monomial).*

Exemple 2.1. Soit $A = k[x, y]$, où k est un corps commutatif.

Prenons le polynôme $f = 5x^3y^2 - 6x^2y + 3y - 1$ de A et l'ordre lexicographique.

Nous avons que LT(f)=$5x^3y^2$, LC(f)=5, et LM(f)=x^3y^2.

Définition 2.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit I un idéal non nul de A.*

- *Notons par* LT(I) *l'ensemble des termes dominants des éléments de I.*
  Autrement dit, LT(I)=$\{a_d\mathrm{x}^d \mid$ *il existe* $f \in I$ *avec* LT(f) = $a_d\mathrm{x}^d\}$.
- *Notons par* $\langle \mathrm{LT}(I) \rangle$ *l'idéal engendré par les éléments de* LT(I).

Proposition 2.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit I un idéal de A.*

On a que

- $\langle \mathrm{LT}(I) \rangle$ *est un idéal monomial.*
- *Il existe* $f_1, \cdots, f_s \in I$ *tel que* $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_s) \rangle$.

Démonstration. Voir (Cox, 1996) page 73. □

3 Outils mathématiques

3.1 Plus petit commun multiple

Définition 3.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient f, g deux polynômes de A.*

Le plus petit commun multiple (PPCM) *entre f et g est un polynôme $h \in A$ tel que $f \mid h$ et $g \mid h$ et tel que si $f \mid h'$ et $g \mid h'$, alors $h \mid h'$, avec $h' \in A$.*

$f \mid h$ veut dire que f divise h, c'est-à-dire qu'il existe $p \in A$ tel que $h = fp$.

Le plus petit commun multiple est déterminé à un multiple inversible près d'un élément de A.

Exemple 3.1. Soit $A = k[x, y]$, où k est un corps commutatif.

Le PPCM$(2x^2y^3, x^3y)$ est un polynôme de la forme ax^3y^3, où a est inversible dans A, c'est-à-dire que a est une constante non nulle. Par convention, on prendra $a = 1$.

Donc PPCM$(2x^2y^3, x^3y) = x^3y^3$.

Exemple 3.2. Soit $A = k[x, y]$, où k est un corps commutatif. Calculons le PPCM$(x^3 - y^3, x^2 - y^2)$.

D'abord, on a que $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ et que $x^2 - y^2 = (x - y)(x + y)$, alors les deux polynômes ont le terme $(x - y)$ en commun.

On aura donc que PPCM$(x^3 - y^3, x^2 - y^2) = (x - y)(x^2 + xy + y^2)(x + y) = x^4 + x^3y - xy^3 - y^4$.

Exemple 3.3. Soit $\mathbb{Z}$ l'anneau des nombres entiers.

On a que PPCM$(3, 5) = 15$ et PPCM$(3, 5) = -15$. Par convention, on prendra celui positif. Donc PPCM$(3, 5) = 15$.

3.2 S-polynôme

Définition 3.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient f, g deux polynômes non nuls de A et soit t un ordre monomial fixé.*

Le S-polynôme de f et g est, par définition,

$$S(f, g) = \frac{\text{PPCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} \cdot f - \frac{\text{PPCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} \cdot g,$$

où les LT *et* LM *sont calculés selon t.*

Le S-polynôme est utilisé, dans les calculs, afin d'annuler les termes dominants.

Exemple 3.4. Soit $A = k[x, y]$, où k est un corps commutatif.

Prenons $f = x^3y^2 - x^2y^3 + x$ et $g = 3x^4y + y^2$, deux polynômes de A.

On peut calculer le S-polynôme de f et g, selon l'ordre lexicographique

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot (x^3y^2 - x^2y^3 + x) - \frac{x^4y^2}{3x^4y} \cdot (3x^4y + y^2) = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

CHAPITRE III

BASES DE GROEBNER D'IDÉAUX

1 Algorithme de division de polynômes

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit t un ordre monomial sur A et soient $f_1, \cdots, f_s$ des éléments de A.

Soient l'idéal $I = \langle f_1, \cdots, f_s \rangle$ de A et une permutation σ de l'ensemble $\{1, \cdots, s\}$.

L'algorithme de division de polynômes sert à diviser un polynôme f de A par une suite de polynômes $F = (f_1, \cdots, f_s)$ de A.

Ce qui permet d'exprimer f sous la forme

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

où les a_i, appelés quotients, sont des polynômes de A et r, appelé reste, est aussi un polynôme de A. L'écriture de f sous la forme $f = a_1 f_1 + \cdots + a_s f_s + r$, où aucun terme de r n'est divisible par un des $\mathrm{LT}(f_i)$, pour $i = 1 \cdots s$, est unique.

r est le reste de la division de f par F et ce, quelque soit la permutation σ. En effet, le reste de la division de f par $(f_1, \cdots, f_s)$ est égal au reste de la division de f par $(f_{\sigma(1)}, \cdots, f_{\sigma(s)})$.

Nous verrons plus tard que si le reste n'est pas nul, alors le polynôme f à diviser n'est

pas dans l'idéal I [1]. L'inverse n'est pas toujours vrai.

Notons par $\overline{f}^F$, le reste de la division de f par les f_i de F.

Algorithme 1.1 (Algorithme de division de polynômes). Prenons un polynôme f de A, $(f_1, \cdots, f_s)$ une suite de polynômes de A et t un ordre monomial sur A.

Calculons d'abord $\mathrm{LT}(f)$ et $\mathrm{LT}(f_i)$ pour $i = 1, \cdots, s$, selon t.

Posons $r = 0$ et $a_1 = \cdots = a_s = 0$.

Trouvons le plus petit i tel que $\mathrm{LT}(f_i) \mid \mathrm{LT}(f)$, s'il existe.

Alors $\mathrm{LT}(f_i) \mid \mathrm{LT}(f)$ deviendra notre premiers terme de a_i.

Cela fera en sorte que

$$f := f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i \text{ et } a_i := a_i + \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)}.$$

S'il n'existe pas de tel i, on a $r := r + \mathrm{LT}(f)$ et $f := f - \mathrm{LT}(f)$.

Recommençons tout, cette fois, avec notre nouveau polynôme f.

L'algorithme se terminera quand $f = 0$.

Pour voir que l'algorithme se termine, observons qu'à chaque fois que la variable f est redéfinie, soit son degré baisse, soit elle devient nulle. Ainsi, $f = 0$ arrivera forcément après un nombres fini d'étapes de l'algorithme et il se terminera.

Exemple 1.1. Soit $A = k[x, y]$, où k est un corps commutatif. Prenons $f = xy^2 + 1 \in A$ et deux polynômes $(xy + 1, y + 1)$ de A.

$\mathrm{LT}(f) = xy^2$, $\mathrm{LT}(xy + 1) = xy$, $\mathrm{LT}(y + 1) = y$, selon l'ordre lexicographique.

$\mathrm{LT}(xy+1) \mid \mathrm{LT}(f)$, puisque $xy \mid xy^2 = y$. Donc $a_1 = y$ et $f := f - (y(xy+1)) = -y+1$.

---

[1] Voir la section sur l'appartenance à un idéal.

Prenons $f = -y + 1$ et $(xy + 1, y + 1)$, $\mathrm{LT}(f) = -y$, $\mathrm{LT}(xy + 1) = xy$, $\mathrm{LT}(y + 1) = y$, selon l'ordre lexicographique.

$\mathrm{LT}(xy + 1) \nmid \mathrm{LT}(f)$, puisque $xy \nmid -y$.

Mais $\mathrm{LT}(y+1) \mid \mathrm{LT}(f)$, puisque $y \mid -y = -1$. Donc $a_2 = -1$ et $f := f-(-1(y+1)) = 2$.

Prenons $f = 2$ et $(xy + 1, y + 1)$, $\mathrm{LT}(xy + 1) \nmid \mathrm{LT}(f)$, puisque $xy \nmid 2$ et $\mathrm{LT}(y + 1) \nmid \mathrm{LT}(f)$, puisque $y \nmid 2$. Donc $r = 2$ et $f = 0$.

Nous avons terminé et nous obtenons

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

Exemple 1.2. Soit $A = k[x, y]$, où k est un corps commutatif. Prenons $f = x^3y+xy^3+y^2 \in A$ et deux polynômes $(x^2 + xy, y^2 - 1)$ de A.

$\mathrm{LT}(f) = x^3y$, $\mathrm{LT}(x^2 + xy) = x^2$, $\mathrm{LT}(y^2 - 1) = y^2$, selon l'ordre lexicographique.

$\mathrm{LT}(x^2 + xy) \mid \mathrm{LT}(f)$, puisque $x^2 \mid x^3y = xy$. Donc $a_1 = xy$ et $f := f - (xy(x^2 + xy)) = xy^3 + y^2 - x^2y^2$.

Mais, nous avons encore que $\mathrm{LT}(x^2 + xy) \mid \mathrm{LT}(f)$, puisque $x^2 \mid -x^2y^2 = -y^2$. Donc $a_1 = xy - y^2$ et $f := f - (-y^2(x^2 + xy)) = 2xy^3 + y^2$.

Prenons $f = 2xy^3+y^2$ et (x^2+xy, y^2-1), $\mathrm{LT}(f) = 2xy^3$, $\mathrm{LT}(x^2+xy) = x^2$, $\mathrm{LT}(y^2-1) = y^2$, selon l'ordre lexicographique.

$\mathrm{LT}(x^2+xy) \nmid \mathrm{LT}(f)$, puisque $x^2 \nmid 2xy^3$, Mais $\mathrm{LT}(y^2-1) \mid \mathrm{LT}(f)$, puisque $y^2 \mid 2xy^3 = 2xy$.

Donc $a_2 = 2xy$ et $f := f - (2xy(y^2 - 1)) = 2xy + y^2$.

Prenons $f = 2xy+y^2$ et (x^2+xy, y^2-1), $\mathrm{LT}(f) = 2xy$, $\mathrm{LT}(x^2+xy) = x^2$, $\mathrm{LT}(y^2-1) = y^2$, selon l'ordre lexicographique.

$\mathrm{LT}(x^2 + xy) \nmid \mathrm{LT}(f)$ et $\mathrm{LT}(y^2 - 1) \nmid \mathrm{LT}(f)$. Donc $r = 2xy + y^2$ et $f = 0$.

Finalement, nous obtenons que

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

2 Théorème de base de Hilbert

Remarque 2.1. Un ensemble de générateurs d'un idéal est parfois appelé base d'un idéal.

Théorème 2.1 (Théorème de base de Hilbert). *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Tout idéal I de A a un nombre fini de générateurs. Il s'écrit sous la forme $I = \langle f_1, \cdots, f_s \rangle$, pour $f_1, \cdots, f_s$ des éléments de I.

Avant de démontrer le théorème de base de Hilbert, énonçons un lemme.

Lemme 2.1. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et $I = \langle x^e \mid e \in E \rangle$ un idéal monomial de A, où E est un sous ensemble de $\mathbb{Z}^n_{\geq 0}$, possiblement infini, tel que vu dans la définition* 1.4. *du chapitre* 1, *section* 1.

Alors, un monôme x^β est dans l'idéal I si et seulement si x^β est divisible par un x^e, pour $e \in E$.

Démonstration du lemme. Voir (Cox, 1996) page 67. □

Démonstration du théorème de base de Hilbert. Si $I = \{0\}$, on prendra l'ensemble de générateurs $\{0\}$ qui est assurément fini, puisqu'il contient un seul élément.

Si $I \neq \{0\}$ et si I contient des polynômes non nuls, alors un ensemble de générateurs $\{f_1, \cdots, f_s\}$ de I peut être construit de la manière suivante.

On sait, par la proposition 2.1. du chapitre 2, section 2, qu'il y a $f_1, \cdots, f_s \in I$ tels que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_s) \rangle$. Nous supposerons que $I = \langle f_1, \cdots, f_s \rangle$.

Il est évident que $\langle f_1, \cdots, f_s \rangle \subset I$, puisque chaque f_i est dans I.

Inversement, soit un polynôme $f \in I$. Si nous appliquons l'algorithme de division de polynômes pour diviser f par $(f_1, \cdots, f_s)$, alors nous obtenons une expression de la forme

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

où aucun terme de r n'est divisible par $\mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_s)$.

Nous supposerons que $r = 0$. Pour montrer cela, notons que

$$r = f - a_1 f_1 - \cdots - a_s f_s \in I.$$

Si $r \neq 0$, alors on aurait $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_s) \rangle$ et par le lemme 2.1., il s'ensuivrait que $\mathrm{LT}(r)$ devrait être divisible par un des $\mathrm{LT}(f_i)$, ce qui contredit la définition même du reste r. Par conséquent, $r = 0$.

Donc,

$$f = a_1 f_1 + \cdots + a_s f_s + 0 \in \langle f_1, \cdots, f_s \rangle,$$

ce qui montre que $I \subset \langle f_1, \cdots, f_s \rangle$. □

3 Base de Groebner d'idéaux

Les bases de Groebner nous permettent de résoudre des problèmes en relation avec les idéaux d'un anneau de polynômes de manière algorithmique et calculatoire.

Définition 3.1. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, I un idéal de A et $g_1, \cdots, g_s$ des éléments de I.*

Pour un ordre monomial fixé t, un sous-ensemble fini $G = \{g_1, \cdots, g_s\}$ de I est appelé base de Groebner de I si et seulement si l'une des deux conditions équivalentes suivantes est satisfaite :

1. *$\langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_s) \rangle$ engendre l'idéal I.*

2. *Le terme dominant de tout élément de l'idéal I est divisible par un des termes dominants* $\mathrm{LT}(g_i)$ *de G, pour au moins un $i = 1, \cdots, s$.*

Remarque 3.1. En général, l'ensemble des LT d'un ensemble de générateurs d'un idéal n'est pas un ensemble de générateurs de l'idéal des LT des éléments de l'idéal.

3.1 Algorithme de Buchberger pour idéaux

Une base de Groebner d'un idéal peut être construite en utilisant l'algorithme de Buchberger, selon un ordre monomial fixé.

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.

Soient $f_1, \cdots, f_s$ des éléments de A et $I = \langle f_1, \cdots, f_s \rangle$, un idéal non nul de A.

Algorithme 3.1 (Algorithme de Buchberger pour idéaux). Soit $G = \{f_1, \cdots, f_s\}$ un ensemble de générateurs de I et soit t un ordre monomial sur A. Soit G', une copie de ce G qui nous sera utile, puisqu'on gardera la valeur initiale de G.

Pour chaque paire d'éléments de G', on en calcule le S-polynôme, selon t. On utilisera ensuite l'algorithme de division de polynômes pour diviser ce S-polynôme par les éléments de G', ce qui nous donnera un reste dans chaque cas. Si ce reste n'est pas nul, alors il s'ajoutera aux éléments de G et on passe à la paire suivante, sinon on passe directement à la paire suivante.

Sinon, on recopie G dans G, et on recommence.

L'algorithme se terminera lorsqu'on aura testé toutes les paires d'éléments de G' et que le reste de l'algorithme de division de polynômes du S-polynôme calculé par les éléments de G' y sera nul à chaque boucle. En d'autres mots, Si un passage dans la boucle n'ajoute pas d'éléments à G', on aura alors construit une base de Groebner de l'idéal I, qui sera composé des éléments de $G = G'$.

Théorème 3.1 (Buchberger). *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient $f_1, \cdots, f_s$ des éléments de A et soit $I = \langle f_1, \cdots, f_s \rangle$ un idéal non nul de A. Soit*

$G = \{f_1, \cdots, f_s\}$ un ensemble de générateurs de I et soit t un ordre monomial sur A.

Une base de Groebner de I peut être construite, en un nombre fini d'étapes, par l'algorithme de Buchberger.

Avant de démontrer le théorème de Buchberger, énonçons deux théorèmes.

Théorème 3.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit I un idéal de A.*

Une base $G = \{g_1, \cdots, g_s\}$ de I est une base de Groebner de I si et seulement si, pour toute paire (i, j) telle que $i \neq j$, $i, j = 1, \cdots, s$, le reste de la division de polynômes du S-polynôme(g_i, g_j) par G, est nul.

Démonstration. Voir (Cox, 1996) page 82. □

Théorème 3.3 (Condition de la chaîne ascendante). *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit $I_1 \subset I_2 \subset I_3 \subset \cdots$ une chaîne ascendante d'idéaux de A.*

Alors, il existe un $N \geq 1$, où $N \in \mathbb{N}$ tel que $I_N = I_{N+1} = I_{N+2} = \cdots$, en d'autres mots, A est noethérien.

Démonstration. Voir (Cox, 1996) page 76. □

Démonstration du théorème de Buchberger. Nous allons d'abord montrer que $G \subset I$ au départ et $G \subset I$ à chaque étape de l'algorithme.

Au départ, on a bien que $G \subset I$. Par la suite, on ajoute à G le reste de la division de polynômes du S-polynôme(p, q), avec $p, q \in G$, par les éléments de G', où G' est une copie de G. Donc, si $G \subset I$, alors p, q et par conséquent S-polynôme(p, q), sont aussi dans I. Puisque l'algorithme de division de polynômes se fait par les éléments de $G' \subset I$, nous avons que $G \cup \{\text{reste}\} \subset I$.

L'algorithme se terminera lorsque le reste de l'algorithme de division de polynômes du S-polynôme(p, q), pour tout p, q dans G, par les éléments de G', sera nul. Par conséquent, par le théorème 3.2., G est une base de Groebner de I.

Il nous reste maintenant à montrer que l'algorithme se termine. Nous avons besoin de voir ce qui se passe après chaque boucle de l'algorithme.

À la fin de chaque test de toutes les paires d'éléments de G', on sait que G se compose des éléments de G' et des restes non nuls de la l'algorithme de division de polynômes des S-polynômes par les éléments de G'. Alors, $\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle$, puisque $G' \subset G$.

A fortiori, si $G' \neq G$, nous pouvons affirmer que $\langle \mathrm{LT}(G') \rangle < \langle \mathrm{LT}(G) \rangle$. Pour ce faire, supposons qu'un reste $r \neq 0$ est ajouté à G'. Puisque r est un reste de l'algorithme de division de polynômes par les éléments de G', $\mathrm{LT}(r)$ n'est divisible par aucun des LT des éléments de G' et donc $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$.

Le fait que $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$ vient appuyer notre affirmation, voulant que $\langle \mathrm{LT}(G') \rangle < \langle \mathrm{LT}(G) \rangle$.

De plus, les idéaux $\langle \mathrm{LT}(G') \rangle$ composés des polynômes calculés à chaque boucle de l'algorithme forment une chaîne ascendante d'idéaux de A. Le théorème 3.3. implique qu'après un nombre fini d'itérations, la chaîne va se stabiliser. Alors, le fait que $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ va éventuellement se produire et donc, notre algorithme se terminera après un nombre fini d'étapes. □

Exemple 3.1. Soient $A = k[x, y, z]$, où k est un corps commutatif, l'idéal $I = \langle x + y, y^3 + xz \rangle$ de A et l'ordre lexicographique. Posons $G = \{x + y, y^3 + xz\}$.

S-polynôme$(x+y, y^3+xz) = -y^3+yz$ et le reste de l'algorithme de division de $-y^3+yz$ par $\{x + y, y^3 + xz\}$ est $-y^3 + yz$. Donc $G = \{x + y, y^3 + xz, -y^3 + yz\}$.

S-polynôme$(x+y, y^3+xz) = -y^3+yz$ et le reste de l'algorithme de division de $-y^3+yz$ par $\{x + y, y^3 + xz, -y^3 + yz\}$ est 0.

S-polynôme$(y^3 + xz, -y^3 + yz) = -y^4 - xyz$ et le reste de l'algorithme de division de $-y^4 - xyz$ par $\{x + y, y^3 + xz, -y^3 + yz\}$ est 0.

S-polynôme$(x + y, -y^3 + yz) = -y^6 - xyz^2$ et le reste de l'algorithme de division de $-y^6 - xyz^2$ par $\{x + y, y^3 + xz, -y^3 + yz\}$ est 0.

Donc, nous avons construit notre base de Groebner de I,

$$G = \{x + y, y^3 + xz, -y^3 + yz\}.$$

Les bases de Groebner qui sont calculées en utilisant l'algorithme de Buchberger tel que décrit précédemment contiennent parfois plus d'éléments que nécessaire. Nous verrons qu'on pourra éliminer des générateurs inutiles.

Théorème 3.4. *Soit G une base de Groebner d'un idéal I et soit un polynôme $p \in G$ tel que* $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Alors, $G \setminus \{p\}$ est aussi une base de Groebner.

Démonstration. On sait que $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$.

Si $\langle \mathrm{LT}(p) \rangle \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$, alors $\mathrm{LT}(G \setminus \{p\}) = \mathrm{LT}(G)$.

Par définition, il s'ensuit que $G \setminus \{p\}$ est une base de Groebner de I. □

En ajustant les constantes afin de réduire les coefficients dominants à 1, en enlevant tous les p tels que $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$ et en remplaçant G par $G \setminus \{p\}$ après chaque retrait d'un tel p, on obtient une base de Groebner minimale.

3.2 Base de Groebner minimale

Définition 3.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient I un idéal de A et t un ordre monomial sur A.*

Une base de Groebner minimale de I est une base de Groebner $G = \{g_1, \cdots, g_s\}$ de I telle que

- *le coefficient dominant* ($\mathrm{LC}(g_i)$) *est* 1, *pour tous les* g_i,
- *aucun* $\mathrm{LT}(g_i)$ *ne doit être dans* $\langle \mathrm{LT}(G \setminus \{g_i\})\rangle$, *où les* LT *et* LC *sont calculés selon* t.

Pour un même idéal, on peut avoir plusieurs bases de Groebner minimales. Heureusement, nous pourrons choisir une base de Groebner minimale qui sera « meilleure »que toutes les autres et qui deviendra une base de Groebner réduite.

3.3 Base de Groebner réduite

Définition 3.3. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soient I un idéal de A et t un ordre monomial sur A.*

Une base de Groebner réduite de I est une base de Groebner $G = \{g_1, \cdots, g_s\}$ de I telle que

- *le coefficient dominant* ($\mathrm{LC}(g_i)$) *est* 1, *pour tous les* g_i,
- *aucun monôme des* g_i *ne doit être dans* $\langle \mathrm{LT}(G \setminus \{g_i\})\rangle$, *où les* LT *et* LC *sont calculés selon* t.

Proposition 3.1 (Unicité). *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et I un idéal non nul de A.*

Alors, pour un ordre monomial donné, I n'a qu'une seule base de Groebner réduite.

Démonstration. Voir (Cox, 1996) page 90. □

Remarque 3.2. Une base de Groebner minimale, voire même réduite, d'un idéal n'est pas nécessairement un ensemble minimal de générateurs de cet idéal.

Remarque 3.3. Une base de Groebner minimale d'un idéal I est un élément minimal dans l'ensemble ordonné par inclusion des bases de Groebner de I. On peut se demander s'il est un élément minimal de l'ensemble de toutes les bases de cet idéal I.

Exemple 3.2. Soit l'idéal $I = \langle x^2 - y, xy - z \rangle$ de $A = k[x, y, z]$, où k est un corps commutatif.

On calcule la base de Groebner réduite de I et on trouve $G = \{x^2 - y, xy - z, xz - y^2, y^3 - z^2\}$. Cette base de Groebner est réduite, donc *a fortiori*, minimale. C'est donc un élément minimal de l'ensemble ordonné par inclusion de toutes les bases de Groebner de I.

Pourtant, on voit bien que G contient strictement la base $\{x^2 - y, xy - z\}$ de I, donc G n'était pas une base minimale de I puisqu'elle en contenait une plus petite.

Remarque 3.4. Le plus petit nombre de générateurs que peut avoir un idéal I peut être strictement plus petit que le nombre de générateurs d'un ensemble minimal de générateurs de I. Autrement dit, si $G_I = (\{S \mid S \text{ est un ensemble de générateurs de } I\}, \subseteq)$, alors les éléments minimaux de G_I n'ont pas tous la même cardinalité.

Exemple 3.3. Soit l'idéal $I = \langle x, 1 - x \rangle$ de $A = k[x]$, où k est un corps commutatif.

L'ensemble $\{x, 1 - x\}$ est certainement un ensemble minimal de générateurs de I, car ni $\{x\}$ ni $\{1 - x\}$ n'engendre A au complet. Cet ensemble a deux éléments.

Cependant, l'anneau $A = \{1\}$ admet aussi l'ensemble $\{1\}$ comme ensemble de générateurs. L'ensemble $\{1\}$ a un élément.

Un est strictement plus petit que deux.

En somme, d'un idéal donné I, on peut trouver une base de Groebner de I. De cette base de Groebner de I, on peut trouver une base de Groebner minimale de I et de cette base de Groebner minimale de I, on peut trouver la base de Groebner réduite de I.

4 Base d'un idéal

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.

Par le théorème de base de Hilbert, vu plus tôt, tout idéal de A est engendré par un

nombre fini de générateurs. I est lui-même une base de I, car tout $f \in I$ peut s'écrire comme $f = 1f$, où $1 \in A$.

4.1 Base minimale d'un idéal

Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et I un idéal de A.

Étant donné une base $\mathcal{B}$ de l'idéal I, telle que $\mathcal{B} = \{f_1, \cdots, f_s\}$, où $f_1, \cdots, f_s$ sont des éléments de A, on peut se demander comment en extraire une base minimale.

Ceci nous amène à trouver un algorithme nous permettant de calculer une base minimale d'un idéal. En voici l'idée.

Ôtons des f_j, pour $j = 1, \cdots, s$, un à la fois et regardons si ce qui reste engendre toujours le même idéal I. Par exemple, si on enlève f_1, est-ce que

$$\langle f_2, \cdots, f_s \rangle \stackrel{?}{=} \langle f_1, f_2, \cdots, f_s \rangle$$

Pour le savoir, calculons une base de Groebner réduite de I pour chacun, si ces bases de Groebner réduites sont égales, c'est que les idéaux sont égaux, par l'unicité de la base de Groebner réduite d'un idéal. Si les idéaux sont égaux, c'est que l'élément enlevé était superflu.

On remplace $\mathcal{B}$ par $\mathcal{B} \setminus f_1$ et on vérifie ensuite si f_2 était superflu et ainsi de suite jusqu'à ce qu'il ne reste plus d'éléments superflus et donc, que la base $\mathcal{B}$ soit minimale.

CHAPITRE IV

APPLICATIONS DE BASES DE GROEBNER D'UN IDÉAL

1 Intersection d'idéaux

Soient $A = k[x_1, \cdots, x_n]$ et $B = k[x_1, \cdots, x_n, u]$, où k est un corps commutatif.

Soient $f_1, \cdots, f_s, g_1, \cdots, g_l$ des éléments de A et soient $I = \langle f_1, \cdots, f_s \rangle$ et $J = \langle g_1, \cdots, g_l \rangle$ deux idéaux de A.

Théorème 1.1. *Soit l'idéal de B engendré par $uI = \langle uf_1, \cdots, uf_s \rangle$ et soit l'idéal de B engendré par $(1-u)J = \langle (1-u)g_1, \cdots, (1-u)g_l \rangle$.*

On a que $(uI \cap A) = \{0\}$ et que $((1-u)J \cap A) = \{0\}$.

Alors, l'intersection des idéaux I et J peut être représentée comme suit :

$$I \cap J = (uI + (1-u)J) \cap A.$$

Démonstration. Voir (Cox, 1996) page 185. □

Cela nous amène à un algorithme permettant de trouver l'intersection de deux idéaux.

Algorithme 1.1 (Algorithme pour l'intersection d'idéaux)**.** Prenons $I = \langle f_1, \cdots, f_s \rangle$ et $J = \langle g_1, \cdots, g_l \rangle$ deux idéaux de A.

Considérons l'idéal $\langle uf_1, \cdots, uf_s, (1-u)g_1, \cdots, (1-u)g_l \rangle$ de B. Trouvons une base de

Groebner de cet idéal, pour un ordre monomial t de sorte que

$$(u > x_1, \cdots, x_n).$$

Les éléments de la base de Groebner de cet idéal ne contenant pas de termes en u formeront une base de Groebner de l'intersection de I et J.

Exemple 1.1. Soit $A = k[x, y]$, où k est un corps commutatif.

Si on veut calculer l'intersection de l'idéal $I = \langle x^2y \rangle$ de A avec l'idéal $J = \langle xy^2 \rangle$ de A, on calcule d'abord l'idéal

$$uI + (1-u)J = \langle ux^2y, uxy^2 - xy^2 \rangle$$

de l'anneau $A[u] = k[u, x, y]$.

Ensuite, on trouve la base de Groebner de cet idéal

$$\{ux^2y, uxy^2 - xy^2, x^2y^2\}.$$

En éliminant les termes en u, on a que $\{x^2y^2\}$ est une base de Groebner de l'idéal $(uI + (1-u)J) \cap A$ et donc, que

$$I \cap J = \langle x^2y^2 \rangle.$$

2 Appartenance à un idéal

Si nous combinons les bases de Groebner avec l'algorithme de division de polynômes, nous arrivons à déterminer si un polynôme appartient ou non à un idéal donné.

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.

Soient $f_1, \cdots, f_s$ des éléments de A et t un ordre monomial sur A et soient $I = \langle f_1, \cdots, f_s \rangle$ un idéal de A et f un polynôme de A.

Algorithme 2.1 (Algorithme pour l'appartenance à un idéal). On trouve une base de Groebner de I et ensuite, on applique l'algorithme de division de polynômes de f par

les éléments de cette base de Groebner de I, ce qui nous donnera un reste r. Le reste ne dépend pas de l'ordre des polynômes par lesquels on divise.

Si r est nul, on a que f appartient à I.

Si r n'est pas nul, f n'appartient pas à I, puisque f n'est pas combinaison linéaire des générateurs de l'idéal I.

En général, ceci n'est pas vrai. Dans notre cas, c'est vrai parce que les générateurs de l'idéal I forment une base de Groebner.

Le fait que l'on ait une base de Groebner ici nous garantit que f n'est pas combinaison linéaire des générateurs de I, parce que $\mathrm{LT}(r)$ n'est pas combinaison linéaire des $\mathrm{LT}(f)$ et des générateurs qui forment une base de Groebner de I, donc $r \in I$ et puisque f est une somme de r et d'un élément de I (la combinaison linéaire des éléments de la base de Groebner), alors $f \notin I$, sinon, on aurait que $r \in I$.

Exemple 2.1. Soit $A = k[x, y, z]$, où k est un corps commutatif. Prenons l'idéal $I = \langle xz - y^2, x^3 - z^2 \rangle$ de A et le polynôme $f = -4x^2y^2z^2 + y^6 + 3z^5 \in A$.

Calculons la base de Groebner de I suivante

$$G = \{xz - y^2, x^3 - z^2, -x^2y^2 + z^3, xy^4 - z^4, -y^6 + z^5\},$$

par l'algorithme de Buchberger vu précédemment, selon l'ordre lexicographique.

En appliquant l'algorithme de division de f par les éléments de G, on obtient

$$f = (-4y^2(xz + y^2) + 0 + 0 + 0 + (-y^6 + z^5)) + 0,$$

avec un reste nul. Le polynôme f appartient donc à l'idéal I.

Nous pouvons même trouver quels coefficients polynômiaux donner aux générateurs initiaux de l'idéal et qui font que notre polynôme en est bien combinaison linéaire. Pour ce faire, nous devons exprimer les éléments de G en fonction des générateurs initiaux de I seulement.

Cela sera possible grâce à un algorithme permettant de trouver les coefficients des générateurs de I qui vont donner G. Dans cet algorithme, on commence par calculer le S-polynôme d'une paire d'éléments de G, en laissant les polynômes factorisés. Ensuite, on applique l'algorithme de division de polynômes de ce S-polynôme par les éléments de G.

Si le reste est nul, alors on ne fait rien et on prend une autre paire d'éléments de G pour en calculer le S-polynôme.

Si le reste n'est pas nul et qu'il est égal au S-polynôme calculé, alors c'est qu'il est un élément de G.

Ce qui donne $G = \{xz - y^2, x^3 - z^2, x^2(xz - y^2) - z(x^3 - z^2), xy^2(xz - y^2) + z(x^2(xz - y^2) - z(x^3 - z^2)), y^4(xz - y^2) + z(xy^2(xz - y^2) + z(x^2(xz - y^2) - z(x^3 - z^2)))\}$.

Ensuite, on prend les éléments de G et on les multiplie par le résultat obtenu de l'algorithme de division de polynômes. Nous obtenons alors un « énorme »polynôme exprimé avec les générateurs donnés de I, $-4y^2(xz + y^2)(xz - y^2) + 3y^4(xz - y^2) + 3z(xy^2(xz - y^2) + z(x^2(xz - y^2) - z(x^3 - z^2)))$.

Les coefficients respectifs des générateurs $xz - y^2$ et $x^3 - z^2$ de I dans ce gros polynôme sont finalement les coefficients cherchés. $N_1 = -xzy^2 - y^4 + 3x^2z^2$ et $N_2 = -3z^3$.

On peut alors constater que

$$f = N_1I_1 + N_2I_2 = (-xzy^2 - y^4 + 3x^2z^2)(xz - y^2) + (-3z^3)(x^3 - z^2) = -4x^2y^2z^2 + y^6 + 3z^5.$$

3 Égalité d'idéaux

Pour d'autres situations, on peut vérifier si deux ensembles de polynômes engendrent le même idéal.

Algorithme 3.1 (Algorithme pour l'égalité d'idéaux). Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.

Soient $f_1, \cdots, f_s, g_1, \cdots, g_r$ des éléments de A, t un ordre monomial sur A et $I = \langle f_1, \cdots, f_s \rangle$ et $J = \langle g_1, \cdots, g_r \rangle$ deux idéaux de A.

Pour un ordre monomial donné t, calculons la base de Groebner réduite de l'idéal I et la base de Groebner réduite de l'idéal J.

On sait, par la proposition 3.1. du chapitre 3, section 3, qu'il n'existe qu'une seule base de Groebner réduite pour un idéal donné. Si, après calcul, on trouve la même base de Groebner réduite, c'est que les deux ensembles de polynômes engendrent le même idéal. On pourra alors conclure que, même si les polynômes des ensembles sont différents, on a égalité d'idéaux.

Exemple 3.1. Soit $A = k[x, y, z]$, où k est un corps commutatif. Prenons $I = \langle x^2y - zx^2 + xy - 1, x^2y - zx^2 + xz - 1 \rangle$ et $J = \langle xy - 1, xz - 1, y - z \rangle$, deux idéaux de A.

Lorsqu'on calcule la base de Groebner réduite de I, on obtient la même chose que lorsqu'on calcule la base de Groebner réduite de J, soit $\{x^2 - y, y^2 - 1\}$. On peut donc conclure que I et J sont des idéaux égaux.

CHAPITRE V

MODULES

La notion d'idéal d'un anneau $A = k[x_1, \cdots, x_n]$ peut être étendue aux sous-modules d'un module A^s, où s est un entier naturel. C'est donc dire que le sous-module est à l'idéal, ce que le module est à l'anneau.

Nous pouvons définir aussi naturellement les notions d'ordre monomial sur un module et de bases de Groebner de sous-modules.

1 Modules

Définition 1.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

On dit que $M = (A, +, .)$ est un module sur A, ou un A-module si

1. *$(A, +)$ est un groupe abélien sous l'addition,*
2. *. est une opération*

$$\begin{array}{ccc} (A \times M) & \to & M \\ (a, m) & \mapsto & a.m \overset{\text{def}}{=} am \end{array}$$

telle que

- $a(m_1 + m_2) = am_1 + am_2$,
- $(a_1 + a_2)m = a_1m + a_2m$,
- $a_1(a_2m) = (a_1a_2)m$,
- $1m = m$,

avec $a, a_1, a_2 \in A$ et $m, m_1, m_2 \in M$.

1.1 Sous-modules

Définition 1.2. *Soit M un A-module. Un sous-ensemble $(N \subseteq M)$ est appelé sous-A-module de M si et seulement si*

1. *N est un sous-groupe abélien de M, c'est-à-dire que les trois conditions suivantes doivent être satisfaites :*
   - $(n_1 \in N \text{ et } n_2 \in N) \Rightarrow (n_1 + n_2 \in N)$,
   - $(n \in N) \Rightarrow (-n \in N)$,
   - $0 \in N$,
2. $(a \in A \text{ et } n \in N) \Rightarrow (an \in N)$.

Remarque 1.1. L'anneau A est lui-même un A-module et les sous-A-modules sont les idéaux de A.

Remarque 1.2. Si A est un corps commutatif, alors les A-modules sont des espaces vectoriels et les sous-A-modules d'un A-module V sont les sous-espaces vectoriels de V.

1.2 Modules gradués

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.

Pour $s \in \mathbb{N}$, posons A_s l'ensemble des polynômes homogènes de degré s, de A. C'est-à-dire l'ensemble des polynômes de A dont chaque terme est de degré s.

Définition 1.3. *Un module gradué sur A, est un A-module M muni d'une famille $(M_d)_{d\in\mathbb{Z}}$ de sous-groupes du groupe additif de M qui satisfont les conditions suivantes :*

1. $M = \bigoplus_{d\in\mathbb{Z}} M_d$.
2. *La décomposition en somme directe de M, ci-dessus, est compatible avec la multiplication par des éléments homogènes de A, dans le sens où $A_s M_d \subset M_{s+d}$ pour $s \in \mathbb{N}$ et $d \in \mathbb{Z}$.*

Les éléments de M_d sont appelés les éléments homogènes de degré d de M.

Remarque 1.3. $A = \bigoplus_{s\in\mathbb{N}} A_s$ est lui-même un A-module gradué.

2 Ordres monomiaux pour modules

Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, s un entier naturel, $M = A^s$ et soit $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

Un monôme de M est un élément de la forme $x^{\alpha} e_i$ pour tout $i = 1, \cdots, s$, avec

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

le i-ième élément de la base canonique de A^s.

Tout élément du module $M = A^s$ peut être écrit de manière unique comme une combinaison linéaire de monômes de M.

Exemple 2.1. Soit $A = k[x, y]$, où k est un corps commutatif et soit

$$p = \begin{pmatrix} 5xy^2 - y^{10} + 3 \\ 4x^3 + 2y \\ 16x \end{pmatrix},$$

un élément de A^3.

Alors, on a que

$$p = 5\begin{pmatrix} xy^2 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} y^{10} \\ 0 \\ 0 \end{pmatrix} + 3\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 4\begin{pmatrix} 0 \\ x^3 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 0 \\ y \\ 0 \end{pmatrix} + 16\begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix},$$

$$p = 5xy^2 e_1 - y^{10} e_1 + 3e_1 + 4x^3 e_2 + 2ye_2 + 16xe_3.$$

La définition d'ordre monomial sur le module A^s est semblable à celle d'ordre monomial sur l'anneau A vu plus tôt.

Définition 2.1. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, s un entier naturel, $M = A^s$ et soit $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.*

Un ordre monomial sur A^s est une relation $>$ sur l'ensemble des monômes de A^s, satisfaisant les trois conditions suivantes :

1. *$>$ est un ordre strict total sur $\mathbb{Z}^n_{\geq 0}$.*
2. *Pour toute paire de monômes (m, n) de A^s, avec $m > n$, nous avons $x^\alpha m > x^\alpha n$, pour tout monôme x^α de A.*
3. *$>$ est un bon ordre sur $\mathbb{Z}^n_{\geq 0}$. Cette dernière condition est équivalente au fait que $x^\alpha m > m$, pour tout monôme $m \in A^s$ et tout monôme $x^\alpha \in A$ tel que $x^\alpha \neq 1$.*

De plus, on pourra déterminer une extension d'ordre monomial sur A de deux manières.

Définition 2.2. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et $>$ un ordre monomial sur A. Soit $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.*

Nous dirons que $x^{\boldsymbol{\alpha}} e_i >_{\mathrm{TOP}} x^{\boldsymbol{\beta}} e_j$ si $x^{\boldsymbol{\alpha}} > x^{\boldsymbol{\beta}}$ ou alors si $x^{\boldsymbol{\alpha}} = x^{\boldsymbol{\beta}}$ et que $i < j$.

Autrement dit, dans ce cas, le terme prédomine sur la position (TOP : term over position).

Définition 2.3. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et $>$ un ordre monomial sur A. Soit $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$.*

Nous dirons que $x^{\boldsymbol{\alpha}} e_i >_{\mathrm{POT}} x^{\boldsymbol{\beta}} e_j$ si $i < j$ ou alors si $i = j$ et que $x^{\boldsymbol{\alpha}} > x^{\boldsymbol{\beta}}$.

Autrement dit, dans ce cas, la position prédomine sur le terme (POT : position over term).

Les définitions de terme dominant, de coefficient dominant et de monôme dominant d'un élément du module A^s sont semblables à celles pour un élément de l'anneau A vues plus tôt [1]. Nous ne les reproduirons pas ici mais illustrons-en une par un exemple. Trouvons le terme dominant d'un élément de module.

[1] Voir la section sur terme, coefficient et monôme dominant.

Exemple 2.2. Prenons le même élément $p \in A^3$ que dans le précédent exemple et l'ordre lexicographique sur A,

$$p = \begin{pmatrix} 5xy^2 - y^{10} + 3 \\ 4x^3 + 2y \\ 16x \end{pmatrix}.$$

On commence d'abord par trouver le terme dominant de chacune des coordonnées de p, selon l'ordre lexicographique.

$\mathrm{LT}(5xy^2 - y^{10} + 3) = 5xy^2$, $\mathrm{LT}(4x^3 + 2y) = 4x^3$, $\mathrm{LT}(16x) = 16x$.

Ensuite, si on prend TOP, on aura que

$$\mathrm{LT}(p) = \begin{pmatrix} 0 \\ 4x^3 \\ 0 \end{pmatrix},$$

et si on prend POT, on aura que

$$\mathrm{LT}(p) = \begin{pmatrix} 5xy^2 \\ 0 \\ 0 \end{pmatrix}.$$

2.1 Algorithme de division d'éléments d'un module

L'algorithme de division d'éléments de module est basé sur les mêmes critères que l'algorithme de division de polynômes vu et énoncé plus haut [2].

Inutile donc, ici, de reproduire l'algorithme de division d'éléments de module en détail sinon, mentionner qu'il fonctionne avec des éléments de module. Cet algorithme a été programmé, comme tous les autres, avec le logiciel Maple 10 et est disponible en annexe.

De manière semblable, on introduit la notion de S-polynôme pour éléments de module. Mais pour ce faire, voyons une propriété des éléments de module.

---

[2] Voir la section sur l'algorithme de division de polynômes.

Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, s un entier naturel et $M = A^s$. Soient $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Z}^n_{\geq 0}$, avec x^α, x^β des monômes de A et $m = x^\alpha e_i, n = x^\beta e_j$ des monômes de A^s, pour $i, j = 1, \cdots, s$.

Nous dirons que $m \mid n$ si et seulement si $x^\alpha \mid x^\beta$ et $i = j$.

Dans ce cas, nous pourrons trouver le PPCM(m, n) et le plus grand commun diviseur entre deux éléments de module, PGCD(m, n). Par contre, si $m \nmid n$, nous conviendrons que PPCM$(m, n) = 0$.

3 Étendre les bases de Groebner aux modules

Définition 3.1. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, m un entier naturel, N un sous-A-module du A-module $M = A^m$ et $<$ un ordre monomial sur N.*

On appelle $\langle \mathrm{LT}_<(N) \rangle$ le sous-module engendré par les LT *de tous les éléments de N.*

Définition 3.2. *Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, m un entier naturel, N un sous-A-module du A-module $M = A^m$ et $<$ un ordre monomial sur N. Soient $g_1, \cdots, g_l$ des éléments de A.*

$\{g_1, \cdots, g_l\} \subseteq N$ est une base de Groebner de N si

$$\langle \mathrm{LT}_<(N) \rangle = \langle \mathrm{LT}_<(g_1), \cdots, \mathrm{LT}_<(g_l) \rangle.$$

La version de l'algorithme de Buchberger pour idéaux, énoncée plus haut, [3] peut être légèrement modifiée pour nous permettre de l'appliquer aux sous-modules. Nous ne la verrons pas en détail ici, mais cet algorithme a été programmé, avec le logiciel Maple 10, en utilisant des éléments de modules et est disponible en annexe. Cet algorithme permet bien d'obtenir une base de Groebner de sous-modules.

---

[3] Voir la section sur l'algorithme de Buchberger pour idéaux

Idem pour la notion de base de Groebner minimale de sous-modules et celle de base de Groebner réduite de sous-modules.

4 Syzygies

Soient $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et M un A-module de type fini, c'est-à-dire avec un nombre fini de générateurs. Soient $\{f_1, \cdots, f_s\}$ un ensemble de générateurs de M.

Prenons la base canonique $\{e_1, \cdots, e_s\}$ de A^s, où $e_1 = (1, 0, \cdots, 0), \cdots, e_s = (0, \cdots, 0, 1)$.

Soit

$$A^s \xrightarrow{\phi} M,$$

la seule application linéaire telle que

$$\phi(e_1) = f_1, \cdots, \phi(e_s) = f_s.$$

On a que

- ϕ est bien définie, car $\{e_1, \cdots, e_s\}$ est une base de A^s.
- ϕ est surjective, car tout élément m de M est de la forme

  $$m = g_1 f_1 + \cdots + g_s f_s$$

  qui est équivalent à dire que

  $$m = g_1\phi(e_1) + \cdots + g_s\phi(e_s) = \phi(g_1 e_1 + \cdots + g_s e_s) = \phi(g_1, \cdots, g_s),$$

  avec $g_1, \cdots, g_s$ des éléments de A.

Définition 4.1. *Si $\phi(g_1, \cdots, g_s) = 0$, alors on dit que $(g_1, \cdots, g_s)$ est une syzygie, plus précisément,*

$$(g_1, \cdots, g_s) \in \mathrm{Syz}(f_1, \cdots, f_s) \subset A^s.$$

Autrement dit,

$$\mathrm{Syz}(f_1, \cdots, f_s) \stackrel{\text{def}}{=} \mathrm{Ker}(\phi) = \{(g_1, \cdots, g_s) \mid \phi(g_1, \cdots, g_s) = 0\}.$$

5 Présentations de modules

Définition 5.1. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif.*

Considérons une suite de A-modules

$$\cdots \to M_{i+1} \xrightarrow{\phi_{i+1}} M_i \xrightarrow{\phi_i} M_{i-1} \to \cdots,$$

avec ϕ_{i+1}, ϕ_i, des homomorphismes.

- *Nous dirons que la suite est exacte pour M_i si*

$$\mathrm{Im}(\phi_{i+1}) = \mathrm{Ker}(\phi_i).$$

- *Nous dirons que la suite entière est exacte si elle est exacte pour chaque M_i qui ne se trouve ni au début ni à la fin de la suite.*

Définition 5.2. *Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif et soit M un A-module.*

Une présentation de M est une suite exacte

$$A^s \xrightarrow{\psi} A^r \xrightarrow{\phi} M \to 0.$$

En prenant la base canonique de A^s, $\{e_1 = (1, 0, \cdots, 0), \cdots, e_s = (0, \cdots, 0, 1)\}$ et la base canonique de A^r, $\{\tilde{e}_1 = (1, 0, \cdots, 0), \cdots, \tilde{e}_r = (0, \cdots, 0, 1)\}$, cela revient à se donner

- *la suite de générateurs $(\phi(\tilde{e}_1), \cdots, \phi(\tilde{e}_r)) \overset{\text{def}}{=} (f_1, \cdots, f_r)$ de M, car ϕ est une fonction surjective,*
- *la suite de générateurs $(\psi(e_1), \cdots, \psi(e_s))$ de $\psi(A^s) = \mathrm{Im}(\psi) = \mathrm{Ker}(\phi) \overset{\text{def}}{=} \mathrm{Syz}(f_1, \cdots, f_r)$.*

On peut se demander comment décrire une telle application

$$A^s \xrightarrow{\psi} A^r ?$$

On se donne une matrice Z de ψ par rapport à une base de A^s et à une base de A^r.

Prenons les bases canoniques introduites plus haut.

La j-ième colonne de la matrice Z est formée des coordonnées de $\psi(e_j)$ en la base $\{\tilde{e}_1, \cdots, \tilde{e}_r\}$,

$$\psi(e_j) = z_{1j}\tilde{e}_1 + \cdots + z_{rj}\tilde{e}_r.$$

La matrice Z est de la forme

$$Z = \begin{bmatrix} z_{11} & \cdots & z_{1s} \\ \vdots & & \vdots \\ z_{r1} & \cdots & z_{rs} \end{bmatrix}$$

En fait, les éléments $\psi(e_1), \cdots, \psi(e_s)$ sont les générateurs de $\mathrm{Im}(\psi)$, et on sait que $\mathrm{Im}(\psi) = \mathrm{Ker}(\phi) \overset{\text{def}}{=} \mathrm{Syz}(f_1, \cdots, f_r)$.

Donc, $\{\psi(e_1), \cdots, \psi(e_s)\}$ est un ensemble de générateurs de $\mathrm{Syz}(f_1, \cdots, f_r)$. En particulier,

$$\psi(e_1) = z_{11}\tilde{e}_1 + \cdots + z_{r1}\tilde{e}_r = (z_{11}, \cdots, z_{r1}).$$

Les coordonnées en base $\{\tilde{e}_1, \cdots, \tilde{e}_r\}$ de $\psi(e_j)$ sont $\begin{bmatrix} z_{1j} \\ \vdots \\ z_{rj} \end{bmatrix}$, correspondant aussi à la j-ième colonne de la matrice Z.

En identifiant un élément $(h_1, \cdots, h_s)$ de A^s, avec la colonne $\begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix}$, on peut définir

$$ZA^s = \{Z \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} \mid (h_1, \cdots, h_s) \in A^s\} = \{[\psi(h_1, \cdots, h_s)]_{(\tilde{e}_1, \cdots, \tilde{e}_r)} \mid (h_1, \cdots, h_s) \in A^s\}.$$

Exemple 5.1. Soient $A = k[x, y]$, où k est un corps commutatif et M un A-module. Soit l'idéal $I = \langle x^2 - x, xy, y^2 - y \rangle$ de A.

I a une présentation donnée par

$$A^3 \xrightarrow{\psi} A^3 \xrightarrow{\phi} I \to 0,$$

où ϕ est l'homomorphisme défini par la matrice $\begin{bmatrix} x^2-x & xy & y^2-y \end{bmatrix}$ et ψ est l'homomorphisme défini par la matrice $\begin{bmatrix} y & y^2-y & 0 \\ 1-x & y-1 & y-1 \\ 0 & -x^2 & -x \end{bmatrix}$. Cette matrice a été calculée à l'aide du logiciel Maple 10 et est détaillée dans le document en annexe.

Il est facile de voir que $\begin{bmatrix} y^2-y \\ y-1 \\ -x^2 \end{bmatrix}$ est combinaison linéaire de $\begin{bmatrix} y \\ 1-x \\ 0 \end{bmatrix}$ et de $\begin{bmatrix} 0 \\ y-1 \\ -x \end{bmatrix}$, puisque

$$(y-1)\begin{bmatrix} y \\ 1-x \\ 0 \end{bmatrix} + x\begin{bmatrix} 0 \\ y-1 \\ -x \end{bmatrix} = \begin{bmatrix} y^2-y \\ y-1 \\ -x^2 \end{bmatrix}.$$

Donc, I a aussi une présentation donnée par

$$A^2 \xrightarrow{\psi'} A^3 \xrightarrow{\phi} I \to 0,$$

où ϕ est l'homomorphisme défini par la matrice $\begin{bmatrix} x^2-x & xy & y^2-y \end{bmatrix}$ et où ψ' est l'homomorphisme défini par la matrice $\begin{bmatrix} y & 0 \\ -x+1 & y-1 \\ 0 & -x \end{bmatrix}$.

On pourra vérifier que

$$\begin{bmatrix} x^2-x & xy & y^2-y \end{bmatrix}\begin{bmatrix} y & 0 \\ -x+1 & y-1 \\ 0 & -x \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}.$$

Ce dernier calcul montre que $\mathrm{Im}(\psi) \subset \mathrm{Ker}(\phi)$. Pour avoir une présentation, il faudrait aussi montrer que $\mathrm{Im}(\psi) \supset \mathrm{Ker}(\phi)$.

Cet exemple a été entièrement programmé à l'aide du logiciel Maple 10, en se basant sur la théorie des présentations de modules, prise dans l'ouvrage (Cox, 1998) et nous garantit que nous aurons $\mathrm{Im}(\psi) = \mathrm{Ker}(\phi)$.

Deuxième partie

Ordres monomiaux

CHAPITRE VI

GROUPES ET CORPS ORDONNÉS

1 Groupe ordonné

Définition 1.1. *Un groupe ordonné est un couple $((C,+),P)$ où $(C,+)$ est un groupe et $P \subseteq C$ est un ensemble tel que*

- *$\{P,\{0\},-P\}$ est une partition de C où 0 est le neutre de $(C,+)$ et $-P = \{-x \mid x \in P\}$,*
- *$P+P \subseteq P$.*

Un ordre total compatible avec l'opération d'un groupe ordonné est complètement déterminé dès qu'on connaît un ensemble P satisfaisant les deux conditions ci-haut. P sera alors l'ensemble des éléments strictement positifs pour cet ordre.

À titre d'exemple, le groupe additif des entiers relatifs $(\mathbb{Z},+)$ muni de la relation d'ordre habituelle, avec $P = \mathbb{R}^*$ et le groupe multiplicatif des réels strictement positifs $(\mathbb{R}_+^*,\cdot)$, avec $P =]1,\infty[$, sont des groupes ordonnés.

Proposition 1.1. *Soient $c_1, c_2 \in C$.*

P permet de définir un ordre total sur C en posant $c_1 \leq c_2$ si et seulement si $(c_2 - c_1) \in P \cup \{0\}$.

Alors cet ordre est compatible avec l'opération de C.

Démonstration. Montrons d'abord que $\leq$ est une relation d'ordre.

- Réflexivité.

  Quelque soit $c \in C$, on a que $c \leq c$, car $c - c = 0 \in P \cup \{0\}$. Donc, $\leq$ est réflexive.

- Anti-symétrie.

  Pour tout c_1,$c_2 \in C$. Si $c_1 \leq c_2$ et $c_2 \leq c_1$, alors $c_2 - c_1 \in P \cup \{0\}$ et $c_1 - c_2 = -(c_2 - c_1) \in P \cup \{0\}$.

  Mais si $c_2 - c_1 \in P$, on aurait aussi que $c_2 - c_1 = -(-(c_2 - c_1)) \in P$. Ce qui contredit le fait que P et $-P$ soient disjoints.

  Ceci implique donc que $c_2 - c_1 = 0$ et alors, $c_1 = c_2$. Donc, $\leq$ est anti-symétrique.

- Transitivité.

  Soient c_1,c_2,$c_3 \in C$ tels que $c_1 \leq c_2$ et $c_2 \leq c_3$.

  Si $c_1 = c_2$ ou $c_2 = c_3$, on a que $c_1 \leq c_3$.

  Si $c_1 \neq c_2$ et $c_2 \neq c_3$, on a que $c_2 - c_1 \in P$ et $c_3 - c_2 \in P$, d'où $(c_3 - c_2) + (c_2 - c_1) = c_3 - c_1 \in P + P \subseteq P$. Donc, $\leq$ est transitive.

Puisque $\leq$ est réflexive, anti-symétrique et transitive, on a bien une relation d'ordre.

De trois choses l'une,

$c_1 - c_2 \in -P$ et alors $c_2 - c_1 \in P$,

$c_1 - c_2 \in P$,

$c_1 - c_2 = 0$.

Donc, ou bien $c_1 < c_2$ ou bien $c_2 < c_1$ ou bien $c_1 = c_2$. On a donc que $\leq$ est un ordre total.

De plus, quelque soit $c \in C$, si $c_1 \leq c_2$, alors $c_2 - c_1 \in P \cup \{0\}$, d'où $c_2 - c_1 = (c_2 + c) - (c_1 + c) \in P \cup \{0\}$.

Ce qui montre que $c_1 + c \leq c_2 + c$ et donc que $\leq$ est compatible avec l'opération du groupe. □

Proposition 1.2. *Dans un groupe ordonné, la somme d'éléments négatifs est un élément négatif.*

Démonstration. Soit un groupe ordonné $((C,+),P)$ tel que $\{P,\{0\},-P\}$ soit une partition de C. Soient $f,g \in -P$.

Posons $f = -f_1$, où $f_1 \in P$ et $g = -g_1$, où $g_1 \in P$. En faisant leur somme, on a $f+g = -f_1 - g_1 = -(f_1+g_1)$.

On sait que $(f_1+g_1) \in P$, car la somme d'éléments positifs est un élément positif. Alors, $-(f_1+g_1) \in -P$ et donc, $f+g \in -P$. □

2 Corps ordonné

Définition 2.1. *Un corps ordonné $((C,+,\cdot),P)$ est un couple formé d'un corps $(C,+,\cdot)$ et d'un sous-ensemble $P \subseteq C$ tel que $((C,+),P)$ soit un groupe ordonné et que P soit stable sous la multiplication, c'est-à-dire que*

$$(f \in P \, et \, g \in P) \Rightarrow (f \cdot g \in P).$$

À titre d'exemple, le corps des rationnels $\mathbb{Q}$ et le corps des réels $\mathbb{R}$, munis de la relation d'ordre habituelle, sont des corps ordonnés.

CHAPITRE VII

FAÇONS DE DÉCRIRE DES ORDRES MONOMIAUX

1 Ordres monomiaux

Définition 1.1. *Étant donné un monoïde, un ordre monoïdal sur ce monoïde est un ordre total, compatible avec l'opération de ce monoïde.*

Un ordre monoïdal sur un groupe G, fait de (G, P) un groupe ordonné, où P est l'ensemble des éléments strictement positifs de G.

Proposition 1.1. *Un ordre monomial sur $\mathbb{N}^n$ est un ordre monoïdal pour lequel tout élément de $\mathbb{N}^n$ est supérieur à $(0, \cdots, 0)$.*

Ceci est équivalent à dire que $\mathbb{N}^n$ est bien ordonné.

Démonstration. Voir (Cox, 1996) page 70. □

Définition 1.2. *La donnée d'un ordre monomial sur l'ensemble $\mathbb{T}^n$ des monômes de $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif, équivaut à la donnée d'un ordre monomial sur le monoïde additif $\mathbb{N}^n$.*

En d'autres mots, l'application

$$\begin{array}{ccc} \mathbb{T}^n & \xrightarrow{\log} & \mathbb{N}^n \\ (x_1^{\alpha_1}, \cdots, x_n^{\alpha_n}) & \mapsto & (\alpha_1, \cdots, \alpha_n) \end{array}$$

est un isomorphisme de monoïdes ordonné.

Puisque la fonction logarithmique est un isomorphisme de monoïdes, on peut travailler avec le monôme ou son logarithme.

Remarque 1.1. Dans la définition de l'ordre lexicographique inversé avec priorité au degré [1], le vecteur différence $(\alpha - \beta)$ est égal au vecteur différence $(\log(x^{\alpha})\text{- }\log(x^{\beta}))$.

1.1 Différents monoïdes

Définition 1.3. *Un ordre monomial sur $\mathbb{Z}^n$ est un ordre monoïdal qui induit, sur $\mathbb{N}^n$, un ordre monomial.*

Définition 1.4. *Un ordre monomial sur $\mathbb{Q}^n$ est un ordre monoïdal sur le groupe additif $\mathbb{Q}^n$ qui induit, sur $\mathbb{Z}^n$, un ordre monomial.*

Nous verrons que la donnée d'un ordre monomial sur l'un des monoïdes $\mathbb{N}^n$, $\mathbb{Z}^n$, $\mathbb{Q}^n$, suffit à en déterminer un et un seul sur tous les autres.

Proposition 1.2. *Un ordre monomial t sur $\mathbb{N}^n$ se prolonge de manière unique en un ordre monomial t' sur $\mathbb{Z}^n$.*

Démonstration. Pour $\mathbf{v} \in \mathbb{Z}^n$, il existe des vecteurs $\mathbf{v_1}, \mathbf{v_2} \in \mathbb{N}^n$ tels que $\mathbf{v} = \mathbf{v_1} - \mathbf{v_2}$.

Nous dirons que

$$\mathbf{v} \leq_{t'} 0 \Leftrightarrow \mathbf{v_1} \leq_t \mathbf{v_2}.$$

Pour voir que ceci est bien défini, prenons deux représentations de $\mathbf{v}$,

$$\mathbf{v} = \mathbf{v_1} - \mathbf{v_2} \text{ et } \mathbf{v} = \mathbf{v_1'} - \mathbf{v_2'},$$

avec $\mathbf{v_1'}, \mathbf{v_2'} \in \mathbb{N}^n$ et notons que

$$\mathbf{v_1} \leq_t \mathbf{v_2} \Leftrightarrow \mathbf{v_1} + \mathbf{v_2'} \leq_t \mathbf{v_2} + \mathbf{v_2'}.$$

---

[1] Voir la section sur l'ordre lexicographique inversé avec priorité au degré

Puisque $\mathbf{v}_1 = \mathbf{v} + \mathbf{v}_2$ et $\mathbf{v}'_2 = \mathbf{v}'_1 - \mathbf{v}$, par les deux représentations de $\mathbf{v}$, on a que

$$\mathbf{v}_1 + \mathbf{v}'_2 \leq_t \mathbf{v}_2 + \mathbf{v}'_2 \Leftrightarrow (\mathbf{v} + \mathbf{v}_2) + (\mathbf{v}'_1 - \mathbf{v}) \leq_t \mathbf{v}_2 + \mathbf{v}'_2.$$

Ce qui nous donne

$$\mathbf{v}'_1 + \mathbf{v}_2 \leq_t \mathbf{v}_2 + \mathbf{v}'_2$$

et donc

$$\mathbf{v}'_1 \leq_t \mathbf{v}'_2.$$

L'unicité de t' vient du fait que pour $\mathbf{v}, \mathbf{v}' \in \mathbb{Z}^n$ tels que

$$\mathbf{v} = \mathbf{v}_1 - \mathbf{v}_2 \text{ et } \mathbf{v}' = \mathbf{v}'_1 - \mathbf{v}'_2,$$

avec $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}'_1, \mathbf{v}'_2 \in \mathbb{N}^n$, on a

$$\mathbf{v} \leq_{t'} \mathbf{v}' \Leftrightarrow \mathbf{v}_1 + \mathbf{v}'_2 \leq_t \mathbf{v}'_1 + \mathbf{v}_2.$$

□

Proposition 1.3. *Un ordre monomial t sur $\mathbb{Z}^n$ se prolonge de manière unique en un ordre monomial t' sur $\mathbb{Q}^n$.*

Démonstration. Si $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{Q}^n$, soit $m \in \mathbb{N}^*$ tel que $m\mathbf{v} = (mv_1, \cdots, mv_n) \in \mathbb{Z}^n$.

Alors, nous dirons que

$$\mathbf{v} >_{t'} \mathbf{0} \Leftrightarrow m\mathbf{v} >_t \mathbf{0}.$$

Notons que ceci ne dépend pas du $m \in \mathbb{N}^*$ choisi. □

2 Ordres monomiaux représentés par des matrices

Soit $A = k[x_1, \cdots, x_n]$, où k est un corps commutatif. Soit $\mathbb{T}^n$ l'ensemble des monômes de A.

Définition 2.1. *Soient* $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$ *et* $\mathbf{v_1}, \cdots, \mathbf{v_n} \in \mathbb{Z}^n$ *des vecteurs linéairement indépendants et* Z *une matrice carrée non singulière, de rang* n, *à coefficients dans* $\mathbb{Z}$, *telle que sa* i*-ième ligne soit les coordonnées de* $\mathbf{v_i}$, *pour* $i = 1, \cdots, n$.

Z *sera de la forme*

$$\begin{bmatrix} \mathrm{v}_{11} & \cdots & \mathrm{v}_{1n} \\ \vdots & & \vdots \\ \mathrm{v}_{n1} & \cdots & \mathrm{v}_{nn} \end{bmatrix}.$$

Nous dirons que $\boldsymbol{\alpha} >_{\mathrm{Ord}(Z)} \boldsymbol{\beta}$ *si et seulement si*

$$Z \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} >_{\mathrm{lex}} Z \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Autrement dit, si le premier coefficient non nul de

$$Z \begin{bmatrix} \alpha_1 - \beta_1 \\ \vdots \\ \alpha_n - \beta_n \end{bmatrix}$$

est positif.

Si $\boldsymbol{\alpha} >_{\mathrm{Ord}(Z)} \boldsymbol{\beta}$, *alors nous pourrons dire que* $x^{\boldsymbol{\alpha}} >_{\mathrm{Ord}(Z)} x^{\boldsymbol{\beta}}$.

Proposition 2.1. *Étant donné une matrice carrée* Z *non singulière, de rang* n, *à coefficients dans* $\mathbb{Z}$, *la relation* $\mathrm{Ord}(Z)$ *est une relation d'ordre monoïdal sur* $\mathbb{Z}^n$.

Démonstration. Cela est une conséquence du fait que $>_{\mathrm{lex}}$ est une relation d'ordre monoïdal sur $\mathbb{Z}^n$ et que l'application

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\phi} & \mathbb{Z}^n \\ (\gamma_1, \cdots, \gamma_n) & \mapsto & (\gamma'_1, \cdots, \gamma'_n) \end{array},$$

dont la matrice, par rapport aux bases canoniques de $\mathbb{Z}^n$, est Z, préserve la somme dans $\mathbb{Z}^n$.

Notons que

$$\begin{bmatrix} \gamma'_1 \\ \vdots \\ \gamma'_n \end{bmatrix} = Z \begin{bmatrix} \gamma'_1 \\ \vdots \\ \gamma'_n \end{bmatrix}.$$

□

Pour déterminer si $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ est positif pour $\mathrm{Ord}(Z)$, on fait le produit scalaire de la première ligne de Z avec le vecteur colonne des coordonnées de $\boldsymbol{\alpha}$.

Si ce produit scalaire est négatif, alors $\boldsymbol{\alpha} < (0, \cdots, 0)$, pour l'ordre $\mathrm{Ord}(Z)$.

S'il est positif, alors $\boldsymbol{\alpha} > (0, \cdots, 0)$, pour l'ordre $\mathrm{Ord}(Z)$.

S'il est nul, on passe à la seconde ligne de Z.

Le fait que la matrice Z soit non singulière nous garantit que si le produit de chaque ligne de Z avec le vecteur colonne des coordonnées de $\boldsymbol{\alpha}$ est nul, alors $\boldsymbol{\alpha}$ sera nul.

De plus, on ne gagnerait rien à accepter des matrices non singulières, car rendu à la première ligne qui dépend des précédentes, le produit scalaire de cette ligne avec le vecteur colonne des coordonnées de $\boldsymbol{\alpha}$ serait automatiquement nul, puisque combinaison linéaire de vecteurs nuls.

Proposition 2.2. *Soit Z la matrice dont les lignes sont les vecteurs linéairement indépendants $\mathbf{v_1}, \cdots, \mathbf{v_n} \in \mathbb{Z}^n$.*

Alors, $\mathrm{Ord}(Z)$ *est un ordre monomial si et seulement si le premier élément non nul de chaque colonne de Z est positif.*

Démonstration. Il est clair qu'un ordre monoïdal t sur $\mathbb{T}^n$ est un ordre monomial si et seulement si $x_i >_t 1$, pour $i = 1, \cdots, n$.

Soit a_i le premier élément non nul de la i-ième colonne de la matrice Z.

Alors,

$$Z \cdot (\log(x_i) - \log(1)) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a_i \\ \vdots \end{bmatrix}$$

montre bien que $(x_i >_{\mathrm{Ord}(Z)} 1)$ est équivalent à $(a_i > 0)$. □

Remarque 2.1. Étant donnée une matrice Z non singulière, de rang n, à coefficients dans $\mathbb{Q}$, on peut définir de façon semblable $\mathrm{Ord}(Z)$.

Mais, on n'obtient pas ainsi de nouveaux ordres monoïdaux, car en multipliant chaque ligne de Z par le plus grand commun dénominateur (strictement positif) des éléments de cette ligne, on ne change pas le fait que le produit scalaire de Z par le vecteur colonne des coordonnées de $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n$, ne change pas de signe.

Remarque 2.2. La condition pour qu'un ordre monoïdal représenté par une matrice carrée de rang n soit bien défini est que les lignes de la matrice soient linéairement indépendantes.

La condition pour qu'un ordre monoïdal, représenté par une matrice non singulière de rang n, soit monomial est que le premier élément de chaque colonne de la matrice soit positif.

2.1 Exemples de représentations par des matrices

Soient $(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

- Ordre lexicographique.

$(\alpha_1, \cdots, \alpha_n) >_{\text{lex}} (0, \cdots, 0) \Leftrightarrow$

$$\begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} >_{\text{lex}} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

- Ordre lexicographique inversé [2].

  $(\alpha_1, \cdots, \alpha_n) >_{\text{invlex}} (0, \cdots, 0) \Leftrightarrow$

$$\begin{bmatrix} 0 & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & 0 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha_n \\ \alpha_{n-1} \\ \vdots \\ \alpha_1 \end{bmatrix} >_{\text{lex}} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

- Ordre avec priorité au degré.

  Si un ordre $<$ est un ordre monomial, alors on définit un ordre $\prec$ par $(\alpha_1, \cdots, \alpha_n) \prec (m_1, \cdots, m_n) \Leftrightarrow$

$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} m_i$$

  ou bien

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} m_i \quad \text{et} \quad (\alpha_1, \cdots, \alpha_n) < (m_1, \cdots, m_n).$$

  Dans le cas où $<$ est l'ordre lexicographique, on obtient l'ordre lexicographique avec priorité au degré.

  $(\alpha_1, \cdots, \alpha_n) >_{\text{grlex}} (0, \cdots, 0) \Leftrightarrow$

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & & & 0 & 0 \\ & 1 & & & \vdots \\ & & \ddots & & \\ 0 & & & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha_1 + \cdots + \alpha_n \\ \alpha_1 \\ \vdots \\ \\ \alpha_{n-1} \end{bmatrix} >_{\text{lex}} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \\ 0 \end{bmatrix}$$

[2] Cet ordre est exactement l'inverse de l'ordre lexicographique tel que nous l'avons défini.

Proposition 2.3. *Soit Z_1 une matrice triangulaire inférieure dont les éléments diagonaux sont strictement positifs.*

Si Z_2 est une matrice carrée non singulière, de rang n, alors

$$Ord(Z_2) = Ord(Z_1 Z_2).$$

Démonstration. Considérons $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n$.

Dire que $\boldsymbol{\alpha}$ est strictement positif pour Ord(Z) c'est dire que

$$\begin{bmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & & \vdots \\ z_{n1} & \cdots & z_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} >_{\text{lex}} \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},$$

où

$$Z = \begin{bmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & & \vdots \\ z_{n1} & \cdots & z_{nn} \end{bmatrix}.$$

C'est donc dire que les $i-1$ premières lignes de

$$Z\alpha^\top = \begin{bmatrix} 0 \\ \vdots \\ \beta_i \\ \vdots \\ \beta_n \end{bmatrix}$$

sont nulles et que $z_{i1}\alpha_1 + \cdots + z_{in}\alpha_n > 0$.

Mais alors, le vecteur colonne

$$Z_1\boldsymbol{\beta}^\top = Z_1 Z_2 \boldsymbol{\alpha}^\top$$

est le produit de Z_1 par un vecteur colonne dont les $i-1$ premières lignes sont nulles et la i-ième ligne est un élément strictement positif.

Comme Z_1 est une matrice triangulaire inférieure, les $i-1$ premières lignes de $Z_1\boldsymbol{\beta}^\top$ seront nulles et comme les éléments diagonaux de Z_1 sont strictement positifs, la i-ième ligne de $Z_1\boldsymbol{\beta}^\top$ sera $z_{ii}\beta_i > 0$, pour $i = 1, \cdots, n$.

Ce qui montre que $\boldsymbol{\alpha}$ est aussi un élément positif pour l'ordre $\mathrm{Ord}(Z_1 Z_2)$.

Si on était partie de $\boldsymbol{\alpha} < 0$ pour $\mathrm{Ord}(Z_2)$, on serait quand même arrivé à $\boldsymbol{\alpha} < 0$ pour $\mathrm{Ord}(Z_1 Z_2)$ ce qui montre que ces deux ordres sont égaux. □

Étant donné que le produit de matrices triangulaires inférieures à éléments strictement positifs sur la diagonale est aussi une matrice triangulaire inférieure à éléments strictement positifs sur la diagonale et que l'inverse d'une matrice triangulaire inférieure à éléments diagonaux strictement positifs est d'une part triangulaire inférieure (car les co-facteurs sont au signe près des déterminants de matrices ayant au moins un élément nul sur la diagonale) et d'autre part à éléments diagonaux strictement positifs, on peut définir une relation d'équivalence $\sim$ sur les matrices d'ordres monomiaux en disant que $Z_1 \sim Z_2$ si et seulement si il existe une matrice triangulaire T à éléments diagonaux positifs telle que $Z_1 = TZ_2$.

Montrons que $\sim$ est une bien relation d'équivalence.

- Réflexivité.

  Pour tout Z_1, on devrait avoir $Z_1 \sim Z_1$.

  Par définition de $\sim$,

  $$Z_1 \sim Z_1 \Leftrightarrow Z_1 = TZ_1,$$

  où T est une matrice triangulaire à éléments diagonaux positifs.

  Prenons T la matrice identité, qui est une matrice triangulaire à éléments diagonaux positifs.

  On a bien que $Z_1 \sim Z_1$, donc, $\sim$ est réflexive.

- Symétrie.

  Pour tout Z_1, Z_2, on devrait avoir $Z_1 \sim Z_2 \Rightarrow Z_2 \sim Z_1$.

Par définition de $\sim$,

$$Z_1 \sim Z_2 \Leftrightarrow Z_1 = TZ_2,$$

où T est une matrice triangulaire à éléments diagonaux positifs.

Puisque l'inverse d'une matrice triangulaire à éléments diagonaux positifs est aussi une matrice triangulaire à éléments diagonaux positifs, on a que $Z_2 = \frac{1}{T}Z_1$.

On a alors que $Z_2 \sim Z_1$, donc $\sim$ est symétrique.

- Transitivité.

  Pour tout Z_1, Z_2, Z_3, on devrait avoir $(Z_1 \sim Z_2$ et $Z_2 \sim Z_3) \Rightarrow Z_1 \sim Z_3$.

  Par définition de $\sim$,

$$Z_1 \sim Z_2 \Leftrightarrow Z_1 = TZ_2 \text{ et } Z_2 \sim Z_3 \Leftrightarrow Z_2 = UZ_3,$$

  où T, U sont des matrices triangulaires à éléments diagonaux positifs.

  Puisque le produit de matrices triangulaires à éléments diagonaux positifs est aussi une matrice triangulaire à éléments diagonaux positifs, on a que

$$Z_1 = T(Z_2) = T(UZ_3) = (TU)Z_3.$$

  On a alors que $Z_1 \sim Z_3$, donc $\sim$ est transitive.

Puisque $\sim$ est réflexive, symétrique et transitive, on a bien une relation d'équivalence.

Remarque 2.3. Il faut cependant faire attention, car si on définit la relation d'équivalence $\simeq$ sur les matrices d'ordres monomiaux en disant que $Z_1 \simeq Z_2$ si et seulement si $Ord(Z_1) = Ord(Z_2)$, la proposition précédente ne permet pas de conclure que $\sim$ est $\simeq$, mais seulement que les classes d'équivalence de $\simeq$ sont des réunions de classes d'équivalence de $\sim$.

On peut alors formuler deux questions.

1. Y a-t-il des ordres monoïdaux, et en particulier monomiaux, sur $\mathbb{Q}^n$ qui ne sont pas de la forme Ord(Z) pour une matrice carrée Z non singulière, de rang n, à coefficients entiers ?
2. Peut-on classifier tous les ordres monomiaux sur $\mathbb{Q}^n$?

Nous verrons qu'il y a une réponse positive à ces deux questions. Mais pour le moment, poursuivons l'étude des ordres monomiaux de la forme $\mathrm{Ord}(Z)$.

Proposition 2.4. *Étant donné un ordre monomial donné par une matrice Z non singulière, de rang n, il existe une matrice Z' non singulière, de rang n à coefficients dans $\mathbb{N}$ telle que* $\mathrm{Ord}(Z) = \mathrm{Ord}(Z')$.

Démonstration. Il suffit de trouver une matrice triangulaire T, à coefficients diagonaux strictement positifs, telle que $TZ = Z'$ soit une matrice à coefficients naturels.

Puisque le fait de multiplier une ligne de Z par un élément strictement positif ne change pas l'ordre monomial décrit par la nouvelle matrice obtenue après cette multiplication, on peut supposer que tous les éléments diagonaux de T sont égaux à 1. On trouve ensuite les lignes de T en écrivant, pour la ligne i, les, au plus i, inéquations linéaires qui doivent être satisfaites par les éléments de T.

Ces inéquations commencent toujours par un coefficient positif, car le premier élément non nul de chaque colonne de Z est positif. On isole alors l'inconnue qui a ce coefficient positif.

La condition à satisfaire par cette inconnue est d'être plus grande qu'une autre combinaison linéaire, car le coefficient par lequel on a divisé est positif. Il ne reste plus qu'à donner des valeurs aux autres inconnues pour que les inégalités soient satisfaites. □

Exemple 2.1. Voyons un exemple avec $n = 5$, en prenant la matrice Z qui décrit l'ordre grevlex.

$$Z = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix}.$$

On peut prendre la matrice triangulaire T suivante à coefficients diagonaux strictement

positifs.

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

En les multipliant, on obtient la matrice Z' à coefficients naturels.

$$Z' = TZ = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

La matrice Z' a été obtenue de la matrice Z, décrivant l'ordre monomial grevlex, multipliée par la matrice T, triangulaire inférieure dont les éléments diagonaux sont strictement positifs. La matrice Z' est à nouveau une matrice décrivant l'ordre monomial grevlex.

Exemple 2.2 (Réponse à la question 1). Exemple d'ordre monomial $<$ sur $\mathbb{Q}^2$ qui n'est pas de la forme $\mathrm{Ord}(Z)$ pour une matrice carrée Z non singulière, de rang 2.

On définit l'ensemble P des éléments strictement positifs comme étant

$$P = \{(x, y) \mid \sqrt{2x} + y > 0\}.$$

P est donc l'ensemble des points à coordonnées rationnelles situés au dessus de la droite d'équation $\sqrt{2x} + y = 0$.

Il est clair que $P + P \subseteq P$, et, puisque par l'irrationnalité de $\sqrt{2}$, il n'y a pas de $(x, y) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$ tels que $\sqrt{2x} + y = 0$, on voit tout de suite que $\{P, \{(0, 0)\}, -P\}$ est une partition de $\mathbb{Q}^2$. De plus, puisque $\mathbb{N}^2 \subset P$, on a bien un ordre monomial.

Par ailleurs, montrons que, quelle que soit la matrice non singulière

$$Z = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

où $a, b, c, d \in \mathbb{Q}$, on peut trouver un élément $(x, y) \in \mathbb{Q}^2$ qui est négatif pour $\mathrm{Ord}(Z) = \prec$ et positif pour l'ordre décrit par P, ce qui montrera que ces deux ordres sont distincts.

Voici les différents cas possibles.

- Cas $a > 0$, $b > 0$ et $\frac{a}{b} < \sqrt{2}$.

  Pour que $(x, y) \prec (0, 0)$, il suffit de prendre $x = 1$ et $y < \frac{-a}{b}$ et pour que $(1, y) > (0, 0)$, il suffit de prendre $y > -\sqrt{2}$. Ces deux conditions peuvent se réaliser en prenant $(1, y)$, avec $-\sqrt{2} < y < \frac{-a}{b}$, ce qui est possible par la densité des rationnels.

- Cas $a > 0$, $b > 0$ et $\frac{a}{b} > \sqrt{2}$.

  Pour que $(x, y) \prec (0, 0)$, il suffit de prendre $x = -1$ et $y < \frac{a}{b}$ et pour que $(-1, y) > (0, 0)$, il suffit de prendre $y > \sqrt{2}$. Ces deux conditions peuvent se réaliser en prenant $(-1, y)$, avec $\sqrt{2} < y < \frac{a}{b}$, ce qui est aussi possible par la densité des rationnels.

- Cas $a > 0$ et $b = 0$.

  Pour que $(x, y) \prec (0, 0)$, il suffit que $x < 0$ et pour que $(x, y) > (0, 0)$ avec $x < 0$, il suffit que $\sqrt{2} < \frac{-y}{x}$. Ces deux conditions peuvent se réaliser en prenant par exemple $(-1, 2)$.

- Cas $a > 0$ et $b < 0$.

  Ce cas ne peut pas se produire car Z est une matrice dont le premier élément non nul de chaque colonne est positif.

- Cas $a = 0$ et $b > 0$.

  Pour que $(x, y) \prec (0, 0)$, il suffit que $y < 0$ et pour que $(x, y) > (0, 0)$, il suffit que $x = 1$ et $y > -\sqrt{2}$. Ces deux conditions peuvent se réaliser en prenant $(1, y)$ avec $-\sqrt{2} < y < 0$, ce qui est possible par la densité des rationnels.

- Cas $a = 0$ et $b = 0$. Ce cas ne peut pas se produire car Z est non singulière.

Nous avons donc examiné tous les cas possibles pour la matrice Z et trouvé dans chaque cas un élément strictement négatif pour $\prec$ et strictement positif pour $<$. Ce qui montre que ces ordres sont distincts.

CHAPITRE VIII

CARACTÉRISATION DE WEISPFENNING

Les ordres monomiaux jouent un rôle fondamental dans la définition et la construction de bases de Groebner d'idéaux sur un anneau de polynômes à un nombre fini d'indéterminées. Ces ordres peuvent être interprétés comme des ordres linéaires sur $\mathbb{N}^n$, compatibles avec l'addition et ayant un plus petit élément $(0, \cdots, 0) \in \mathbb{N}^n$.

Dans ce chapitre, nous montrerons l'approche de l'auteur Volker Weispfenning sur la caractérisation de tels ordres monomiaux [1].

1 Généralités sur les corps ordonnés

Lemme 1.1. *Un corps ordonné est toujours de caractéristique nulle.*

Démonstration. Supposons que non et posons $c \in \mathbb{N}$, avec $c \neq 0$, la caractéristique du corps ordonné.

On a que

$$1 > 0,$$

$$1 + 1 > 0,$$

car c'est une somme de $1 > 0$, donc d'éléments positifs,

$$(1 + 1) + 1 > 0,$$

[1] Traduit de l'anglais, dans l'article de Weispfenning, *Admissible orders.*

car c'est une somme d'éléments positifs,

$$\vdots$$

$$\underbrace{1 + \cdots + 1}_{\text{c fois}} = c > 0,$$

car c'est toujours une somme d'éléments positifs.

Mais on aurait du avoir $c = 0$, pour que c soit la caractéristique d'un corps ordonné. Contradiction ! Donc, c ne peut pas être la caractéristique du corps ordonné et par conséquent, un corps ordonné est de caractéristique nulle. □

Corollaire 1.1. *Un corps ordonné contient nécessairement $\mathbb{Q}$, car un corps de caractéristique nulle contient toujours $\mathbb{Q}$ comme plus petit sous-corps.*

Proposition 1.1. *Soit $F = ((C, +, \cdot), Q)$ un corps ordonné.*

Soient $a_1, \cdots, a_n \in F$ tels que pour $(x_1, \cdots, x_n) \in \mathbb{Q}^n$,

$$(a_1x_1 + \cdots + a_nx_n = 0) \Rightarrow (x_1 = \cdots = x_n = 0),$$

c'est-à-dire tels que tous les a_i soient indépendants sur $\mathbb{Q}$.

Alors, en définissant par $>_F$ la relation d'ordre sur F, on a que

$$P = \{(x_1, \cdots, x_n) \in \mathbb{Q}^n \mid a_1x_1 + \cdots + a_nx_n >_F 0\}$$

est l'ensemble des éléments strictement positifs pour un ordre $\prec$ sur $\mathbb{Q}^n$.

De plus, $\prec$ sur $\mathbb{Q}^n$ est un ordre monomial si et seulement si tous les a_i sont positifs, pour $i = 1, \cdots, n$.

Démonstration. Vérifions d'abord la première propriété de P voulant que $\{P, \{0\}, -P\}$ soit une partition de $\mathbb{Q}^n$.

Soit $(x_1, \cdots, x_n) \in \mathbb{Q}^n$, nous avons trois cas possibles.

- Si $\sum_{i=1}^{n} a_ix_i >_F 0$, alors $(x_1, \cdots, x_n) \in P$.

- Si $\sum_{i=1}^{n} a_i x_i <_F 0$, alors $(-x_1, \cdots, -x_n) \in -P$.
- Si $\sum_{i=1}^{n} a_i x_i = 0$, alors $(x_1, \cdots, x_n) = (0, \cdots, 0)$, car les a_i sont indépendants sur $\mathbb{Q}$.

Vérifions maintenant la seconde propriété de P voulant que $P + P \subseteq P$.

Soient $(x_1, \cdots, x_n) \in P$ et $(y_1, \cdots, y_n) \in P$ des éléments positifs.

On a que

$$\sum_{i=1}^{n} a_i x_i >_F 0, \text{ avec } \sum_{i=1}^{n} a_i x_i \in Q$$

et que

$$\sum_{i=1}^{n} a_i y_i >_F 0, \text{ avec } \sum_{i=1}^{n} a_i y_i \in Q.$$

On a aussi que $Q + Q \subset Q$, car F est un corps ordonné. Alors,

$$\sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i y_i \in Q$$

$$\Leftrightarrow \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i y_i >_F 0$$

$$\Leftrightarrow \sum_{i=1}^{n} a_i (x_i + y_i) >_F 0$$

$$\Rightarrow (x_1 + y_1, \cdots, x_n + y_n) \in P.$$

On a donc bien que P est l'ensemble des éléments strictement positifs pour un ordre $\prec$ sur $\mathbb{Q}^n$.

Supposons maintenant tous les a_i positifs, pour $i = 1, \cdots, n$.

Si $(x_1, \cdots, x_n) \in \mathbb{N}^n \setminus \{(0, \cdots, 0)\}$, alors

$$a_1 x_1 + \cdots + a_n x_n >_F 0,$$

car c'est une somme de produits d'éléments positifs qui ne sont pas tous nuls.

En effet, soient $a_i x_i >_F 0$, pour $i = 1, \cdots, n$. Puisque les $a_i x_i$ sont positifs, on a que

$$\sum_{i=1}^{n} a_i x_i >_F 0 \Rightarrow (x_1, \cdots, x_n) \in P.$$

Donc, $\mathbb{N}^n \setminus \{(0,\cdots,0)\} \subseteq P$.

Réciproquement, si $\mathbb{N}^n\setminus\{(0,\cdots,0)\} \subseteq P$, on a en particulier, que $e_i = (0,\cdots,1,\cdots,0) \in \mathbb{N}^n \setminus \{(0,\cdots,0)\}$ est positif, et donc

$$a_1 \cdot 0 + \cdots + a_i \cdot 1 + \cdots + a_n \cdot 0 = a_i >_F 0.$$

Ceci montre bien que $\prec$ sur $\mathbb{Q}^n$ est un ordre monomial. □

2 Lemmes préliminaires

Définition 2.1. *Soit $\prec$ un ordre monoïdal sur $\mathbb{Q}^n$. Soit $(e_1,\cdots,e_n)$ la base canonique de $\mathbb{Q}^n$.*

Nous dirons que $\prec$ est un ordre conditionné [2] *sur $\mathbb{Q}^n$ si*

$$0 \prec e_1 \prec \cdots \prec e_n.$$

Lemme 2.1. *Étant donné $\prec$ un ordre monoïdal sur $\mathbb{Q}^n$, on peut trouver un automorphisme f de $\mathbb{Q}^n$ tel que $f(\prec) = \prec'$ soit un ordre conditionné sur $\mathbb{Q}^n$.*

Illustrons ce lemme par un exemple.

Prenons (e_1,e_2,e_3,e_4,e_5) la base canonique de $\mathbb{Q}^5$, avec un ordre monoïdal $\prec$ sur $\mathbb{Q}^5$ tel que

$$e_5 \prec e_1 \prec 0 \prec e_3 \prec e_2 \prec e_4.$$

On a alors que les éléments $-e_1, e_2, e_3, e_4$ et $-e_5$ sont tous positifs.

Supposons qu'ils sont ordonnés comme suit

$$0 \prec e_3 \prec e_2 \prec -e_5 \prec e_4 \prec -e_1.$$

---

[2] Traduit de l'anglais, *restricted order*.

Un automorphisme de $\mathbb{Q}^5$ étant complètement déterminé par son effet sur les éléments d'une base de $\mathbb{Q}^5$, prenons un automorphisme f défini par

$$\mathbb{Q}^5 \xrightarrow{f} \mathbb{Q}^5$$

$$\begin{aligned} f(e_3) &= e_1 \\ f(e_2) &= e_2 \\ f(-e_5) &= e_3 \\ f(e_4) &= e_4 \\ f(-e_1) &= e_5 \end{aligned}$$

afin que

$$0 \prec' f(e_3) \prec' f(e_2) \prec' f(-e_5) \prec' f(e_4) \prec' f(-e_1),$$

où $\prec'$ est l'ordre sur $\mathbb{Q}^5$ obtenu par transport de $\prec$ le long de f.

On aura alors que $\prec'$ est un ordre conditionné sur $\mathbb{Q}^5$, par définition.

Démonstration. Soit

$$f_i = \begin{cases} e_i & \text{si } e_i > 0 \\ -e_i & \text{si } e_i < 0. \end{cases}$$

On a que $\{f_1, \cdots, f_n\}$ est une base de $\mathbb{Q}^n$.

Puisque $\prec$ est un ordre total sur $\mathbb{Q}^n$, on peut ordonner les f_i comme suit,

$$0 \prec f_{i_1} \prec f_{i_2} \prec \cdots \prec f_{i_n}.$$

Soit

$$\mathbb{Q}^n \xrightarrow{\phi} \mathbb{Q}^n$$

définie par

$$\phi(f_{i_j}) = e_j$$

et

$$\prec' = \{(\alpha, \beta) \in \mathbb{Q}^n \times \mathbb{Q}^n \mid \phi^{-1}(\alpha) \prec \phi^{-1}(\beta)\}.$$

Alors, $\prec'$ est un ordre conditionné sur $\mathbb{Q}^n$. □

Lemme 2.2. *Soient un sous-corps $K \subseteq \mathbb{R}$ tel que $K = \mathbb{Q}(g_1, \cdots, g_{n-1})$, un élément $t \in \mathbb{R}$, un corps ordonné $F = K(t)$ tel que tout élément de K soit strictement inférieur à t, $(t > K)$ et des éléments $1 \leq a_1 \leq \cdots \leq a_n \in K[t]$.*

Alors, t ne peut pas être algébrique sur K.

Illustrons ce lemme par un exemple.

Prenons le polynôme $p(x) = x^2 + bx + c$, avec $a = 1, b, c \in K[t]$ et $x \neq 0$. Prenons $\alpha \in F$ une racine du polynôme $p(x)$.

On a donc que

$$\begin{aligned} \alpha^2 + b\alpha + c &= 0 \\ \alpha^2 &= -b\alpha - c \\ |\alpha|^2 = |-b\alpha - c| &\leq |b||\alpha| + |c| = |\alpha|(|b| + |c||\alpha|^{-1}). \end{aligned}$$

Si $|\alpha| \leq 1$, alors $-1 \leq \alpha \leq 1$.

Si $|\alpha| > 1$, alors $|\alpha|^{-1} < 1$ et donc $|\alpha|^2 \leq |\alpha|(|b| + |c|)$, d'où $|\alpha| \leq (|b| + |c|)$.

Dans les deux cas, $|\alpha| \leq \max(1, |b| + |c|)$. C'est donc dire que

$$-\max(1, |b| + |c|) < \alpha < \max(1, |b| + |c|),$$

avec $-\max(1, |b| + |c|), \max(1, |b| + |c|) \in K$.

On voit alors qu'une racine de polynôme à coefficients dans K est comprise entre deux éléments de K. Cette racine ne peut donc pas être strictement supérieure à tout élément de K.

Par la condition $(t > K)$, t ne peut donc pas être une racine du polynôme $p(x)$. On sait qu'un nombre transcendant sur K est un nombre $\in \mathbb{R}$ (ou $\in \mathbb{C}$) qui n'est racine d'aucun polynôme à coefficients dans K. On a alors que t est un nombre transcendant, il n'est donc pas algébrique sur K, pour un polynôme de degré 2.

Démonstration. Soit le polynôme $p(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + b_k x^k$, avec $b_i \in K[t]$ et $b_k = 1$.

Si t était une racine de ce polynôme, on aurait

$$p(t) = b_0 + b_1 t + \cdots + b_{k-1}t^{k-1} + t^k = 0$$

$$t^k = -b_0 - b_1 t - \cdots - b_{k-1}t^{k-1}.$$

$$|t^k| = |t|^k = |-b_0 - b_1 t - \cdots - b_{k-1}t^{k-1}| \leq |b_0| + |b_1||t| + \cdots + |b_{k-1}||t|^{k-1}$$

$$= |t|^{k-1}(|b_0||t|^{-(k-1)} + |b_1||t|^{-(k-2)} + \cdots + |b_{k-1}|).$$

Si $|t| \leq 1$, alors $-1 \leq t \leq 1$, ce qui est impossible, par la condition $t > K$.

Si $|t| > 1$, alors $|t|^{-1} < 1$. Donc, $|t|^k \leq |t|^{k-1}(|b_0||t|^{k-1} + |b_1||t|^{k-2} + \cdots + |b_{k-1}|)$, d'où $|t| \leq |b_0| + |b_1| + \cdots + |b_{k-1}|$.

Donc,

$$\sum_{j=1}^{k-1} |b_j| \leq t \leq -\sum_{j=1}^{k-1} |b_j|,$$

ce qui impossible, par la condition $t > K$.

t ne peut donc pas être une racine de polynôme. On a alors que t est un nombre transcendant, il n'est donc pas algébrique sur K. □

Proposition 2.1. *Le degré de transcendance des réels sur les rationnels est infini.*

Démonstration. Le corps des éléments algébriques sur $\mathbb{Q}$ est dénombrable.

Plus généralement, le corps des éléments algébriques sur un corps dénombrable est dénombrable, car chaque polynôme de degré n est déterminé par $n+1$ coefficients et il

a un nombre dénombrable de coefficients possibles de degrés 1 à n. De plus, il y a un nombre dénombrable de degrés et chaque polynôme a un nombre fini de racines, ce qui fait un nombre dénombrable de racines de polynômes.

Supposons que K soit le plus petit corps obtenu en ajoutant un élément transcendant t à un sous-corps dénombrable F de $\mathbb{R}$. K est alors égal au corps formé des expressions $\frac{f(t)}{g(t)}$, où f et g sont des polynômes à coefficients dans K, avec $g \neq 0$. Ceci est possible, car tout corps contenant K et t contient les $\frac{f(t)}{g(t)}$ et l'ensemble de ces $\frac{f(t)}{g(t)}$ est un corps, donc, ce corps est le plus petit corps contenant K et t.

Puisqu'il y a un nombre dénombrable de tels polynômes, le corps K est dénombrable.

Remarquons que le degré de transcendance de $\mathbb{R}$ sur $\mathbb{Q}$ est infini non dénombrable, car après un nombre dénombrable de telles extensions, on a toujours un corps dénombrable.

□

Lemme 2.3. *Pour tout ordre conditionné $\prec$ sur $\mathbb{Q}^n$ dont P est l'ensemble des éléments strictement positifs, il existe un sous-corps $K \subseteq \mathbb{R}$, tel que $K = \mathbb{Q}(g_1, \cdots, g_{n-1})$, un élément $t \in \mathbb{R}$, un corps ordonné $F = K(t)$ tel que tout élément de K soit strictement inférieur à t et des éléments $1 \leq a_1 \leq \cdots \leq a_n \in K[t]$ tels qu'en définissant par $>_F$ la relation d'ordre sur F et avec $(x_1, \cdots, x_n) \in \mathbb{Q}^n$, on a que*

$$(a_1x_1 + \cdots + a_nx_n >_F 0) \Rightarrow (x_1, \cdots, x_n) \in P.$$

Démonstration. Si $n = 1$, on a

1. $0 \prec e_1 = 1$, car e_1 est la base canonique de $\mathbb{Q}^1$,
2. $K = \mathbb{Q}$, car $K = \mathbb{Q}(g_1, \cdots, g_{n-1})$, avec $n - 1 = 0$ générateur ajouté,
3. $a_1 \geq 1 \in K[t] = \mathbb{Q}(t)$.

Alors,

$$(1x_1 >_F 0) \Rightarrow (x_1 \in P).$$

Ici, on ne connaît pas explicitement P mais il suffit de montrer que le seul P possible soit $\mathbb{Q}_+^*$, car on a une seule structure de groupe ordonné sur $\mathbb{Q}^1$ telle que $\mathbb{N}^* \subseteq P$.

Voyons d'abord que $P \subseteq \mathbb{Q}_+^*$.

Soit $\frac{p}{q} \in \mathbb{Q}_+^*$. Sans perte de généralité, on peut supposer que $q > 0$, alors $p > 0$.

Montrons que $\frac{p}{q} \in P$.

Sinon, puisque $\frac{p}{q} \neq 0$, on aurait $\frac{p}{q} \in -P$, c'est-à-dire $\frac{p}{q} < 0$. Alors, $\underbrace{(\frac{p}{q} + \cdots + \frac{p}{q})}_{\text{q fois}} = p <$ 0. Contradiction !

Donc, $P \subseteq \mathbb{Q}_+^*$.

Voyons ensuite que $P \supseteq \mathbb{Q}_+^*$.

Si $\frac{p}{q} \in \mathbb{Q}_+^*$, avec $q > 0$, donc $p > 0$, alors

$$p > 0 \Leftrightarrow \frac{p}{q} \in P.$$

Si $\frac{p}{q} \notin \mathbb{Q}_+^*$, on aurait $\frac{p}{q} \in -P$. Donc, $\underbrace{(\frac{p}{q} + \frac{p}{q} + \cdots + \frac{p}{q})}_{\text{q fois}} = p \in -P$, car une somme d'éléments de $-P$ est dans $-P$.

Hors, $p \in \mathbb{N}^* \subset P$. On aurait donc que $p \in (P \cap -P)$, contradiction, car $\{P, \{0\}, -P\}$ doit être une partition de $\mathbb{Q}$. Donc, $P \supseteq \mathbb{Q}_+^*$.

Ceci montre que $P = \mathbb{Q}_+^*$.

Voilà pour $n = 1$.

Supposons maintenant $n > 1$.

On a un ordre conditionné $\prec$ sur $\mathbb{Q}^n$, avec $0 \prec e_1 \prec \cdots \prec e_n$, où $(e_1, \cdots, e_n)$ est la base canonique de $\mathbb{Q}^n$. Plongeons $\mathbb{Q}^{n-1}$ dans $\mathbb{Q}^n$ comme suit

$$\begin{array}{ccc} \mathbb{Q}^{n-1} & \xrightarrow{h} & \mathbb{Q}^n \\ (x_1, \cdots, x_{n-1}) & \mapsto & (x_1, \cdots, x_{n-1}, 0) \end{array}$$

et restreignons-nous à $\mathbb{Q}^{n-1}$.

Soient $\prec'$ un ordre sur $\mathbb{Q}^{n-1}$ tel que $w \prec' v$ si et seulement si $h(w) \prec h(v)$, avec $w, v \in \mathbb{Q}^{n-1}$, P' l'ensemble des éléments positifs

$$P' = \{(x_1, \cdots, x_{n-1}) \mid (x_1, \cdots, x_{n-1}, 0) \in P\}$$

et $(e'_1, \cdots, e'_{n-1})$ la base canonique de $\mathbb{Q}^{n-1}$.

Par définition de $\prec'$, on a que $0 \prec' e'_1 \prec' \cdots \prec' e'_{n-1}$. Il est donc facile de voir que $\prec'$ est un ordre conditionné sur $\mathbb{Q}^{n-1}$.

Dans $\mathbb{Q}^n$, on identifie P' à $\{(x_1, \cdots, x_n) \in P \mid x_n = 0\}$.

Par hypothèse de récurrence, il existe un sous-corps $K' \subseteq \mathbb{R}$, tel que $K' = \mathbb{Q}(g_1, \cdots, g_{n-2})$, un élément $t \in \mathbb{R}$, un corps ordonné $F' = K'(t)$ et des éléments $1 \leq a_1 \leq \cdots \leq a_{n-1} \in K'[t]$.

Posons $\mathcal{A} = \{q \in \mathbb{Q} \mid qe_{n-1} = (0, \cdots, q, 0) \prec (0, \cdots, 0, 1) = e_n\}$.

1. Si $\mathcal{A} \neq \varnothing$, alors il existe un minorant de $\mathcal{A}$. On peut prendre n'importe quel $q < 1$, $q \in \mathbb{Q}$, car $e_{n-1} \prec e_n$. Donc, il existe un plus grand minorant de $\mathcal{A}$ dans $\mathbb{R}$ qui, par définition, est l'infimum de $\mathcal{A}$ (noté $\inf(\mathcal{A})$) et comme aucun $q < 1$ n'est élément de $\mathcal{A}$, on a que $\inf(\mathcal{A}) \geq 1$.

   Posons $b = \inf(\mathcal{A})$ et $K = K'(b)$.

2. Si $\mathcal{A} = \varnothing$, alors $K[t] = K'[t]$ et $b = t$.

Dans les deux cas, posons $a_n = a_{n-1}b$.

Dans le cas où $\mathcal{A} \neq \varnothing$, on a $K[t]$ avec $K = \mathbb{Q}(g_1, \cdots, g_{n-1}, b)$, car $K = K'(b)$ et dans le cas où $\mathcal{A} = \varnothing$, on a $b = t$ et $K[t] = K'[t]$, avec $K' = \mathbb{Q}(g_1, \cdots, g_{n-2})$.

Remarque 2.1. Dans le premier cas, $b \geq 1$, alors $a_n = a_{n-1}b \geq a_{n-1}$.

Dans le deuxième cas, $b = t > a_{n-1}$, alors $a_n = a_{n-1}b = a_{n-1}t > a_{n-1}$.

Il reste à voir que les a_i ainsi construits dans le corps F, satisfont la condition du lemme voulant qu'en supposant que $\sum_{i=1}^{n} a_i x_i >_F 0$, on puisse conclure que $(x_1, \cdots, x_n) \in P$.

Voyons tous les cas possibles.

- Si $x_n = 0$, alors

$$(x_1, \cdots, x_n) = (x_1, \cdots, x_{n-1}, 0)$$

et

$$(\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n-1} a_i x_i >_F 0) \Rightarrow (x_1, \cdots, x_{n-1}) \in P',$$

par hypothèse de récurrence. D'où $(x_1, \cdots, x_n) \in P$.

- Si $\mathcal{A} = \varnothing$ et $x_n \neq 0$, alors on sait que $b = t$ et que $a_n = a_{n-1}t$. Donc,

$$\left.\begin{array}{r} (t >_F \frac{a_1x_1+\cdots+a_{n-1}x_{n-1}}{x_n}) \\ (t <_F -(\frac{a_1x_1+\cdots+a_{n-1}x_{n-1}}{x_n})) \end{array}\right\} \Rightarrow t >_F |\frac{a_1x_1 + \cdots + a_{n-1}x_{n-1}}{x_n}|,$$

d'où

$$|a_nx_n| = |a_{n-1}tx_n| \geq_F |tx_n| >_F |a_1x_1 + \cdots + a_{n-1}x_{n-1}|, \tag{8.1}$$

car $a_i \geq 1$, pour $i = 1, \cdots, n$.

On en vient à deux sous-cas du cas $\mathcal{A} = \varnothing$.

- Si $x_n < 0$, alors $a_nx_n <_F 0$, car $a_n > 0$. On aurait donc que

$$|a_nx_n| = -a_nx_n >_F |a_1x_1 + \cdots + a_{n-1}x_{n-1}| \geq_F (a_1x_1 + \cdots + a_{n-1}x_{n-1}),$$

c'est-à-dire que

$$0 >_F a_1x_1 + \cdots + a_nx_n >_F 0,$$

par (8.1) d'une part et par hypothèse de récurrence d'autre part. Contradiction ! Donc, x_n doit être positif.

- Si $x_n > 0$, alors

$$(\frac{-x_1e_1}{x_n} + \cdots + \frac{-x_{n-1}e_{n-1}}{x_n}) \leq (\frac{|x_1|}{x_n}e_{n-1} + \cdots + \frac{|x_{n-1}|}{x_n}e_{n-1}) \leq e_n,$$

car $\mathcal{A} = \varnothing$.

Ceci implique que

$$(-x_1e_1 - \cdots - x_{n-1}e_{n-1}) \leq x_ne_n.$$

Donc,

$$x_ne_n - (-x_1e_1 - \cdots - x_{n-1}e_{n-1}) = \sum_{i=1}^{n} x_ie_i \geq 0.$$

L'inégalité ci-dessus doit être stricte, car sinon tous les x_i seraient nuls et on est dans le cas où $x_n > 0$.

Donc, on a que

$$(x_1, \cdots, x_n) = \sum_{i=1}^{n} x_i e_i \in P.$$

Il nous reste le cas $\mathcal{A} \neq \varnothing$.

- Si $\mathcal{A} \neq \varnothing$ et $x_n \neq 0$, alors on a comme hypothèse que $a_1 x_1 + \cdots + a_n x_n >_F 0$, avec $a_n = a_{n-1} b$.

Soit

$$\begin{array}{ccc} K & \xrightarrow{f} & K' \\ q & \mapsto & f(q) = a_1 x_1 + \cdots + a_{n-1} x_{n-1} + a_{n-1} q x_n. \end{array}$$

Soit $d = \max(\deg(a_i(t)), i = 1, \cdots, n-2)$.

- Si $\deg(a_{n-1}(t)) \leq d$, alors il existe $0 < q < b < q'$, avec $q, q' \in \mathbb{Q}$ tels que $f(q) >_F 0$ et $f(q') >_F 0$.
- Si $\deg(a_{n-1}(t)) > d$, alors $x_n > 0$.

Puisque $q < b = \inf(\mathcal{A})$, alors $q \notin \mathcal{A}$, donc, $q e_{n-1} \preceq e_n$.

Puisque $q' > b = \inf(\mathcal{A})$, alors $q' \in \mathcal{A}$, donc $q' e_{n-1} \succ e_n$.

On a

$$f(b) = a_1(t) x_1 + \cdots + a_{n-2}(t) x_{n-2} + a_{n-1}(t)(x_{n-1} + b x_n),$$

un polynôme de degré d.

Soit a le coefficient du terme de plus haut degré dans $f(b)$.

- Si $\deg(a_{n-1}(t)) \leq d$, alors a est de la forme

$$a = c + x_{n-1} + b x_n,$$

où c est la somme des coefficients des termes de plus haut degré dans les termes $a_i(t) x_i$, pour $i = 1, \cdots, n-2$. Le coefficient a est dans $\mathbb{R}_+^*$ et c'est lui qui déterminera le signe de $f(b)$.

$$a = c + x_{n-1} + b x_n > 0.$$

Si on augmente ou diminue légèrement b, a sera encore positif. Sous forme d'équation d'une droite,

$$a = x_n b + (c + x_{n-1}),$$

où x_n est la pente de la droite et $(c + x_{n-1})$ l'ordonnée à l'origine.

- Si $\deg(a_{n-1}(t)) > d$, alors a est de la forme

$$a = c(x_{n-1} + bx_n),$$

où c est le coefficient du terme $a_{n-1}(t)(x_{n-1} + bx_n)$. Le coefficient a est dans $\mathbb{R}_+^*$ et c'est lui qui déterminera le signe de $f(b)$.

$$a = c(x_{n-1} + bx_n) > 0.$$

Si on augmente ou diminue légèrement b, a sera encore positif. Sous forme d'équation d'une droite,

$$a = cx_{n-1} + cbx_n = (cx_n)b + (cx_{n-1}),$$

où cx_n est la pente de la droite et (cx_{n-1}) l'ordonnée à l'origine.

Cela montre l'existence des $q, q' \in \mathbb{Q}$ en terme de variation de b.

On en vient à deux sous-cas du cas $\mathcal{A} \neq \varnothing$.

- Si $x_n > 0$, alors puisqu'on a $qe_{n-1} \preceq e_n$, on aura $x_n qe_{n-1} \preceq x_n e_n$. D'où

$$(x_1e_1 + \cdots + x_ne_n) \succeq (x_1e_1 + \cdots + x_{n-1}e_{n-1} + x_nqe_{n-1}) \in P,$$

par hypothèse de récurrence, car $f(q) = a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_{n-1}qx_n >_F 0$.

- Si $x_n < 0$, alors puisqu'on a $q'e_{n-1} \succ e_n$, on aura $x_nq'e_{n-1} \prec x_ne_n$. D'où

$$(x_1e_1 + \cdots + x_ne_n) \succ (x_1e_1 + \cdots + x_{n-1}e_{n-1} + x_nq'e_{n-1}) \in P,$$

par hypothèse de récurrence, car $f(q') = a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_{n-1}q'x_n >_F 0$.

□

3 Classification proprement dite

Le théorème suivant se veut la réciproque de la proposition 1.1..

Théorème 3.1. *Soit un ordre $\prec$ sur $\mathbb{Q}^n$ dont P est l'ensemble des éléments strictement positifs.*

Alors, il existe un corps ordonné F et des éléments $a_1, \cdots, a_n \in F$, tels que pour $(x_1, \cdots, x_n) \in \mathbb{Q}^n$,

$$(a_1x_1 + \cdots + a_nx_n = 0) \Rightarrow (x_1 = \cdots = x_n = 0),$$

c'est-à-dire que tous les a_i soient indépendants sur $\mathbb{Q}$.

En définissant par $>_F$ la relation d'ordre sur F, on a que

$$P = \{(x_1, \cdots, x_n) \in \mathbb{Q}^n \mid a_1x_1 + \cdots + a_nx_n >_F 0\}.$$

Démonstration. Par le lemme 2.1., nous pouvons supposer, sans perte de généralité, que $\prec$ est un ordre conditionné sur $\mathbb{Q}^n$.

Par le lemme 2.3., il existe un corps ordonné $F = K(t)$ et des éléments $1 \leq a_1 \leq \cdots \leq a_n \in K[t]$, avec $K = \mathbb{Q}(g_1, \cdots, g_{n-1})$, tels que

$$(a_1x_1 + \cdots + a_nx_n >_F 0) \Rightarrow (x_1, \cdots, x_n) \in P.$$

Posons

$$\mathcal{E} = \{(x_1, \cdots, x_n) \in \mathbb{Q}^n \mid \sum_{i=1}^{n} a_ix_i = 0\}$$

et $s = \dim(\mathcal{E})$, avec $s < n$.

Il est facile de voir que $\mathcal{E}$ est un espace vectoriel. Cet espace vectoriel n'est pas $\mathbb{Q}^n$ au complet, car il suffit de prendre un élément de $\mathcal{E}$ satisfaisant la condition $\sum_{i=1}^{n} a_ix_i \neq 0$.

Sachant que $a_1 \geq 1$, par le lemme 2.3., prenons simplement $(1, 0, \cdots, 0) \in \mathcal{E}$, qui satisfait cette condition.

Soient les bases $\mathbf{b_1} = (b_{11}, \cdots, b_{n1}), \cdots, \mathbf{b_s} = (b_{1s}, \cdots, b_{ns})$ de $\mathcal{E}$, avec $(0, \cdots, 0) < \mathbf{b_1} < \cdots < \mathbf{b_s}$.

Soit

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\phi} & \mathbb{Q}^s \\ b_i & \mapsto & e_i, \end{array}$$

où e_i est le i-ième élément de la base canonique $(e_1, \cdots, e_s)$ de $\mathbb{Q}^s$.

Munissons $\mathbb{Q}^s$ de la structure de groupe ordonné $(\mathbb{Q}^s, P')$ obtenue par transport de structure le long de F de la structure de groupe ordonné de $\mathcal{E}$. Autrement dit,

$$(q_1, \cdots, q_s) \in P' \Leftrightarrow \sum_{i=1}^{s} q_i b_i \in P.$$

Soit

$$\begin{array}{ccc} \mathbb{Q}^s & \xrightarrow{\psi} & \mathbb{Q}^n \\ q_1 b_1 + \cdots + q_s b_s & \mapsto & q_1 b_1 + \cdots + q_s b_s + 0 + \cdots + 0. \end{array}$$

Par hypothèse de récurrence, il existe un corps ordonné F' et des éléments $a'_1, \cdots, a'_s \in F'$, tels que pour $(x'_1, \cdots, x'_s) \in \mathbb{Q}^s$,

$$(a'_1 x'_1 + \cdots + a'_s x'_s = 0) \Rightarrow (x'_1 = \cdots = x'_s = 0),$$

c'est-à-dire que tous les a'_i soient indépendants sur $\mathbb{Q}$.

En définissant par $>_{F'}$ la relation d'ordre sur F', on a que

$$P' = \{(x'_1, \cdots, x'_s) \in \mathbb{Q}^s \mid a'_1 x'_1 + \cdots + a'_s x'_s >_{F'} 0\}.$$

Maintenant, soit

$$\begin{aligned} (d_1, \cdots, d_n) \cdot (x_1, \cdots, x_n) &= (a_1, \cdots, a_n)\phi(x_1, \cdots, x_n) \\ d_1 x_1 + \cdots + d_n x_n &= a_1 \phi(x_1) + \cdots + a_n \phi(x_n), \end{aligned}$$

avec $(d_1, \cdots, d_n) \in F'$, tel que

$$(d_1 x_1 + \cdots + d_n x_n = 0) \Rightarrow (x_1 = \cdots = x_n = 0),$$

c'est-à-dire que tous les d_i soient indépendants sur $\mathcal{E}$.

Soit B la matrice dont les colonnes sont les coordonnées de $\mathbf{b_1}, \cdots, \mathbf{b_s}$ de $\mathcal{E}$.

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1s} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{ns} \end{bmatrix}$$

Cette matrice est de rang s, on peut la multiplier à gauche, par une matrice inversible M $(n \times n)$ qui est un produit de matrices-lignes élémentaires.

On aura donc que $MB = I_0$, avec

$$I_0 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix},$$

qui est la forme échelonnée-réduite de la matrice B.

On a

$$M = \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & & \vdots \\ m_{s1} & \cdots & m_{sn} \\ m_{s+1,1} & \cdots & m_{s+1,n} \\ \vdots & & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix}.$$

On a donc

$$\begin{aligned} M(x_1, \cdots, x_n) &= MB(q_1, \cdots, q_s) \\ &= I_0(q_1, \cdots, q_s) \\ &= (q_1, \cdots, q_s, 0, \cdots, 0), \end{aligned}$$

et donc,

$$\begin{aligned} a'_1q_1 + \cdots + a'_sq_s &= a'_1(Mx_1) + \cdots + a'_s(Mx_n) \\ &= a'_1(m_{11}x_1 + \cdots + m_{1n}x_n) + \cdots + a'_s(m_{s1}x_1 + \cdots + m_{sn}x_n) + 0 + \cdots + 0 \\ &= (a'_1m_{11} + \cdots + a'_sm_{s1})x_1 + \cdots + (a'_1m_{1n} + \cdots + a'_sm_{sn})x_n \\ &= d_1x_1 + \cdots + d_nx_n. \end{aligned}$$

Nous avons alors trouvé nos d_i, avec $i = 1, \cdots, n$, qui sont non nuls, à moins que tous les x_i le soient.

Considérons maintenant $c_i = d_i + a_it$, pour $i = 1, \cdots, n$. Alors,

$$(c_1x_1 + \cdots + c_nx_n = 0) \Rightarrow (x_n = \cdots = x_n = 0),$$

c'est-à-dire que tous les c_i sont indépendants sur $\mathbb{Q}$, puisque

$$(c_1x_1 + \cdots + c_nx_n = 0) \Rightarrow (d_1x_1 + \cdots + d_nx_n + (a_1x_1 + \cdots + a_nx_n)t = 0).$$

On a

$$a_1x_1 + \cdots + a_nx_n = 0 = d_1x_1 + \cdots + d_nx_n$$

et donc $(x_1, \cdots, x_n) \in \mathcal{E}$, d'une part et $(x_1, \cdots, x_n) = (0, \cdots, 0)$ d'autre part.

Plus encore, si $c_1x_1 + \cdots + c_nx_n > 0$, alors $a_1x_1 + \cdots + a_nx_n >_F 0$, ou alors $a_1x_1 + \cdots + a_nx_n = 0$ et $d_1x_1 + \cdots + d_nx_n > 0$.

Dans le premier cas, $(x_1, \cdots, x_n) \in P$, par le lemme 2.3.

Dans le deuxième cas, $a_1\phi(x_1) + \cdots + a_n\phi(x_n) > 0$, et donc $\phi(x_1, \cdots, x_n) \in P'$ et on a bien que $(x_1, \cdots, x_n) \in P$. □

CHAPITRE IX

CLASSIFICATION DE ROBBIANO

Dans la présente section, nous voulons caractériser tous les ordres monoïdaux sur $\mathbb{Q}^n$ et parmi ceux-ci, les ordre monomiaux.

Nous montrerons l'approche de l'auteur Lorenzo Robbiano sur la caractérisation des ordres monomiaux [1]. Pour ce faire, nous allons plonger $\mathbb{Q}^n$ dans $\mathbb{R}^n$.

1 Rappel de topologie sur les réels

Précisons qu'il n'est pas nécessaire, ici, de connaître les définitions générales d'espace de Hilbert, d'espace normé, d'espace métrique et d'espace topologique pour lire cette présente section.

Munissons $\mathbb{R}^n$ du produit scalaire usuel, ce qui fera de $(\mathbb{R}^n, \cdot)$ un espace de Hilbert :

$$\boldsymbol{\alpha} \cdot \boldsymbol{\beta} = (\alpha_1, \cdots, \alpha_n) \cdot (\beta_1, \cdots, \beta_n) = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n.$$

À l'aide de ce produit scalaire, nous pouvons définir une norme $\| - \|$ qui fera de $(\mathbb{R}^n, \| - \|)$ un espace normé :

$$\|\boldsymbol{\alpha}\| = \sqrt{\boldsymbol{\alpha} \cdot \boldsymbol{\beta}} = \sqrt{\alpha_1^2 + \cdots + \alpha_n^2}.$$

À l'aide de cette norme, nous pouvons définir une distance d qui fera de $(\mathbb{R}^n, d)$ un

---

[1] Traduit de l'anglais, dans l'article de Robbiano, *Term ordering*.

espace métrique :

$$d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \|\boldsymbol{\alpha} - \boldsymbol{\beta}\|.$$

À l'aide de cette distance, nous pouvons définir une topologie $\mathcal{T}$ qui fera de $(\mathbb{R}^n, \mathcal{T})$ un espace topologique :

$$\mathcal{T} = \{U \subseteq \mathbb{R}^n \mid (\forall \boldsymbol{\alpha} \in U)(\exists \epsilon \in \mathbb{R})(\{\boldsymbol{\beta} \in \mathbb{R}^n \mid d(\boldsymbol{\alpha}, \boldsymbol{\beta}) < \epsilon\} \subseteq U)\}.$$

Un élément de $\mathcal{T}$ est appelé un ouvert de $\mathbb{R}^n$. À titre d'exemple, $\varnothing$ et $\mathbb{R}^n$ sont des ouverts de $\mathbb{R}^n$.

Définition 1.1. *Un voisinage d'un point $\boldsymbol{\alpha} \in \mathbb{R}^n$ est un ensemble E tel qu'il existe un ouvert U de $\mathbb{R}^n$ avec*

$$\boldsymbol{\alpha} \in U \subseteq E.$$

Pour un point $\boldsymbol{\alpha} \in \mathbb{R}^n$, on note $\mathcal{V}(\boldsymbol{\alpha})$ l'ensemble des voisinages de α.

Définition 1.2. *L'adhérence $\overline{E}$ d'un sous-ensemble E de $\mathbb{R}^n$ est l'ensemble des points de $\mathbb{R}^n$ dont tout voisinage a une intersection non vide avec E.*

L'adhérence de E est aussi appelée la fermeture de E.

Proposition 1.1. $\overline{\mathbb{Q}^n} = \mathbb{R}^n$.

C'est-à-dire l'ensemble des réels est l'adhérence de l'ensemble des rationnels.

Démonstration. Voir (Mercier, 2006) page 86. □

Définition 1.3. *Un sous-ensemble E de $\mathbb{R}^n$ est dit disconnexe s'il existe deux ouverts U_1 et U_2 de $\mathbb{R}^n$ tels que*

$$(U_1 \cap E \neq \varnothing) \text{ et } (U_2 \cap E \neq \varnothing) \text{ et } (U_1 \cap U_2 \cap E = \varnothing).$$

E est connexe s'il n'est pas disconnexe.

Définition 1.4. *Un sous-ensemble E de $\mathbb{R}^n$ est dit connexe par arcs si deux points quelconques p et q de E peuvent être reliés par un chemin entièrement dans E, autrement dit, s'il existe une fonction continue*

$$\begin{array}{ccc} [0,1] & \xrightarrow{\gamma} & E \\ c & \mapsto & \gamma(c) \end{array}$$

telle que $\gamma(0) = p$ et $\gamma(1) = q$.

Proposition 1.2. *Si un sous-ensemble E de $\mathbb{R}^n$ est connexe par arcs, alors il est connexe.*

Démonstration. Voir (Ramis, 1998) page 76. □

2 Lemmes préliminaires

Lemme 2.1. *Si W est un sous-espace vectoriel de dimension k, d'un espace vectoriel V de dimension r, de $\mathbb{R}^n$ et si $k \leq r-2$, alors $V \setminus W$ est connexe par arcs.*

Démonstration. Prenons une base $(b_1, \cdots, b_k)$ de W et prolongeons-là en une base $\mathcal{B} = (b_1, \cdots, b_r)$ de V.

Soient

$$p = \lambda_1 b_1 + \cdots + \lambda_k b_k + \lambda_{k+1} b_{k+1} + \cdots + \lambda_r b_r$$

$$q = \mu_1 b_1 + \cdots + \mu_k b_k + \mu_{k+1} b_{k+1} + \cdots + \mu_r b_r$$

deux points de $V \setminus W$, donc, dans le complément de W, où $(\lambda_1, \cdots, \lambda_r)$ et $(\mu_1, \cdots, \mu_r)$ sont dans $\mathbb{R}^r$.

Il y a au moins un indice u et un indice v dans $\{k+1, \cdots, r\}$ tels que $\lambda_u \neq 0$ et $\lambda_v \neq 0$. Il s'agit de trouver un chemin de p à q, à toute étape duquel au moins un des indices entre $k+1$ et r est non nul. Il se peut qu'on doive prendre $u = v$ si toutes les autres coordonnées d'indice supérieur à $k+1$ en base $\mathcal{B}$ de p et q sont nulles.

Posons

$$p' = \sum_{\substack{1\leq j\leq r\\ j\notin\{u,v\}}} \lambda_j b_j \text{ et } q' = \sum_{\substack{1\leq j\leq r\\ j\notin\{u,v\}}} \mu_j b_j.$$

- Si $u \neq v$, on peut prendre le chemin γ suivant de p à q entièrement dans $V \setminus W$:

$$\gamma(t) = (1-t)p' + tq' + \begin{cases} \lambda_u b_u + ((1-2t)\lambda_v + 2t\mu_v)b_v & \text{si } 0 \leq t \leq \frac{1}{2} \\ (1-2(t-\frac{1}{2}))\lambda_u b_u + 2(t-\frac{1}{2})\mu_u b_u + \mu_v b_v & \text{si } \frac{1}{2} \leq t \leq 1. \end{cases}$$

- Si $u = v$ et que toutes les autres coordonnées en base $\mathcal{B}$ d'indice supérieur à k de p et q sont nulles, alors on prend un indice $w \neq u$ dans $\{k+1, \cdots, r\}$ et on fabrique un chemin dont on s'assure qu'il a, sur toute sa longueur, la composante d'indice w non nulle lorsque celle d'indice u est nulle (afin qu'il ne pénètre pas dans W).

  Par exemple,

$$\gamma(t) = (1-t)p' + tq' + \begin{cases} (1-2t)\lambda_u b_u + 2tb_w & \text{si } 0 \leq t \leq \frac{1}{2} \\ 2(t-\frac{1}{2})\mu_u b_u + (1-2(t-\frac{1}{2}))b_w & \text{si } \frac{1}{2} \leq t \leq 1. \end{cases}$$

Nous allons, de plus, considérer $\mathbb{R}^n$ comme un espace vectoriel sur le corps $\mathbb{Q}$. Pour un sous-$\mathbb{Q}$-espace vectoriel G de $\mathbb{Q}^n$, de dimension r, notons

$$G_{\mathbb{R}} = \{\sum_{j=1}^{s} \lambda_j \alpha_j \mid \lambda_j \in \mathbb{R}, \alpha_j \in G \text{ et } s \in \mathbb{N}\},$$

le sous-$\mathbb{R}$-espace vectoriel de $\mathbb{R}$ engendré par G.

À titre d'exemple, si G est le sous-$\mathbb{Q}$-espace vectoriel de dimension 2 de $\mathbb{Q}^3$ engendré par $(1,0,0)$ et $(0,1,0)$, alors $G_{\mathbb{R}}$ est le plan d'équation $z = 0$ de $\mathbb{R}^3$. □

Proposition 2.1. *Les éléments de la base $\mathcal{B} = (b_1, \cdots, b_r)$ engendrent $G_{\mathbb{R}}$, par définition.*

$b_1, \cdots, b_r$ sont linéairement indépendants sur $\mathbb{R}$, car la matrice des coordonnées de $(b_1, \cdots, b_r)$ est une matrice de rang r et ceci, indépendamment du corps dans lequel les éléments de la matrice sont plongés.

Démonstration. Le fait que la matrice $r \times n$ des coordonnées des b_i, pour $i = 1, \cdots, r$ soit de rang r, en tant que matrice à coefficients dans $\mathbb{Q}$, implique qu'elle soit de rang r comme matrice à coefficients dans $\mathbb{R}$ (c'est la même matrice !) et donc $(b_1, \cdots, b_r)$ est aussi une base de $G_{\mathbb{R}}$. □

Pour la suite de ce chapitre, nous supposerons $\mathbb{Q}^n$ muni d'une structure de groupe ordonné dont l'ensemble des éléments strictement positifs est P.

Lemme 2.2. *Un multiple rationnel strictement positif $\frac{a}{b}$, avec $b > 0$, d'un élément de P est encore un élément de P.*

Un multiple rationnel strictement négatif $\frac{a}{b}$, avec $b > 0$, d'un élément de P est un élément de $-P$.

Démonstration. On a deux cas.

- Cas $a > 0$.

  Soit $p \in P$. Si $\frac{1}{b}p \notin P$, alors $\frac{1}{b}p \in -P$ et comme la somme d'éléments de $-P$ est dans $-P$, on aurait que p, qui est la somme de a termes égaux à $\frac{1}{b}p$, serait un élément de $-P$. Contradiction ! Ensuite $\frac{a}{b}p \in P$, car c'est la somme de a éléments de P, tous égaux à $\frac{1}{b}p$.
- Cas $a < 0$.

  On a que $\frac{-a}{b}p \in P$, par ce qu'on vient de voir. Donc $\frac{a}{b}p = -\frac{-a}{b}p \in -P$.

□

Théorème 2.1. *Soit G un sous-espace vectoriel de $\mathbb{Q}^n$ de dimension r, et soit I_G l'ensemble des points de $G_{\mathbb{R}}$ dont tout voisinage contient un élément strictement positif de G et un élément strictement négatif de G.*

Alors I_G est un sous-$\mathbb{R}$-espace vectoriel de $G_{\mathbb{R}}$ de dimension $r - 1$,

$$I_G = \{p \in G_{\mathbb{R}} \mid (\forall U \in \mathcal{V}(p))(U \cap P \cap G_{\mathbb{R}} \neq \varnothing \text{ et } U \cap -P \cap G_{\mathbb{R}} \neq \varnothing\}.$$

Démonstration. Montrons d'abord que I_G est un sous-$\mathbb{R}$-espace vectoriel de $G_{\mathbb{R}}$.

On a que $\mathbf{0} = (0, \cdots, 0) \in I_G$. En effet, tout voisinage U de $\mathbf{0}$ contient un voisinage de la forme

$$V = \mathcal{B}_{G_{\mathbb{R}}}(\mathbf{0}\,;\,\delta) = \{\boldsymbol{\alpha} \in G_{\mathbb{R}} \mid \|\alpha\| < \delta\}$$

et V contient au moins un point p à coordonnées rationnelles autre que $\mathbf{0}$, car $\overline{\mathbb{Q}^n} = \mathbb{R}^n$ et $G_{\mathbb{R}}$ est un espace vectoriel, donc $\mathbf{0} \in G_{\mathbb{R}}$.

Si $p \in P$ alors $-p \in -P$. Mais comme, par définition de V, $-p \in V$, on a que $\mathbf{0} \in I_G$.

Soient p et q deux éléments de I_G et soit U un voisinage de $p+q$. L'image inverse de $p+q$ par l'application continue

$$\mathbb{R}^n \times \mathbb{R}^n \xrightarrow{+} \mathbb{R}^n$$

est un voisinage V de (p,q) et il existe alors des voisinages V_p de p et V_q de q dans $\mathbb{R}^n$ tels que $V \supseteq V_p \times V_q$.

Soient $p_+ \in (V_p \cap P \cap G_{\mathbb{R}})$ et $q_+ \in (V_q \cap P \cap G_{\mathbb{R}})$. On a que

$$(p_+, q_+) \in V_p \times V_q \subseteq V$$

et par définition de V, $p_+ + q_+ \in U$. Mais $p_+ + q_+ \in P + P \subseteq P$ et donc, le voisinage arbitraire U de $p+q$ contient un élément de $P \cap G_{\mathbb{R}}$.

Semblablement, on montre que U contient un élément de $-P$, ce qui montre que $p+q \in I_G$, c'est-à-dire que I_G est stable sous la somme. De plus si $\lambda \in \mathbb{R}$ et $p \in I_G$, on prend un voisinage U de λp.

On doit raisonner suivant le signe de λ.

- Si $\lambda = 0$, alors $\lambda p = \mathbf{0} \in I_G$.
- Si $\lambda > 0$, alors on considère le voisinage

$$V = \frac{1}{\lambda}U = \{\frac{1}{\lambda}q \mid q \in U\}$$

de p.

Deux situations se présentent.

1. On prend $p_+ \in (V \cap P \cap G_{\mathbb{R}})$ et une suite de rationnels strictement positifs (r_j) qui converge vers λ. La suite $(r_j p_+)$ est alors une suite d'éléments de P qui converge vers λp_+. Il y a donc un $N \in \mathbb{N}$ tel que $r_N p_+ \in U$, ce qui montre que $(U \cap P \cap G_{\mathbb{R}}) \neq \varnothing$.

2. On prend $p_- \in (V \cap -P \cap G_{\mathbb{R}})$. La suite $(r_j p_-)$ converge vers λp_-. Il y a donc un $M \in \mathbb{N}$ tel que $r_M p_- \in U$, ce qui montre que $(U \cap -P \cap G_{\mathbb{R}}) \neq \varnothing$ et donc que $\lambda p \in I_G$.

- Si $\lambda < 0$, alors un raisonnement semblable permet, à partir de l'existence d'un élément de P dans $V \cap G_{\mathbb{R}}$, à celle d'un élément de $-P$ dans $U \cap G_{\mathbb{R}}$ et à partir de l'existence d'un élément de $-P$ dans V, à celle d'un élément de P dans U, de conclure que $\lambda p \in I_G$.

Venons-en à la dimension de I_G. Montrons d'abord que $I_G \neq G_{\mathbb{R}}$, donc que $\dim_{\mathbb{R}}(I_G) \leq r - 1$. Soit $\mathcal{B} = (b_1, \cdots, b_r)$ une base du $\mathbb{Q}$-espace vectoriel G.

Si on remplace chaque élément d'une base de G par un multiple de lui-même, on a encore une base de G. On peut donc supposer que $b_i > 0$, pour $i = 1, \cdots, r$.

Posons

$$\mathrm{Pos}_G = \{p \in G_{\mathbb{R}} \mid (\exists U \in \mathcal{V}(p))(U \cap P \cap G_{\mathbb{R}} \neq \varnothing \text{ et } U \cap -P \cap G_{\mathbb{R}} = \varnothing\}$$

$$\mathrm{Neg}_G = \{p \in G_{\mathbb{R}} \mid (\exists U \in \mathcal{V}(p))(U \cap P \cap G_{\mathbb{R}} = \varnothing \text{ et } U \cap -P \cap G_{\mathbb{R}} \neq \varnothing\}.$$

Par définition de $G_{\mathbb{R}}$ et de I_G, la réunion des deux ensembles ci-dessus forme le complément de I_G dans $G_{\mathbb{R}}$.

Avant de poursuivre la démonstration du théorème, regardons quelques exemples qui aideront à mieux comprendre la classification des ordres monoïdaux.

Exemple 2.1. Prenons $G = \mathbb{Q}^3$ et P l'ensemble des éléments strictement positifs pour l'ordre grevlex.

Alors I_G est le plan d'équation $x + y + z = 0$, Pos_G est le demi-espace ouvert déterminé par le plan I_G contenant $\mathbb{N}^n$ et Neg_G est l'autre demi-espace ouvert déterminé par le plan I_G.

Exemple 2.2. Prenons G_1 l'ensemble des points de $\mathbb{Q}^3$ situés dans le plan d'équation $x + y + z = 0$ et P_1 l'ensemble des éléments de G_1 strictement positifs pour l'ordre

grevlex dans $\mathbb{Q}^3$.

Alors I_{G_1} est la droite du plan d'équation $x+y+z=0$ formée des éléments de ce plan pour lesquels $z=0$. Pos_{G_1} est le demi-plan ouvert déterminé par I_{G_1} dans le plan G_1 et qui contient le point $(0,1,-1)$ et Neg_{G_1} est l'autre demi-plan ouvert déterminé par I_{G_1} dans le plan G_1.

Exemple 2.3. Prenons G_2 l'ensemble des points de $\mathbb{Q}^3$ situés sur la droite d'équations $x+y+z=0$ et $z=0$ et P_2 l'ensemble des éléments strictement positifs de G_2 pour l'ordre grevlex dans $\mathbb{Q}^3$.

Alors I_{G_2} est $\{(0,0,0)\}$. Pos_{G_2} est la demi-droite ouverte de la droite G_2 contenant le point $(1,-1,0)$ et Neg_{G_2} est l'autre demi-droite ouverte de G_2 déterminée par I_{G_2}.

Exemple 2.4. Prenons $G=\mathbb{Q}^2$ et $P=\{(\alpha_1,\alpha_2)\in\mathbb{Q}^2 \mid \sqrt{3}\alpha_1+\alpha_2>0\}$.

Alors $I_G=\{(\alpha_1,\alpha_2)\in\mathbb{R}^2 \mid \sqrt{3}\alpha_1+\alpha_2=0\}$. $Pos_G=\{(\alpha_1,\alpha_2)\in\mathbb{R}^2 \mid \sqrt{3}\alpha_1+\alpha_2>0\}$ est le demi-plan ouvert déterminé par I_G et contenant le point $(1,1)$ et Neg_G est l'autre demi-plan ouvert déterminé par I_G.

Retournons maintenant au cas général de la démonstration du théorème.

Montrons que $\mathrm{Pos}_G \neq \varnothing$. Prenons $p=b_1+\cdots+b_r\in P\subseteq G\subseteq G_{\mathbb{R}}$.

Soit U l'ensemble des combinaisons linéaires à coefficients dans les réels strictement positifs des éléments de la base $\mathcal{B}$. U est un ouvert de $G_{\mathbb{R}}$, car c'est l'image de l'ouvert $(\mathbb{R}_+^*)^r$ de $\mathbb{R}^r$ par l'application linéaire bijective et bi-continue suivante

$$\begin{array}{ccc} \mathbb{R}^r & \xrightarrow{\xi} & G_{\mathbb{R}} \\ (\lambda_1,\cdots,\lambda_r) & \mapsto & \lambda_1 b_1+\cdots+\lambda_k b_k+\cdots+\lambda_r b_r \end{array}$$

et U ne contient aucun élément de $-P$, car

$$\lambda_1 b_1+\cdots+\lambda_k b_k+\cdots+\lambda_r b_r\in U.$$

L'ensemble

$$U \cap G = \{\mu_1 b_1 + \cdots + \mu_k b_k + \cdots + \mu_r b_r \in U \mid \mu_j \in \mathbb{Q}_+^*, 1 \leq j \leq r\}$$

ne contient que des éléments positifs, car il est une somme d'éléments positifs. Donc, $p \in \mathrm{Pos}_G$ et alors $I_G \neq G_{\mathbb{R}}$ et $\dim_{\mathbb{R}}(I_G) \leq r-1$.

Nous allons maintenant montrer que le complément $\mathrm{Pos}_G \cup \mathrm{Neg}_G$ de I_G dans $G_{\mathbb{R}}$ n'est pas connexe, ce qui va exclure la possibilité que $\dim_{\mathbb{R}}(I_G) \leq r-2$ et il ne restera donc plus que $\dim(I_G) = r-1$. Pour cela, il suffit de voir que Pos_G et Neg_G sont des ouverts disjoints et non vides de $\mathrm{Pos}_G \cup \mathrm{Neg}_G$.

On a déjà vu que $\mathrm{Pos}_G \neq \varnothing$ et un raisonnement semblable montrerais que $\mathrm{Neg}_G \neq \varnothing$. De plus, ils sont disjoints de par leur définition même.

Enfin, ils sont des ouverts dans $G_{\mathbb{R}}$, car tous les points de Pos_G d'un ouvert, contenant un point de Pos_G, sont aussi contenus dans cet ouvert qui contient un élément de P et aucun élément de $-P$. Un point de Pos_G a donc un voisinage ouvert dans Pos_G, ce qui montre que Pos_G est aussi un ouvert.

Il en est de même de Neg_G. □

Définition 2.1. *Soit un vecteur* $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n$.

Nous appelons dimension rationnelle de $\boldsymbol{\alpha}$, *la dimension du* $\mathbb{Q}$*-espace vectoriel engendré par les coordonnées de* $\boldsymbol{\alpha}$ *et nous la notons*

$$d(\boldsymbol{\alpha}) = \dim_{\mathbb{Q}}\langle\{\alpha_1, \cdots, \alpha_n\}\rangle.$$

Définition 2.2. *Soit une matrice* M *à coefficients dans* $\mathbb{R}$.

Notons $d(M)$ *la dimension rationnelle du vecteur dont les coordonnées sont les éléments de* M.

Lemme 2.3. *Soit une matrice M à coefficients dans $\mathbb{R}$ et soient A, B deux matrices-lignes inversibles, à coefficients dans $\mathbb{R}$.*

Alors, $d(M) = d(AMB)$.

Démonstration. Le $\mathbb{Q}$-espace vectoriel engendré par les éléments de la matrice M et le $\mathbb{Q}$-espace vectoriel engendré par les éléments de la matrice AMB sont les mêmes. □

Définition 2.3. *Soient G un sous-espace vectoriel de $\mathbb{Q}^n$, $\mathcal{B} = (b_1, \cdots, b_r)$ une base de G et $\boldsymbol{\alpha} \in G_{\mathbb{R}}$.*

On a $\boldsymbol{\alpha} = \lambda_1 b_1 + \cdots + \lambda_r b_r$, où $(\lambda_1, \cdots, \lambda_r)^\top$ sont les coordonnées de $\boldsymbol{\alpha}$ en base $\mathcal{B}$.

Nous appelons dimension rationnelle de $\boldsymbol{\alpha}$ relativement à G, la dimension du $\mathbb{Q}$-espace vectoriel engendré par les coordonnées de $\boldsymbol{\alpha}$ dans la base $\mathcal{B}$ et nous la notons

$$d_G(\boldsymbol{\alpha}) = \dim_{\mathbb{Q}} \langle \{\lambda_1, \cdots, \lambda_r\} \rangle.$$

Notons que $d_G(\boldsymbol{\alpha})$ ne dépend pas du choix de la base de G.

Remarque 2.1. Remarquons que $d(\boldsymbol{\alpha}) = d_{\mathbb{Q}^n}(\boldsymbol{\alpha})$.

Lemme 2.4. *Soient G un sous-espace vectoriel de $\mathbb{Q}^n$, une base $(b_1, \cdots, b_r)$ de G, $\boldsymbol{\alpha} \in G_{\mathbb{R}}$ et $\tau \in \mathbb{R}^*$. On a $\boldsymbol{\alpha} = \lambda_1 b_1 + \cdots + \lambda_r b_r$, où $(\lambda_1, \cdots, \lambda_r)^\top$ sont les coordonnées de $\boldsymbol{\alpha}$ en base $\mathcal{B}$.*

Alors $d_G(\boldsymbol{\alpha}) = d_G(\tau\boldsymbol{\alpha})$.

Démonstration. Il suffit de voir qu'un sous-ensemble $\{\alpha_{j_1}, \cdots, \alpha_{j_k}\}$ de $\{\lambda_1, \cdots, \lambda_r\}$ est indépendant sur $\mathbb{Q}$ si et seulement si $\{\tau\alpha_{j_1}, \cdots, \tau\alpha_{j_k}\}$ l'est aussi.

Si $\{\alpha_{j_1}, \cdots, \alpha_{j_k}\}$ est indépendant sur $\mathbb{Q}$, alors prenons une combinaison linéaire nulle à coefficients dans $\mathbb{Q}$ de $\{\tau\alpha_{j_1}, \cdots, \tau\alpha_{j_k}\}$

$$\sum_{i=i}^{k} q_i(\tau\alpha_{j_i}) = 0 \Leftrightarrow \tau(\sum_{i=i}^{k} q_i\alpha_{j_i}) = 0$$

et comme $\tau \neq 0$, ça implique que

$$\sum_{i=1}^{k} q_i \alpha_{j_i} = 0.$$

Puisque les α_{j_i} sont indépendants sur $\mathbb{Q}$, ceci implique que $\alpha_{j_1} = \cdots = \alpha_{j_k} = 0$. Cela montre que les $\tau\alpha_{j_i}$ sont indépendants.

La réciproque s'obtient de la même façon, mais cette fois en multipliant par τ^{-1}. □

Définition 2.4. *Soient G un sous-espace vectoriel de $\mathbb{Q}^n$ et $H \subset G_{\mathbb{R}}$, une droite de $\mathbb{R}^n$.*

Notons $d_G(H)$ la dimension rationnelle relativement à G d'un élément quelconque de H.

Étant donné un sous-espace vectoriel G de dimension r sur $\mathbb{Q}$ et un ordre monoïdal sur G, on a vu que $G_{\mathbb{R}}$ est de dimension r sur $\mathbb{R}$ et I_G est de dimension $r-1$ sur $\mathbb{R}$.

Par conséquent, les vecteurs de $G_{\mathbb{R}}$, qui sont orthogonaux à I_G, forment un sous-espace $\mathcal{O}(G)$ de dimension 1 de $G_{\mathbb{R}}$.

Lemme 2.5. *L'élément* $\mathbf{0}$ *de la droite $\mathcal{O}(G)$ détermine deux demi-droites ouvertes dont une seule est contenue dans* Pos_G.

Démonstration. Les demi-droites ouvertes sont connexes et sont situées chacune dans un demi-espace différent déterminé par I_G, car si l'une d'entre elles touchait aux deux demi-espaces, on aurait deux composantes connexes du complément de I_G liées par un segment de droite, ce qui est impossible !

Par ailleurs, si $p \in \mathcal{O}(G)$, alors $-p \in \mathcal{O}(G)$. Ce qui montre que $\mathcal{O}(G)$ a une intersection non vide avec chacune des deux composantes connexes du complément de $\mathcal{O}(G)$. □

Définition 2.5. *Étant donné un sous-espace vectoriel G de $\mathbb{Q}^n$ de dimension r.*

Notons $U(G)$ la demi-droite ouverte de $\mathcal{O}(G)$ partant de l'origine et contenue dans Pos_G.

Ramenons-nous maintenant aux exemples précédents.

Dans l'exemple 2.1.,

$$U(G) = \mathbb{R}_+^*(1,1,1),$$

c'est-à-dire les multiples strictement positifs de $(1,1,1)$.

Dans l'exemple 2.2., $U(G_1)$ est la demi-droite entièrement contenue dans $x+y+z=0$ et qui est perpendiculaire à I_{G_1}. Les coordonnées (x,y,z) d'un point de cette demi-droite doivent donc satisfaire $x+y+z=0$, pour appartenir à G_1 et $z=0$, pour appartenir à I_{G_1}.

Les points de I_{G_1} sont les points de G_1 pour lesquels $z=0$. Ce sont donc les solutions de $x+y+z=0, z=0$, qui sont de la forme $(t,-t,0)$, pour tout $t \in \mathbb{R}$. En plus de satisfaire $x+y+z=0$, un point de $U(G_1)$ doit satisfaire

$$(x,y,z)\cdot(t,-t,0)=0,$$

avec en particulier $t \neq 0$, c'est-à-dire $x-y=0$.

Les points de $U(G_1)$ satisfont donc au système $x+y+z=0, z=0$. La droite contenant $U(G_1)$ sera formée des points $(t,t,-2t)$ et puisque $U(G_1) \subset \mathrm{Pos}_{G_1}$, on doit avoir $-2t<0$, c'est-à-dire $t>0$, d'où

$$U(G_1) = \mathbb{R}_+^*(1,1,-2).$$

Pour s'assurer que $U(G_1)$ est bien perpendiculaire à I_{G_1}, on peut vérifier que

$$(1,1,-2)\cdot(1,-1,0)=0.$$

Dans l'exemple 2.3., $U(G_2)$ est la demi-droite de I_{G_2} pour laquelle $y<0$.

Pos_{G_2} est l'ensemble des éléments (x,y,z) de G_2 pour lesquels $x+y+z=0, z=0$ et où $y<0$.

Avec $x+y+z=0, z=0$, on a que $x+y=0$, c'est-à-dire que $x=-y$. Donc, les points de la forme $(t,-t,0)$, pour tout $t \in \mathbb{R}$ pour lesquels $-t<0$. On a alors que

$$U(G_2) = \mathbb{R}_+^*(1,-1,0).$$

Ce qui nous permet d'obtenir la matrice

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}$$

représentant l'ordre grevlex.

Dans l'exemple 2.4., nous devons trouver un vecteur v qui soit perpendiculaire à I_G. Prenons $v=(\sqrt{3},1)$. On a

$$(\sqrt{3},1)\cdot(\alpha_1,\alpha_2)=0,$$

car $\sqrt{3}\alpha_1+\alpha_2=0$, par définition de I_G.

Puisque le produit scalaire est positif, alors v est positif, par définition de P. On a donc que

$$U(G) = \mathbb{R}_+^*(\sqrt{3},1).$$

De plus, $d_G(U(G)) = d(U(G)) = d(\sqrt{3},1) = 2$, car $\sqrt{3}$ et 1 sont des éléments de $\mathbb{R}$ indépendants sur $\mathbb{Q}$. On est donc assuré qu'il n'y a pas d'éléments de P sur I_G.

Ceci nous permet d'obtenir la matrice

$$\begin{bmatrix} \sqrt{3} & 1 \end{bmatrix}$$

représentant l'ordre.

Lemme 2.6. *Soient G un sous-espace vectoriel de $\mathbb{Q}^n$ de dimension r et $\boldsymbol{\alpha} \in G_{\mathbb{R}} \subseteq \mathbb{R}^n$.*

Alors, $d(\boldsymbol{\alpha}) \leq d_G(\boldsymbol{\alpha}) \leq r$.

Démonstration. Soit une base $(b_1, \cdots, b_r)$ de G. Remarquons que la base $\mathcal{B}$ est aussi une base de $G_{\mathbb{R}}$.

On a $\boldsymbol{\alpha} = \lambda_1 b_1 + \cdots + \lambda_r b_r$, où $(\lambda_1, \cdots, \lambda_r)^\top$ sont les coordonnées de $\boldsymbol{\alpha}$ en base $\mathcal{B}$.

Chacune des coordonnées de $\boldsymbol{\alpha}$ dans $\mathbb{R}$ est donc combinaison linéaire à coefficients rationnels des λ_i, pour $i = 1, \cdots, r$, donc est un élément du $\mathbb{Q}$-espace vectoriel $W = \langle \lambda_1, \cdots, \lambda_r \rangle$ qui est de dimension $d_G(\boldsymbol{\alpha}) \leq r$. □

3 Classification proprement dite et commentaires

Proposition 3.1. *Soient G un sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^n$ de dimension r et $\leq$ un ordre sur G provenant d'un ordre monoïdal sur $\mathbb{Q}^n$.*

Soient $\mathbf{u} \in U(G)$ et $d = d_G(\mathbf{u}) = d_G(U(G))$, alors

$$\dim_{\mathbb{Q}}(I_G \cap \mathbb{Q}^n) = r - d = \dim_{\mathbb{Q}}(G) - d_G(U(G)).$$

Démonstration. Soit $\mathcal{B} = (b_1, \cdots, b_r)$ une base de G. Le $\mathbb{Q}$-espace vectoriel $I_G \cap \mathbb{Q}^n$ est formé des vecteurs $\mathbf{v} \in G$ qui sont orthogonaux à $U(G)$.

Un tel vecteur $\mathbf{v}$ est de la forme

$$\mathbf{v} = q_1 b_1 + \cdots + q_r b_r,$$

où $\mathcal{B}$ est orthonormale, car $\mathbf{v}$ est dans G.

On a $\mathbf{u} = \lambda_1 b_1 + \cdots + \lambda_r b_r$.

L'affirmation voulant que $\mathbf{u} \perp \mathbf{v} \Leftrightarrow \mathbf{u} \cdot \mathbf{v} = 0$ s'écrit sous la forme

$$(\lambda_1 b_1 + \cdots + \lambda_r b_r) \cdot (q_1 b_1 + \cdots + q_r b_r) = 0,$$

où $\cdot$ est le produit scalaire usuel dans $\mathbb{R}^n$.

Ce produit est donc égal à

$$\sum_{i=1}^{r} \sum_{j=1}^{r} \lambda_i q_j (b_i \cdot b_j) = \sum_{i=1}^{r} \lambda_i q_i = 0, \tag{9.1}$$

car $\mathcal{B}$ est orthonormale.

Cependant, le fait que $d_G(\mathbf{u}) = d$ veut dire qu'on peut trouver d coordonnées de $\mathbf{u}$, en base $\mathcal{B}$, qui sont indépendantes sur $\mathbb{Q}$, disons celles dont les indices sont les éléments de $\{j_1, \cdots, j_d\}$ et les autres qui sont combinaisons linéaires à coefficients dans $\mathbb{Q}$ de ces coordonnées-là, soient celles dont les indices sont éléments de

$$\{1, \cdots, r\} \setminus \{j_1, \cdots, j_d\} = \{k_1, \cdots, k_{r-d}\}.$$

Posons

$$\begin{aligned}
\lambda_{k_1} &= \sum_{\mu=1}^{d} \gamma_{k_1\mu}\lambda_{j_\mu} = \gamma_{k_1 1}\lambda_{j_1} + \cdots + \gamma_{k_1 d}\lambda_{j_d} \\
&\vdots \\
\lambda_{k_i} &= \sum_{\mu=1}^{d} \gamma_{k_i\mu}\lambda_{j_\mu} = \gamma_{k_i 1}\lambda_{j_1} + \cdots + \gamma_{k_i d}\lambda_{j_d} \\
&\vdots \\
\lambda_{k_{r-d}} &= \sum_{\mu=1}^{d} \gamma_{k_{r-d}\mu}\lambda_{j_\mu} = \gamma_{k_{r-d}1}\lambda_{j_1} + \cdots + \gamma_{k_{r-d}d}\lambda_{j_d}.
\end{aligned}$$

On remplace ensuite les λ_i, dans l'équation (9.1), par les valeurs données ci-dessus et on obtient une combinaison linéaire égale à 0, à coefficients rationnels des nombres réels

$\mathbb{Q}$-indépendants λ_{j_i}, avec $i = 1, \cdots, d$,

$$
\begin{aligned}
&= \lambda_1 q_1 + \cdots + \lambda_r q_r = 0 \\
&= \lambda_{j_1} q_{j_1} + \cdots + \lambda_{j_d} q_{j_d} + \lambda_{k_1} q_{k_1} + \cdots + \lambda_{k_{r-d}} q_{k_{r-d}} = 0 \\
&= \lambda_{j_1} q_{j_1} + \cdots + \lambda_{j_d} q_{j_d} + (\sum_{\mu=1}^{d} \gamma_{k_1 \mu} \lambda_{j_\mu}) q_{k_1} + \cdots + (\sum_{\mu=1}^{d} \gamma_{k_{r-d} \mu} \lambda_{j_\mu}) q_{k_{r-d}} = 0 \\
&\vdots \\
&= \sum_{i=1}^{d} \lambda_{j_i} (q_{j_i} + \sum_{\tau=1}^{r-d} q_{k_\tau} \gamma_{k_\tau i}) = 0
\end{aligned}
$$

Les coefficients de λ_{j_1}, de λ_{j_2}, $\cdots$, de λ_{j_d} sont donc nuls.

Ces coefficients nous donnent alors d équations dont les solutions sont les coordonnées $(q_1, \cdots, q_r)$, en base $\mathcal{B}$, des éléments de $I_G \cap \mathbb{Q}^n$.

$$
\begin{aligned}
q_{j_1} + \sum_{\tau=1}^{r-d} q_{k_\tau} \gamma_{k_\tau 1} &= 0 \\
&\vdots \\
q_{j_d} + \sum_{\tau=1}^{r-d} q_{k_\tau} \gamma_{k_\tau d} &= 0
\end{aligned}
$$

Sous forme matricielle, ce système d'équations peut s'écrire

$$
\begin{bmatrix}
1 & & & 0 & \gamma_{k_1 1} & \cdots & \gamma_{k_{r-d} 1} \\
& 1 & & & \gamma_{k_1 2} & \cdots & \gamma_{k_{r-d} 2} \\
& & & & & & \\
& & \ddots & & \vdots & & \vdots \\
& & & & & & \\
0 & & & 1 & \gamma_{k_1 d} & \cdots & \gamma_{k_{r-d} d}
\end{bmatrix}
\begin{bmatrix}
q_{j_1} \\ \vdots \\ q_{j_d} \\ q_{k_1} \\ \vdots \\ q_{k_{r-d}}
\end{bmatrix}
=
\begin{bmatrix}
0 \\ \\ \\ \vdots \\ \\ 0
\end{bmatrix}
$$

La dimension de $I_G \cap \mathbb{Q}^n$ est égale à la dimension de l'espace des coordonnées $(q_1, \cdots, q_r)$

en base $\mathcal{B}$ de ses éléments. C'est donc $r-$ rang(M), où

$$M = \begin{bmatrix} 1 & & & 0 & \gamma_{k_1 1} & \cdots & \gamma_{k_{r-d}1} \\ & 1 & & & \gamma_{k_1 2} & \cdots & \gamma_{k_{r-d}2} \\ & & \ddots & & \vdots & & \vdots \\ 0 & & & 1 & \gamma_{k_1 d} & \cdots & \gamma_{k_{r-d}d} \end{bmatrix}.$$

Remarquons que cette matrice M contient la matrice identité de rang d. □

Proposition 3.2. *Soient G un sous-espace vectoriel de $\mathbb{Q}^n$ de dimension r, une base $\mathcal{B} = (b_1, \cdots, b_r)$ de G et $\mathbf{u} \in G_{\mathbb{R}}$.*

Alors, $d(\mathbf{u}) = d_G(\mathbf{u})$.

Démonstration. Soit $\mathcal{E} = (e_1, \cdots, e_n)$ la base canonique de $\mathbb{R}^n$.

Soient $(u_1, \cdots, u_n)^\top$ le vecteur colonne des coordonnées de $\mathbf{u}$ en base $\mathcal{E}$ et $(\lambda_1, \cdots, \lambda_r)^\top$ le vecteur colonne des coordonnées de $\mathbf{u}$ en base $\mathcal{B}$.

On a $\mathbf{u} = \lambda_1 \mathbf{b_1} + \cdots + \lambda_r \mathbf{b_r}$.

Soit $(b_{1i}, \cdots, b_{ni})^\top$ le vecteur colonne des coordonnées des $\mathbf{b_i}$ en base $\mathcal{E}$. Notons $M_{\mathcal{B}}^{\mathcal{E}}$ la matrice $n \times r$ suivante,

$$M_{\mathcal{B}}^{\mathcal{E}} = \begin{bmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nr} \end{bmatrix}.$$

On a alors que

$$(u_1, \cdots, u_n)^\top = M_{\mathcal{B}}^{\mathcal{E}} (\lambda_1, \cdots, \lambda_r)^\top. \tag{9.2}$$

Le rang de $M_{\mathcal{B}}^{\mathcal{E}}$ est r, car les r colonnes de cette matrice sont des vecteurs indépendants. On peut, par une suite d'opérations-lignes élémentaires, ramener cette matrice à une

matrice échelonnée-réduite dont les lignes 1 à r forment la matrice identité et les lignes $r+1$ à n sont nulles.

$$I_0 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}.$$

Autrement dit, puisque chaque opérations-lignes élémentaires correspond à la multiplication par une matrice élémentaire $n \times n$ nécessairement inversible, on a la matrice

$$I_0 = NM_{\mathcal{B}}^{\mathcal{E}},$$

où N est le produit de ces matrices élémentaires.

On a donc

$$\begin{aligned} I_0 &= NM_{\mathcal{B}}^{\mathcal{E}} \\ I_0(\lambda_1, \cdots, \lambda_r)^\top &= NM_{\mathcal{B}}^{\mathcal{E}}(\lambda_1, \cdots, \lambda_r)^\top \\ (\lambda_1, \cdots, \lambda_r)^\top &= N(u_1, \cdots, u_n)^\top. \end{aligned}$$

Cela signifie que le $\mathbb{Q}$-espace vectoriel engendré par $(\lambda_1, \cdots, \lambda_r)^\top$ est inclus dans le $\mathbb{Q}$-espace vectoriel engendré par $(u_1, \cdots, u_n)^\top$, puisque chaque λ_i, pour $i = 1, \cdots, r$, est combinaison linéaire à coefficients rationnels des u_j, pour $j = 1, \cdots, n$. Donc $d_G(\mathbf{u}) \leq d(\mathbf{u})$.

Réciproquement, chaque u_j, pour $j = 1, \cdots, n$, est combinaison linéaire à coefficients rationnels des λ_i, pour $i = 1, \cdots, r$, car $\mathbf{u} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_r \mathbf{b}_r$. Donc $d(\mathbf{u}) \leq d_G(\mathbf{u})$.

Ceci montre bien que $d(\mathbf{u}) = d_G(\mathbf{u})$. □

Définition 3.1. *Étant donné un sous-espace vectoriel W de $\mathbb{R}^n$, notons*

$$W^{\perp} = \{\mathbf{v} \in \mathbb{R}^n \mid \forall \mathbf{w} \in W, \mathbf{w} \cdot \mathbf{v} = 0\}.$$

Théorème 3.1. *Soit $\leq_\sigma$ un ordre monoïdal sur $\mathbb{Q}^n$.*

Il existe $s \leq n$ vecteurs orthogonaux $\mathbf{u}_1, \cdots, \mathbf{u}_s$ de $\mathbb{R}^n$ tels que, en posant

$$\begin{aligned} G_0 &= \mathbb{Q}^n \\ G_1 &= \langle \mathbf{u}_1 \rangle^{\perp} \cap \mathbb{Q}^n \\ G_2 &= \langle \mathbf{u}_1, \mathbf{u}_2 \rangle^{\perp} \cap \mathbb{Q}^n \\ &\vdots \\ G_{s-1} &= \langle \mathbf{u}_1, \cdots, \mathbf{u}_{s-1} \rangle^{\perp} \cap \mathbb{Q}^n, \end{aligned}$$

on ait $G_s = 0$ et $n = d(\mathbf{u}_1) + d(\mathbf{u}_2) + \cdots + d(\mathbf{u}_s)$ et tels que pour un vecteur quelconque $\mathbf{v} \in \mathbb{Q}^n$, on ait $\mathbf{v} > 0$ si et seulement si la première composante non nulle de $(\mathbf{v} \cdot \mathbf{u}_1, \cdots, \mathbf{v} \cdot \mathbf{u}_s)$ est positive.

En d'autres mots, si on considère l'ordre lex sur $\mathbb{R}^s$ et si $\mathbf{u}_i = (u_{i1}, \cdots, u_{in})$ et $\mathbf{v} = (v_1, \cdots, v_n)$, alors

$$(v_1, \cdots, v_n) >_\sigma 0 \Leftrightarrow \begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{s1} & \cdots & u_{sn} \end{bmatrix} \begin{bmatrix} v_1 \\ \\ \vdots \\ \\ v_n \end{bmatrix} >_{\text{lex}} \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Démonstration. On part avec $G_0 = \mathbb{Q}^n$, $\mathbf{u}_1 \in U(G_0)$.

Par construction, si $\mathbf{v} \notin I_{G_0}$, alors $\mathbf{v} \cdot \mathbf{u}_1 \neq 0$, si ce produit scalaire est positif, $\mathbf{v}$ sera dans le même demi-espace Pos_{G_0} que 1 et ce demi-espace ne contient pas de négatifs. Donc $\mathbf{v} > 0$.

Dans le cas contraire, $\mathbf{v} < 0$. Si $I_{G_0} = 0$, autrement dit si $d_(\mathbf{u_1}) = n$, on a fini.

Si, par contre, $\mathbf{v} \in (I_{G_0} \cap \mathbb{Q}^n) \neq 0$, on ne peut décider tout de suite. On pose $G_1 = I_{G_0} \cap \mathbb{Q}^n$, cet espace est de dimension $n - d_(\mathbf{u_1})$ et on prend $\mathbf{u_2} \in U(G_1)$.

Par la proposition précédente, $d(\mathbf{u_2}) \leq n - d(\mathbf{u_1})$.

Le raisonnement ci-dessus montre que si $\mathbf{v} \in G_1$ et $\mathbf{v} \notin I_{G_1}$, alors $\mathbf{v} \cdot \mathbf{u_2} \neq 0$ et un tel $\mathbf{v}$ ne sera strictement positif que si son produit scalaire avec $\mathbf{u_2}$ est strictement positif. Notons qu'un tel $\mathbf{v}$, étant déjà dans G_1, est orthogonal à $\mathbf{u_1}$.

On continue ainsi et après un nombre fini d'étapes, on arrive à $G_s = 0$. □

Définition 3.2. *Avec les notations du théorème précédent, on appelle le type d'ordre de $>_\sigma$, le nombre s de lignes de la matrice trouvée et on appelle la composition d'ordre de $>_\sigma$, la composition de n, de longueur s, donnée par $(d(\mathbf{u_1}), \cdots, d(\mathbf{u_s}))$.*

Remarque 3.1. Dans le cas où $s = 1$, l'ordre est appelé de type archimédien.

Soient $\boldsymbol{\varepsilon} = (\varepsilon_1, \cdots, \varepsilon_n) >_\sigma 0$ et $\mathbf{r} = (r_1, \cdots, r_n) >_\sigma \mathbf{0}$, avec $\boldsymbol{\varepsilon}, \mathbf{r} \in \mathbb{Q}^n$.

Soit $\mathbf{u_1} = (u_{11}, \cdots, u_{1n}) \in \mathbb{R}^n$.

On veut montrer qu'il existe un entier $n \in \mathbb{N}^*$ tel que $n\boldsymbol{\varepsilon} >_\sigma \mathbf{r}$. Le fait que $\boldsymbol{\varepsilon} >_\sigma \mathbf{0}$ veut dire que $(u_{11}\varepsilon_1, \cdots, u_{1n}\varepsilon_n) > \mathbf{0}$ et le fait que $\mathbf{r} >_\sigma \mathbf{0}$ veut dire que $(u_{11}r_1, \cdots, u_{1n}r_n) > \mathbf{0}$.

Utilisons le fait que $(\mathbb{Q}, >)$ soit archimédien. Il existe donc un entier naturel n strictement positif tel que

$$n(u_{11}\varepsilon_1, \cdots, u_{1n}\varepsilon_n) > (u_{11}r_1, \cdots, u_{1n}r_n).$$

Ceci exprime précisément le fait que $n\boldsymbol{\varepsilon} >_\sigma \mathbf{r}$.

Remarque 3.2. Dans le cas où $s = n$, l'ordre est appelé de type lexicographique.

Il existe un isomorphisme f d'espace vectoriel qui préserve l'ordre, tel que

$$(\mathbb{Q}^n, >_\sigma) \xrightarrow{f} (\mathbb{Q}^n, >_{\text{lex}}).$$

L'ordre est isomorphe à un ordre lexicographique.

Remarque 3.3. En prenant les exemples 2.1.,2.2. et 2.3. de la précédente section, on voit que grevlex est de type 3 et de composition $(1,1,1)$ et est donné par la matrice orthogonale

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}.$$

Remarque 3.4. On notera que les matrices déjà données pour grevlex s'obtenaient l'une de l'autre par multiplication par une matrice triangulaire inférieure à éléments positifs sur la diagonale.

Par contre, la matrice de la remarque précédente ne s'obtient pas ainsi des autres. On voit que les deux relations d'équivalence introduites sur les matrices $n \times n$ sont effectivement différentes.

Exemple 3.1. Soit notre matrice

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}.$$

Prenons la matrice 3×3 décrivant l'ordre grevlex,

$$Z = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

et une matrice triangulaire inférieure à éléments positifs sur la diagonale,

$$T = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix},$$

avec $a, b, c \in \mathbb{N}$.

Essayons maintenant d'obtenir notre matrice M par multiplication de T et de Z.

$$TZ = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ a & a & a-1 \\ b & b-1 & b-c \end{bmatrix}.$$

La matrice obtenue TZ devrait donc correspondre à notre matrice M,

$$\begin{bmatrix} 1 & 1 & 1 \\ a & a & a-1 \\ b & b-1 & b-c \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}.$$

Pour les éléments de la première ligne, ça fonctionne, car $1 = 1$.

Pour les éléments de la deuxième ligne, première et deuxième colonne, pour que ça fonctionne, nous devons prendre $a = 1$.

Mais pour l'élément de la deuxième ligne, troisième colonne, nous avons $a - 1 = -2$, donc que $a = -1$, mais puisqu'on avait $a = 1$, nous arrivons à la contradiction $1 = -1$.

Notre matrice M ne peut donc être obtenue de cette manière.

Remarque 3.5. L'ordre monomial de l'exemple 2.4. de la précédente section est de type 1 (type archimédien) et de composition (2) et est donné par la matrice

$$\begin{bmatrix} \sqrt{3} & 1 \end{bmatrix}.$$

Remarque 3.6. Les ordres monoïdaux, déjà rencontrés, décrits par une matrice $n \times n$ sont les ordres de type n et par conséquent, de composition $(1, \cdots, 1)$.

Proposition 3.3. *Pour qu'un ordre monoïdal soit un ordre monomial, il faut que le premier élément non nul de chaque colonne de la matrice le représentant soit strictement positif.*

Démonstration. Voir (Robbiano, 2000) page 53. □

On a vu qu'un ordre monoïdal peut être représenté par s vecteurs, on peut alors se demander quelles conditions faut-il pour que s vecteurs de $\mathbb{R}^n$ déterminent un ordre monoïdal ?

Théorème 3.2. *Étant donné un entier $s \leq n$ et une composition $(d_1, \cdots, d_s)$ de n et s vecteurs $\mathbf{u_1}, \cdots, \mathbf{u_s}$ de $\mathbb{R}^n$, orthogonaux deux à deux, et tels que, si G_i est le sous-espace vectoriel de $\mathbb{Q}^n$ formé des vecteurs orthogonaux à $\mathbf{u_1}, \cdots, \mathbf{u_s}$, alors $\mathbf{u_i} \in (G_{i-1})_{\mathbb{R}}$ et $d_(\mathbf{u_i}) = d_i$, pour $i = 1, \cdots, s$.*

On détermine un ordre monoïdal en posant $P = \{\mathbf{v} \in \mathbb{Q}^n \mid$ le premier élément non nul de $(\mathbf{v} \cdot \mathbf{u_1}, \cdots, \mathbf{v} \cdot \mathbf{u_s})$ est strictement positif$\}$.

De plus, deux telles suites de vecteurs de $\mathbb{R}^n$, $(\mathbf{u_1}, \cdots, \mathbf{u_s})$ et $(\mathbf{u'_1}, \cdots, \mathbf{u'_s})$ déterminent le même ordre monoïdal si et seulement s'il existe $\lambda_1, \cdots, \lambda_s \in \mathbb{R}_+$ tels que $\mathbf{u'_i} = \lambda_i \mathbf{u_i}$, pour $i = 1, \cdots, s$.

Démonstration. Ce théorème ne fait que résumer les observations déjà faites. □

CONCLUSION

Ce travail a permis de connaître en détail la notion de bases de Groebner et de savoir pour quelles situations mathématiques elles sont essentielles.

De plus, ce travail est le premier ouvrage à exposer en détail la classification des ordres monomiaux et à analyser les articles des auteurs Volker Weispfenning (Allemagne) et Lorenzo Robbiano (Italie) de façon explicite, avec des démonstrations détaillées.

Grâce à cette analyse, nous avons vu que la caractérisation des ordres monomiaux telle qu'esquissée par Robbiano et détaillée dans ce mémoire, permet d'avoir une forme standardisée pour chacun des ordres monomiaux, ce qui n'est pas le cas de celle de Weispfenning.

La théorie des bases de Groebner pour les anneaux de polynômes, énoncée dans ce mémoire, a été développée en 1965 en Autriche, par Bruno Buchberger.

Un concept analogue pour les anneaux locaux a été développé indépendamment, en 1964 au Japon, par Heisuke Hironaka, qui les a appelés, bases standards. Ce pourrait être l'objet d'une étude ultérieure.

Aussi, il serait intéressant de voir la notion de bases de Groebner dans le contexte d'algèbres non commutatives, par exemple, les algèbres de Ore traitées dans le logiciel Maple ou les récents travaux de Huishi Li sur les « Gamma-Leading Homogeneous Algebras » qui paraîtront en 2008 dans « Algebra Colloquium ».

D'un point de vue informatique, nous pourrions vérifier la vitesse d'exécution des algorithmes à l'aide du logiciel Maple, en comparant différents ordres sur les monômes.

Certaines publications prétendent que l'ordre lexicographique inversé avec priorité au degré, tel que nous l'avons vu, donne lieu au calcul le plus rapide de base de Groebner, mais nous n'avons pas encore trouvé de preuve de ce fait.

BIBLIOGRAPHIE

Abramov, S. A., H. Q. Le et Z. Li. 2004. *Univariate Ore Polynomial Rings in Computer Algebra.* Translated from Sovremennaya Matematika i Ee Prilozheniya (Contemporary Mathematics and Its Applications). Volume 13. Springer Science+Business Media, Inc.

Bouchard, Pierre. 1989. Article. *A Commutative Algebra and Algebraic Geometry Laboratory with the Use of the Computer.* Alcuni Aspetti della Teoria degli Anelli Commutativi. Dip. Mat. Univ. Rome.

Bouchard, Pierre. 1990. Conférence. *Des règles de réécriture aux bases de Groebner.* Document d'accompagnement. Université du Québec à Montréal. Montréal.

Buchberger, B. et C. Kollreider. s.d. *An Improved Algorithmic Construction of Gröbner-Bases for Polynomial Ideals.* Johannes Kepler Universität. A-4045 Linz. Autriche.

Chyzak, Frédéric. 2004. *Bases de Gröbner, algorithme de Buchberger et applications.* Notes de cours.

Chyzak, Frédéric. s.d. *Introduction au Calcul formel. Algorithmes et complexité.* INRIA.

Cox, David, John Little et Donal O'Shea. 1996. *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer. Second Edition.

Cox, David, John Little et Donal O'Shea. 1998. *Using Algebraic Geometry.* Springer.

Eisenbud, David et Lorenzo Robbiano. 1991. *Computational Algebraic Geometry and Commutative Algebra.* Symposia Mathematica Volume XXXIV. Cambridge.

Eisenbud, David. 2005. *The Geometry of Syzygies.* Preface : Algebra and Geometry. Volume 229. Springer. New York.

Martin-Deschamps, Mireille. s.d. *Méthodes Algébriques Effectives.*

Mercier, Dany-Jack. 2006. *L'épreuve d'exposé au CAPES mathématiques.* Volume 2. Éditions Publibook.

Mora, Teo. 1988. *Seven Variations on Standard Bases.* N. 45. Università di Genova. Genève.

Ramis, Edmond, Claude Deschamps et Jacques Odoux. 1998. *Cours de mathématiques, 3. topologie et éléments d'analyse.* Les cours de référence. Dunod, Paris.

Robbiano, Lorenzo et Martin Kreuzer. 2000. *Computational Commutative Algebra 1.* Springer.

Robbiano, Lorenzo et Martin Kreuzer. 2005. *Computational Commutative Algebra 2.* Springer.

Robbiano, Lorenzo. 2007. Article. *Classification of Orderings.*

Robbiano, Lorenzo. 1984-1985. Article. *Term Orderings on the Polynomial Ring.* EUROCAL. Lecture Notes in Computer Science Springer, Heidelberge 204. pages 513-517. Istituto Matematico dell'Università di Genova. Genève.

Robbiano, Lorenzo. 1985. Article. *On the Theory of Graded Structures.* Istituto Matematico dell'Università di Genova. Genève.

Salvy, Bruno, Frédéric Chyzak et Marni Mishna. 2005. Article. *Effective Scalar Products of D-finite Symmetric Functions.* arXiv :math.CO/0310132 v2.

Salvy, Bruno. s.d. Article. *Systèmes polynomiaux. Bases de Gröbner.* INRIA.

Schwarz, Fritz. s.d. *Monomial Orderings and Gröbner Bases.* GMD, Institut F1. Postfach 1240, 5205 St. Augustin. Allemagne.

Sturmfels, Bernd. 1995. *Gröbner Bases and Conves Polytopes.* Volume 8. University Lecture Series. American Mathematical Society.

Weispfenning, Volker et Thomas Becker, avec la collaboration de Heinz Kredel. 1993. *Gröbner Bases, A Computational Approach to Commutative Algebra.* Springer-Verlag.

Weispfenning, Volker. s.d. Article. *Admissible Orders and Linear Forms.* Mathematisches Institut der Universitaet. D-6900 Heidelberg, W. Allemagne.

Documentation de CoCoA, logiciel CoCoA (Computations in Commutative Algebra).

Documentation de Macaulay, logiciel Macaulay 2.

Documentation de Maple, logiciel Maple 10.

Documentation de Singular, logiciel Singular.

Index

Librairies

Librairie offrant des outils permettant de manipuler des listes.

```
> with(ListTools):
```

Librairie permettant de construire et de manipuler des matrices et des vecteurs, de calculer des opérations standards, des résultats et de résoudre des problèmes d'algèbre linéaire.

```
> with(LinearAlgebra):
```

Librairie pemettant de faire des calculs avec des idéaux d'un anneau de polynômes, à une ou plusieurs variables, sur un corps commutatif.

```
> with(PolynomialIdeals):
```

Librairie permettant de faires des calculs de bases de Groebner et des opérations sur les idéaux d'un anneau de polynômes, à une ou plusieurs variables, sur un corps commutatif.

```
> with(Groebner):
```

Commandes de Maple

NormalForm

Commande permettant de connaître le reste de la division d'un polynôme, par un ensemble de polynômes, selon l'algorithme de division de polynômes.

En prenant l'ordre lexicographique: plex.

```
> NormalForm(x^3+3*y^2,[x^2+y,x+2*x*y],plex(x,y));
```

$$3\,y^2+\frac{1}{2}\,x \tag{2.1.1}$$

En prenant l'ordre lexicographique avec priorité au degré: grlex.

```
> NormalForm(x^3+3*y^2,[x^2+y,x+2*x*y],grlex(x,y));
```

$$3\,y^2+\frac{1}{2}\,x \tag{2.1.2}$$

En prenant l'ordre lexicographique inversé avec priorité au degré: tdeg.

```
> NormalForm(x^3+3*y^2,[x^2+y,x+2*x*y],tdeg(x,y));
```

$$3\,y^2+\frac{1}{2}\,x \tag{2.1.3}$$

Dans "CLO.1", p.59, exemple 1.

```
> NormalForm(x*y^2+1,[x*y+1,y+1],plex(x,y));
```

$$2 \tag{2.1.4}$$

Dans "CLO.1", p.60, exemple 2.

```
> NormalForm(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],plex(x,y));
```

$$x + y + 1 \tag{2.1.5}$$

Basis

Commande permettant de trouver une liste de polynômes constituant une base de Groebner réduite, pour un idéal donné et un ordre fixé sur les variables.

```
> Basis([x^2+y,2*x*y+y^2],plex(x,y));
```

$$[y^3 + 4\,y^2,\ 2\,x\,y + y^2,\ x^2 + y] \tag{2.2.1}$$

Dans cet exemple, les coefficients sont eux-mêmes des polynômes.

```
> Basis([v*x^2+y,u*x*y+y^2],plex(x,y));
```

$$[v\,y^3 + y^2\,u^2,\ u\,x\,y + y^2,\ v\,x^2 + y] \tag{2.2.2}$$

Leading

Commandes qui retournent le coefficient dominant et/ou le monôme dominant d'un polynôme, selon un ordre fixé sur les variables.

Le coefficient dominant, en prenant l'ordre lexicographique.

```
> LeadingCoefficient((u+v)*x*y+y^2,plex(x,y));
```

$$u + v \tag{2.3.1}$$

Le coefficient dominant, en prenant l'ordre lexicographique inversé avec priorité au degré.

```
> LeadingCoefficient((x+y)*(x^2+y),tdeg(x,y));
```

$$1 \tag{2.3.2}$$

Le monôme dominant, en prenant l'ordre lexicographique avec priorité au degré.

```
> LeadingMonomial(320*x*y^2-9*x^3*y^4-96*z^2*y^4*x+1600*y^3,
  grlex(x,y,z));
```

$$y^4\,x^3 \tag{2.3.3}$$

Le coefficient dominant et le monôme dominant, en prenant l'ordre lexicographique inversé avec priorité au degré.

```
> LeadingTerm(96*z^2*y^4*x+1600*y^3,tdeg(x,y,z));
```

$$96,\ z^2\,y^4\,x \tag{2.3.4}$$

divide

Commande qui détermine si un polynôme peut être divisé par un autre polynôme.

```
> unassign('q');
```

```
divide(2*x*y,x,q); q;
```

true

$$2\,y \tag{2.4.1}$$

```
> unassign('q');
  divide(2*x*y,y^2,'q'); q;
```

false

$$q \tag{2.4.2}$$

Procédures

LT ("leading term")

Procédure qui prend le coefficient dominant et le monôme dominant d'un polynôme, selon un ordre fixé sur les variables et qui fait le produit des deux pour retourner le terme dominant du polynôme en question.

```
> LT:=proc(polynome,ordre)
  local l,coeff,monom;
    l:=LeadingTerm(polynome,ordre);
    coeff:=l[1];
    monom:=l[2];
  return(coeff*monom);
  end proc:
```

Le calcul du coefficient dominant et du monôme dominant, avec la commande de Maple, selon l'ordre lexicographique inversé avec priorité au degré.

```
> LeadingTerm(2*x*y+y^2,tdeg(x,y));
```

$$2, x\,y \tag{3.1.1}$$

Le calcul du terme dominant, avec la procédure LT, selon l'ordre lexicographique.

```
> LT(2*x*y+y^2,plex(x,y));
```

$$2\,x\,y \tag{3.1.2}$$

```
> LT(-2*x*y+y^2,plex(x,y));
```

$$-2\,x\,y \tag{3.1.3}$$

vE (vecteur unitaire) et vNul (vecteur nul)

vE: Procédure qui génère une liste de vecteurs unitaires, selon le nombre d'éléments demandés.

```
> delta:=proc(i,j) if i = j then 1 else 0 end if end proc:
> vE:=proc(n)
    return([seq([seq(delta(i,j),j=1..n)],i=1..n)]);
```

```
  end proc:
```

Liste de deux vecteurs unitaires à deux éléments.

```
> vE(2);
```

$$[[1, 0], [0, 1]] \tag{3.2.1}$$

Liste de trois vecteurs unitaires à trois éléments.

```
> vE(3);
```

$$[[1, 0, 0], [0, 1, 0], [0, 0, 1]] \tag{3.2.2}$$

vNul: Procédure qui génère une liste de vecteurs nuls, selon le nombre d'éléments demandés.

```
> deltaNul:=proc(i,j) return 0; end proc:
> vNul:=proc(n)
    return([seq([seq(deltaNul(i,j),j=1..n)],i=1..n)]);
  end proc:
```

Liste de trois vecteurs nuls è à trois éléments.

```
> vNul(3);
```

$$[[0, 0, 0], [0, 0, 0], [0, 0, 0]] \tag{3.2.3}$$

LTM

Procédure qui calcule le terme dominant d'un élément d'un module, selon un ordre fixé sur les variables et une position déterminée.

```
> LTM:=proc(eModule,tOrd,ordre)
  local i,j,k,lt,Lm,lm,ltm,L,trouve,e;
  L:=[];

  for i from 1 to nops(eModule) do
    lt:=LT(eModule[i],tOrd);
    L:=[op(L),lt];
  od;

  e:=vE(nops(eModule));

  trouve:=false;
  k:=1;
  while (trouve=false) do

    if (L[k]<>0) then
```

```
      if (ordre='POT') then
        ltm:=L[k];
        trouve:=true;

      elif (ordre='TOP') then
        Lm:=[seq(LeadingMonomial(L[h],tOrd),h=1..nops(L))];
        lm:=LeadingMonomial(convert(Lm,`+`),tOrd);

        for j from nops(Lm) by (-1) to 1 do
          if lm=Lm[j] then
            k:=j;
          end if;
        end do;

        trouve:=true;
        ltm:=LT(L[k],tOrd);

      else
        trouve:=false;
      end if;

    else
      k:=k+1;
    end if;

  end do;
  return(expand(ltm*e[k]));
  end proc:
```

Le terme dominant d'un module, selon l'ordre lexicographique et avec la position qui prédomine sur le terme (POT: Position Over Term).

```
> LTM([5*x*y^2-y^10+3,4*x^3+2*y,16*x],plex(x,y),POT);
```

$$[5\,x\,y^2, 0, 0] \tag{3.3.1}$$

```
> LTM([x*y,0,y^2],plex(x,y),POT);
```

$$[x\,y, 0, 0] \tag{3.3.2}$$

Le terme dominant d'un module, selon l'ordre lexicographique et avec le terme qui prédomine sur la position (TOP: Term Over Position).

```
> LTM([5*x*y^2-y^10+3,4*x^3+2*y,16*x],plex(x,y),TOP);
```

$$[0, 4\,x^3, 0] \tag{3.3.3}$$

```
> LTM([x^2+2*y^2,x^2-y^2],plex(x,y),TOP);
```

(3.3.4)

$$[x^2, 0] \qquad (3.3.4)$$

siDivise et divise

siDivise: Procédure qui vérifie si un élément d'un module peut être divisé par un autre élément du même module, en évitant les divisions par zéro.
La procédure retourne vrai si oui, faux sinon.

```
> siDivise:=proc(eModule1,eModule2)
  local i,j,k,n,m;

  unassign('q');

  n:=0;
  for j from 1 to nops(eModule1) do
   if eModule1[j]=0 then n:=n+1; end if;
  end do;
  m:=0;
  for k from 1 to nops(eModule2) do
    if eModule2[k]=0 then m:=m+1; end if;
  end do;
  if (n=nops(eModule1) and m=nops(eModule2)) then
    return(true);                                    #-- 0 est un
  diviseur de 0 mais 0/0 n'est pas défini.
  end if;

  i:=1;
  while (i<=nops(eModule1)) do

    if (eModule1[i]=0 and eModule2[i]<>0) then
      return(false);

    elif (eModule1[i]<>0 and eModule2[i]=0) then
      return(false);

    elif (eModule1[i]<>0 and eModule2[i]<>0) then
      if divide(eModule1[i],eModule2[i],'q') then
        return(true);
      else
        return(false);
      end if;

    else
```

```
      i:=i+1;

    end if;

  end do;
  end proc:
```

divise: Procédure qui calcule le résultat de la division d'un élément d'un module par un autre élément du même module.
La procédure retourne le résultat obtenu ou retourne 0 si la divison ne peut être effectuée.

```
> divise:=proc(eModule1,eModule2)
  local i,j,k,n,m;

  unassign('q');

  n:=0;
  for j from 1 to nops(eModule1) do
   if eModule1[j]=0 then n:=n+1; end if;
  end do;
  m:=0;
  for k from 1 to nops(eModule2) do
   if eModule2[k]=0 then m:=m+1; end if;
  end do;
  if (n=nops(eModule1) and m=nops(eModule2)) then    #-- les 2
  éléments sont nuls
   return("indetermine");                            #-- 0 est un
  diviseur de 0 mais 0/0 n'est pas défini.
  end if;

  i:=1;
  while (i<=nops(eModule1)) do

    if (eModule1[i]=0 and eModule2[i]<>0) then
      return(0);

    elif (eModule1[i]<>0 and eModule2[i]=0) then
      return(0);

    elif (eModule1[i]<>0 and eModule2[i]<>0) then
      if divide(eModule1[i],eModule2[i],'q') then
        return(q);
      else
        return(0);
      end if;

    else
      i:=i+1;
```

```
    end if;

  end do;
  end proc:
```

Prendre deux éléments d'un même module, ltm1 et ltm2.

```
> ltm1:=LTM([5*x*y^2-y^10+3,4*x^3+2*y,16*x],plex(x,y),POT);
```

$$ltm1 := [5\,x\,y^2,\ 0,\ 0] \tag{3.4.1}$$

```
> ltm2:=LTM([x*y,0,y^2],plex(x,y),POT);
```

$$ltm2 := [x\,y,\ 0,\ 0] \tag{3.4.2}$$

Vérifier si ltm1 peut être divisé par ltm2.

```
> siDivise(ltm1,ltm2);
```

$$true \tag{3.4.3}$$

Calcul le résutat de la division de ltm1 par ltm2.

```
> divise(ltm1,ltm2);
```

$$5\,y \tag{3.4.4}$$

Exemples où la division est possible mais où le résultat de la division est indéterminé.

```
> siDivise([0,0,0],[0,0,0]);
```

$$true \tag{3.4.5}$$

```
> divise([0,0,0],[0,0,0]);
```

$$\text{"indetermine"} \tag{3.4.6}$$

Exemple où la division est impossible.

```
> siDivise([80*x,0,0],[0,y,0]);
```

$$false \tag{3.4.7}$$

Exemple où la division est possible, même lorsque la division est par zéro.

```
> siDivise([0,x^3,0],[0,x,0]);
```

$$true \tag{3.4.8}$$

```
> siDivise([x^2,y,z],[x^2,0,0]);
```

$$true \tag{3.4.9}$$

PPCM

Procédure qui calcule le plus petit commun multiple entre les monômes dominants d'un ensemble de polynômes, selon un ordre fixé sur les variables, à l'aide de la commande LCM, qui calcule le plus petit commun multiple entre deux termes.

```
> PPCM:=proc(polynome,tOrd)
    local reponse,i;
```

```
    for i from 1 to (nops(polynome)-1) do
      reponse:=lcm(LeadingMonomial(polynome[i],tOrd),
LeadingMonomial(polynome[i+1],tOrd));
    end do;
end proc:
```

Le plus petit commun multiple entre deux polynômes, en prenant l'ordre lexicographique avec priorité au degré.

```
> PPCM([-4*x^2*y^2*z^2+y^6+3*z^5,3*x^4*y+y^2],grlex(x,y,z));
```

$$z^2 y^2 x^4 \tag{3.5.1}$$

ppcmModule

Procédure qui calcule le plus petit commun muliple entre deux éléments d'un même module, selon un ordre fixé sur les variables.
La procédure retourne 0 si les deux éléments n'ont rien en commun.

```
> ppcmModule:=proc(eModule1,eModule2,tOrd)
local reponse,i,e;

e:=vE(nops(eModule1));

i:=1;
while (i<=nops(eModule1)) do
  if (eModule1[i]=0 and eModule2[i]<>0) then
    return(0);

  elif (eModule1[i]<>0 and eModule2[i]=0) then
    return(0);

  elif (eModule1[i]<>0 and eModule2[i]<>0) then
    return(expand(lcm(eModule1[i],eModule2[i])*e[i]));

  else
    i:=i+1;
  end if;
end do;

end proc:
```

Le plus petit commun multiple entre deux éléments d'un même module, en prenant l'ordre lexicographique.

```
> ppcmModule([x*y,0],[x^2,0],plex(x,y));
```

$$[x^2 y, 0] \tag{3.6.1}$$

```
> ppcmModule([x*y,0],[0,0],plex(x,y));
```

$$0 \tag{3.6.2}$$

Spolynome et SpLong

Spolynome: Procédure qui calcule le S-polynôme entre deux polynômes, selon un ordre fixé sur les variables.

```
> Spolynome:=proc(f,tOrd)
    SPolynomial(f[1],f[2],tOrd);
  end proc:
```

Calcul du S-polynôme avec la commande de Maple, Spolynomial, utilisant trois paramètres, en prenant l'ordre lexicographique avec priorité au degré.

```
> SPolynomial(x^3*y^2-x^2*y^3+x,3*x^4*y+y^2,grlex(x,y));
```

$$-3\,y^3x^3+3\,x^2-y^3 \tag{3.7.1}$$

Calcul du S-polynôme avec la procédure Spolynome, utilisant deux paramètres, en prenant l'ordre lexicographique avec priorité au degré.

```
> Spolynome([x^3*y^2-x^2*y^3+x,3*x^4*y+y^2],grlex(x,y));
```

$$-3\,y^3x^3+3\,x^2-y^3 \tag{3.7.2}$$

SpLong: Procédure qui calcule le S-polynôme entre deux polynômes, en gardant les polynômes telsquels, sans les entendre, selon un ordre fixé sur les variables.

```
> SpLong:=proc(f,g,tOrd)
  local F,G;
  return(PPCM([f,g],tOrd)/LT(f,tOrd)*f-PPCM([f,g],tOrd)/LT(g,
  tOrd)*g);
  end proc:
```

Exemples de calcul du S-polynôme au long, entre deux polynômes, en prenant l'ordre lexicographique.

```
> SpLong(x*z-y^2,x^3-z^2,plex(x,y,z));
```

$$x^2\left(x\,z-y^2\right)-z\left(x^3-z^2\right) \tag{3.7.3}$$

```
> SpLong(x*z-y^2,-x^2*y^2+z^3,plex(x,y,z));
```

$$x\,y^2\left(x\,z-y^2\right)+z\left(-x^2y^2+z^3\right) \tag{3.7.4}$$

spModule

Procédure qui calcule le S-polynôme de deux éléments d'un même module, selon un ordre fixé sur les variables et une position déterminée.

```
> spModule:=proc(eModule1,eModule2,tOrd,ordre)
  local ltm1,ltm2,ppcmM,sp,n,j;
```

```
ltm1:=LTM(eModule1,tOrd,ordre);
ltm2:=LTM(eModule2,tOrd,ordre);

ppcmM:=ppcmModule(ltm1,ltm2);

sp:=expand(divise(ppcmM,ltm1)*eModule1)-expand(divise(ppcmM,
ltm2)*eModule2);

n:=0;
for j from 1 to nops(sp) do
  if sp[j]=0 then
    n:=n+1;
  end if;
end do;
if n=nops(sp) then
  sp:=0;
end if;

return(sp);
end proc:
```

Calcul du S-polynôme entre deux éléments d'un même module, en prenant l'ordre lexicographique et tel que la position prédomine sur le terme (POT).

```
> spModule([x*y-x,x^3+y],[x^2+2*y^2,x^2-y^2],plex(x,y),POT);
```

$$\left[-2\,y^3-x^2,\ -x^2\,y+y^3+x^4+x\,y\right] \tag{3.8.1}$$

Calcul du S-polynôme entre deux éléments d'un même module, en prenant l'ordre lexicographique et tel que le terme prédomine sur la position (TOP).

```
> spModule([x*y-x,x^3+y],[x+2*y^2,x^2-y^2],plex(x,y),TOP);
```

$$\left[-x^2-2\,x\,y^2+x\,y-x,\ x\,y^2+y\right] \tag{3.8.2}$$

mulScalList et mulList

mulScalList: Procédure qui multiplie deux listes, ayant le même nombre d'éléments, en utilisant le produit scalaire, comme la multiplication de deux matrices.

```
> mulScalList:=proc(l1,l2)
  local L,M,i,j;
  L:=[];
  M:=[];
  for i from 1 to nops(l1) do
    L:=[op(L),(l1[i]*l2[i])];
```

```
end do;
expand(convert(L,`+`));
end proc:
```

Prendre deux listes ayant le même nombre d'éléments pour voir un exemple.

```
> L:=[2,4,6]; M:=[3,2,6];
```

$$L := [2, 4, 6]$$
$$M := [3, 2, 6] \quad (3.9.1)$$

Calcul de la multiplication des deux listes, selon la procédure mulScalList.

```
> mulScalList(L,M);
```

$$50 \quad (3.9.2)$$

Exemple de multiplication de deux listes ayant le même nombre d'éléments, selon la procédure mulScalList.

```
> mulScalList([x^2-x,x*y,y^2-y],[y,-x+1,0]);
```

$$0 \quad (3.9.3)$$

mulList: Procédure qui multiplie les éléments, deux à deux, de deux listes ayant le même nombre d'éléments.

```
> mulList:=proc(l1,l2)
  local L,M,i,j;
  L:=[];
  M:=[];
  for i from 1 to nops(l1) do
    L:=[op(L),expand(l1[i]*l2[i])];
  end do;
  return(L);
  end proc:
```

Prendre deux listes ayant le même nombre d'éléments pour voir un exemple.

```
> L:=[2,4,6]; M:=[3,2,6];
```

$$L := [2, 4, 6]$$
$$M := [3, 2, 6] \quad (3.9.4)$$

Calcul de la multiplication des deux listes, selon la procédure mulList.

```
> mulList(L,M);
```

$$[6, 8, 36] \quad (3.9.5)$$

Exemple de multiplication de deux listes ayant le même nombre d'éléments, selon la procédure mulList.

```
> mulList([x^2-x,x*y,y^2-y],[y,-x+1,0]);
```

$$[x^2 y - x y, x y - x^2 y, 0] \quad (3.9.6)$$

Algorithme de division de polynômes

Algorithme de division de polynômes

Procédure qui prend en entrée un polynôme à diviser, un ensemble de polynômes qui seront les diviseurs et un ordre fixé sur les variables, l'algorithme de division est effectuée.
La procédure retourne le reste de l'algortihme de division de polynômes.

```
> algorithmeDivision:=proc(polynome,liste,tOrd,compteur)
  local a,r,p,i,divisionSeProduit,c;
  c:=0;
  for i from 1 to nops(liste) do a[i]:=0 end do;
  r:=0;
  p:=polynome;

  i:=1;
  while (p<>0) do

    divisionSeProduit:=false;
    while ((i<=nops(liste)) and (divisionSeProduit=false)) do
      if divide(LT(p,tOrd),LT(liste[i],tOrd),'q') then
        a[i]:=factor(a[i]+(LT(p,tOrd)/LT(liste[i],tOrd)));
        p:=factor(p-((LT(p,tOrd)/LT(liste[i],tOrd))*liste[i]));
        divisionSeProduit:=true;
        c:=c+6;
      else
        i:=i+1;
      fi;
    end do;
    if (divisionSeProduit=false) then
      r:=factor(r+LT(p,tOrd));
      p:=factor(p-LT(p,tOrd));
      c:=c+2;
      i:=i+1;
    fi;
  end do;
  compteur:=c;
  return(r);
  end proc:
```

Algorithme de division de polynômes, avec résulat au long

Procédure qui prend en entrée un polynôme à diviser, un ensemble de polynômes qui seront les diviseurs et un ordre fixé sur les variables, ensuite, l'algorithme de division est effectuée.

La procédure retourne le polynôme f = a[1]g[1] + ... + a[s]g[s] + r, sous la forme [a [1], ... ,a[s], r].

```
> algorithmeDivisionLong:=proc(polynome,liste,tOrd,compteur)
  local a,r,p,i,divisionSeProduit,c,l;
  c:=0;

  for i from 1 to nops(liste) do a[i]:=0
  end do;

  r:=0;
  p:=polynome;

  i:=1;
  while (p<>0) do

    divisionSeProduit:=false;

    while ((i<=nops(liste)) and (divisionSeProduit=false)) do
      if divide(LT(p,tOrd),LT(liste[i],tOrd),'q') then
        a[i]:=factor(a[i]+(LT(p,tOrd)/LT(liste[i],tOrd)));
        p:=factor(p-((LT(p,tOrd)/LT(liste[i],tOrd))*liste[i]));
        divisionSeProduit:=true;
        c:=c+6;
      else
        i:=i+1;
      fi;
    end do;

    if (divisionSeProduit=false) then
      r:=factor(r+LT(p,tOrd));
      p:=factor(p-LT(p,tOrd));
      c:=c+2;
      i:=i+1;
    fi;

  end do;

  l:=[];  l:=[seq(a[i],i=1..nops(liste)),r];
  compteur:=c;
  return(l);
  end proc:
```

exemples

Dans "CLO.1", p.59, exemple 1, avec l'ordre lexicographique.

```
> algorithmeDivision(x*y^2+1,[x*y+1,y+1],plex(x,y),'c');
```

$$2 \tag{4.3.1}$$

```
> algorithmeDivisionLong(x*y^2+1,[x*y+1,y+1],plex(x,y),'c');
```

$$[y, -1, 2] \tag{4.3.2}$$

Dans "CLO.1", p.59, exemple 1, avec l'ordre lexicographique avec priorité au degré.

```
> algorithmeDivision(x*y^2+1,[x*y+1,y+1],grlex(x,y),'c');
```

$$2 \tag{4.3.3}$$

```
> algorithmeDivisionLong(x*y^2+1,[x*y+1,y+1],grlex(x,y),'c');
```

$$[y, -1, 2] \tag{4.3.4}$$

Dans "CLO.1", p.59, exemple 1, avec l'ordre lexicographique inversé avec priorité au degré.

```
> algorithmeDivision(x*y^2+1,[x*y+1,y+1],tdeg(x,y),'c');
```

$$2 \tag{4.3.5}$$

```
> algorithmeDivisionLong(x*y^2+1,[x*y+1,y+1],tdeg(x,y),'c');
```

$$[y, -1, 2] \tag{4.3.6}$$

Dans "CLO.1", p.60, exemple 2, avec l'ordre lexicographique.

```
> algorithmeDivision(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],plex(x,y),
  'c');
```

$$y^2 + x + y \tag{4.3.7}$$

```
> algorithmeDivisionLong(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],plex(x,y)
  ,'c');
```

$$[x + y, 0, y^2 + x + y] \tag{4.3.8}$$

Dans "CLO.1", p.60, exemple 2, avec l'ordre lexicographique avec priorité au degré.

```
> algorithmeDivision(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],grlex(x,y),
  'c');
```

$$x + y + 1 \tag{4.3.9}$$

```
> algorithmeDivisionLong(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],grlex(x,
  y),'c');
```

$$[x + y, 1, x + y + 1] \tag{4.3.10}$$

Algorithme de division d'éléments de Modules

Algorithme de division de polynômes appliqué aux éléments d'un module.

```
> algoDivisionModule:=proc(eModule,liste,tOrd,ordre,compteur)
  local i,j,c,a,r,m,n,divisionSeProduit,l;
```

```
c:=0;
for i from 1 to nops(liste) do a[i]:=0 end do;
r:=0;

m:=eModule;
while (m<>0) do
  i:=1;
  divisionSeProduit:=false;
  while ((i<=nops(liste)) and (divisionSeProduit=false)) do
    if siDivise(LTM(m,tOrd,ordre),LTM(liste[i],tOrd,ordre)) then
      a[i]:=factor(a[i]+divise(LTM(m,tOrd,ordre),LTM(liste[i],
tOrd,ordre)));
      m:=factor(m-expand(divise(LTM(m,tOrd,ordre),LTM(liste[i],
tOrd,ordre))*liste[i]));
      divisionSeProduit:=true;
      c:=c+6;
    else
      i:=i+1;
    fi;
  end do;

  if (divisionSeProduit=false) then
    r:=factor(r+LTM(m,tOrd,ordre));
    m:=factor(m-LTM(m,tOrd,ordre));
    c:=c+2;
  fi;

n:=0;
for j from 1 to nops(m) do
  if m[j]=0 then
    n:=n+1;
  end if;
end do;
if n=nops(m) then
  m:=0;
end if;

end do;
l:=[];  l:=[seq(a[i],i=1..nops(liste)),r];
compteur:=c;
return(l);
```

```
end proc:
```

exemples

Dans "CLO.2", p.203, exercice 3, avec l'ordre lexicographique et POT.

```
> algoDivisionModule([5*x*y^2-y^10+3,4*x^3+2*y,16*x],[[x*y+4*x,
  0,y^2],[0,y-1,x-2]],plex(x,y),POT,'c');
```

$$[5y-20,\ 2,\ [80x-y^{10}+3,\ 2+4x^3,\ 14x+4+20y^2-5y^3]] \qquad (5.1.1)$$

Dans "CLO.2", p.203, exercice 3, avec l'ordre lexicographique et TOP.

```
> algoDivisionModule([5*x*y^2-y^10+3,4*x^3+2*y,16*x],[[x*y+4*x,
  0,y^2],[0,y-1,x-2]],plex(x,y),TOP,'c');
```

$$[5y-20,\ 16,\ [80x-y^{10}+3,\ 16-14y+4x^3,\ 32+20y^2-5y^3]] \qquad (5.1.2)$$

Appartenance à un idéal

Appartenance

Procédure qui vérifie si un polynôme est dans un idéal donné, en construisant une base de Groebner d'après cet idéal et en vérifiant le reste de l'algorithme de division de polynômes, selon un ordre fixé sur les variables.

```
> Appartenance:=proc(polynome,ideal,tOrd,compteur)
  local bg,combinebg,i,j,k,sp,G,c,n,L,lesSP,cpt,rep,coef1,coef2,
  polynomes;

  L:=[];
  lesSP:=ideal;
  cpt:=0;
  G:=ideal;
  bg:=algorithmeBuchberger(ideal,tOrd,compteur); print('bg'=bg);

  combinebg:=algorithmeDivisionLong(polynome,bg,tOrd,compteur);
  print('combinebg'=combinebg);

  if op(nops(combinebg),combinebg)=0 then
    print("oui, le polynome est dans l'ideal");

    while cpt<nops(G) do
      for i from 1 to (nops(G)-1) do
        for j from i+1 to nops(G) do
```

```
          sp:=SpLong(G[i],G[j],tOrd);
          L:=algorithmeDivisionLong(expand(sp),G,tOrd,'c');
          n:=op(nops(L),L);

          if n<>0 then
            if n=expand(sp) then
              G:=[op(G),sp];
              lesSP:=[op(lesSP),sp];
            else
              G:=[op(G),n];
              lesSP:=[op(lesSP),sp];
            end if;
          else
            cpt:=cpt+1;
          end if;

        od;
      od;
    od;
print('lesSP'=lesSP);

rep:=0;
for k in 1..(nops(combinebg)-1) do
  rep:=rep+combinebg[k]*lesSP[k];
od;

coef1:=coeff(rep,ideal[1]);
coef2:=coeff(rep,ideal[2]);

polynomes:=[expand(coef1),expand(coef2)]; print('polynomes'=
polynomes);

else
  print("non, le polynome n'est pas dans l'ideal");
fi;

end proc:
```

exemples

Prenons un polynôme et un idéal pour voir un exemple.

```
> f:=-4*x^2*y^2*z^2+y^6+3*z^5; ideal:=[x*z-y^2,x^3-z^2];
```

$$f := -4\,x^2\,y^2\,z^2 + y^6 + 3\,z^5$$

$$ideal := \left[x\,z - y^2,\ x^3 - z^2\right] \tag{6.2.1}$$

Le polynôme est combinaion linéaire des générateurs donnés de l'idéal et on peut afficher des polynômes A et B tels que notre polynôme = A * idéal[1] + B * idéal[2] + 0 (reste nul).

```
> Appartenance(f,ideal,grlex(x,y,z),'c');
```

$$bg = \left[x\,z - y^2,\ x^3 - z^2,\ -x^2\,y^2 + z^3,\ x\,y^4 - z^4,\ -y^6 + z^5\right]$$

$$combinebg = \left[-4\,y^2\,(x\,z + y^2),\ 0,\ 0,\ 0,\ 3,\ 0\right]$$

"oui, le polynome est dans l'ideal"

$$lesSP = \left[x\,z - y^2,\ x^3 - z^2,\ x^2\,(x\,z - y^2) - z\,(x^3 - z^2),\ x\,y^2\,(x\,z - y^2)\right.$$
$$+ z\,(x^2\,(x\,z - y^2) - z\,(x^3 - z^2)),\ y^4\,(x\,z - y^2) + z\,(x\,y^2\,(x\,z - y^2)$$
$$\left. + z\,(x^2\,(x\,z - y^2) - z\,(x^3 - z^2)))\right]$$

$$polynomes = \left[-x\,z\,y^2 - y^4 + 3\,z^2\,x^2,\ -3\,z^3\right] \tag{6.2.2}$$

Calcul pour bien voir que le polynôme est combinaion linéaire des générateurs donnés de l'idéal.

```
> expand((-x*z*y^2-y^4+3*x^2*z^2)*ideal[1]+(-3*z^3)*ideal[2]);
```

$$-4\,x^2\,y^2\,z^2 + y^6 + 3\,z^5 \tag{6.2.3}$$

Commande de Maple qui montre que le polynôme est dans l'idéal.

```
> IdealMembership(f,<ideal>);
```

$$true \tag{6.2.4}$$

Exemple d'un polynôme qui appartient à un idéal donné.

```
> g:=y^6-z^5; ideal:=[x*z-y^2,x^3-z^2];
```

$$g := y^6 - z^5$$

$$ideal := \left[x\,z - y^2,\ x^3 - z^2\right] \tag{6.2.5}$$

```
> Appartenance(g,ideal,grlex(x,y,z),'c');
```

$$bg = \left[x\,z - y^2,\ x^3 - z^2,\ -x^2\,y^2 + z^3,\ x\,y^4 - z^4,\ -y^6 + z^5\right]$$

$$combinebg = \left[0,\ 0,\ 0,\ 0,\ -1,\ 0\right]$$

"oui, le polynome est dans l'ideal"

$$lesSP = \left[x\,z - y^2,\ x^3 - z^2,\ x^2\,(x\,z - y^2) - z\,(x^3 - z^2),\ x\,y^2\,(x\,z - y^2)\right.$$
$$+ z\,(x^2\,(x\,z - y^2) - z\,(x^3 - z^2)),\ y^4\,(x\,z - y^2) + z\,(x\,y^2\,(x\,z - y^2)$$
$$\left. + z\,(x^2\,(x\,z - y^2) - z\,(x^3 - z^2)))\right]$$

$$polynomes = \left[-z^2\,x^2 - x\,z\,y^2 - y^4,\ z^3\right] \tag{6.2.6}$$

Commande de Maple qui montre que le polynôme est dans l'idéal.

```
> IdealMembership(g,<ideal>);
```

$$true \tag{6.2.7}$$

Exemple d'un polynôme qui n'appartient pas à un idéal donné.

```
> h:=x*y-5*z^2+x; ideal:=[x*z-y^2,x^3-z^2];
```

$$h := x\,y - 5\,z^2 + x$$

$$ideal := \left[x\,z - y^2,\ x^3 - z^2\right] \tag{6.2.8}$$

```
> Appartenance(h,ideal,grlex(x,y,z),'c');
```

$$bg = \left[x\,z - y^2,\ x^3 - z^2,\ -x^2\,y^2 + z^3,\ x\,y^4 - z^4,\ -y^6 + z^5\right]$$

$$combinebg = \left[0, 0, 0, 0, 0, x\,y - 5\,z^2 + x\right]$$

"non, le polynome n'est pas dans l'ideal" (6.2.9)

Commande de Maple qui montre que le polynôme n'est pas dans l'idéal.

```
> IdealMembership(h,<ideal>);
```

$$false \tag{6.2.10}$$

Dans "CLO.1", p.98, exercice 2, avec l'ordre lexicographique avec priorité au degré.

```
> polyP:=x^3*z-2*y^2; idealP:=[x*z-y,x*y+2*z^2,y-z];
```

$$polyP := z\,x^3 - 2\,y^2$$

$$idealP := \left[x\,z - y,\ x\,y + 2\,z^2,\ y - z\right] \tag{6.2.11}$$

```
> bgP:=Basis(idealP,grlex(x,y,z));
```

$$bgP := \left[y - z,\ 2\,z^2 + z,\ x\,z - z\right] \tag{6.2.12}$$

```
> Appartenance(polyP,idealP,grlex(x,y,z),'c');
```

$$bg = \left[x\,z - y,\ x\,y + 2\,z^2,\ y - z,\ -y^2 - 2\,z^3,\ 2\,z^2 + y,\ x\,y^3 + 2\,y^2\,z^2,\ -y^4 + y^2\,z^2,\ -x\,y^2 - 2\,z\,y^2,\ -z\,y^3 + y^2\,z^2,\ y^3 - z\,y^2\right]$$

$$combinebg = \left[x^2, x, 0, 0, -x, 0, 0, 0, 0, 0, y\,(-2\,y + x)\right]$$

"non, le polynome n'est pas dans l'ideal" (6.2.13)

Commande de Maple qui montre que le polynôme n'est pas dans l'idéal.

```
> IdealMembership(polyP,<idealP>);
```

$$false \tag{6.2.14}$$

Algorithme de Buchberger pour Idéaux

Procédure qui construit une base de Groebner d'un idéal, selon un ordre fixé sur les variables, d'après la première version de l'algorithme de Buchberger.

```
> algorithmeBuchberger:=proc(ideal,tOrd,compteur)
  local G,s,n,L,i,j,cpt,c;

  G:=ideal;
  cpt:=0;
  c:=compteur;
  L:=[];
```

```
if (nops(G)<>1) then

while cpt<nops(G) do
  for i from 1 to (nops(G)-1) do
    for j from i+1 to nops(G) do
      s:=expand(SPolynomial(G[i],G[j],tOrd));
      L:=expand(algorithmeDivisionLong(s,G,tOrd,c));
      n:=op(nops(L),L);

      if n<>0 then
        G:=[op(G),n];
       else
        cpt:=cpt+1;
      end if;
    end do;
  end do;
end do;
return(G);

else
  return(G);

fi;

end proc:
```

exemples

Dans "CLO.1", p.86, exemple1, avec l'ordre lexicographique avec priorité au degré.

```
> q1:=x^3-2*x*y;
  q2:=x^2*y-2*y^2+x;
```

$$q1 := x^3 - 2\,x\,y$$

$$q2 := x^2\,y - 2\,y^2 + x \tag{7.1.1}$$

```
> unassign('ideal'); ideal:=[q1,q2];
```

$$ideal := \left[x^3 - 2\,x\,y,\ x^2\,y - 2\,y^2 + x\right] \tag{7.1.2}$$

```
> algorithmeBuchberger(ideal,grlex(x,y),'c');
```

$$\left[x^3 - 2\,x\,y,\ x^2\,y - 2\,y^2 + x,\ -x^2,\ 2\,x\,y,\ 2\,y^2 - x,\ 2\,x\,y\right] \tag{7.1.3}$$

Dans "CLO.1", p.86, exemple1, avec l'ordre lexicographique avec priorité au degré.

```
> algorithmeBuchberger([x*z-y^2,x^3-z^2],grlex(x,y,z),'c');
```

$$\left[x\,z - y^2,\ x^3 - z^2,\ -x^2\,y^2 + z^3,\ x\,y^4 - z^4,\ -y^6 + z^5\right] \tag{7.1.4}$$

Dans "CLO.1", p.92, exercice 2a, avec l'ordre lexicographique.

```
> algorithmeBuchberger([x^2*y-1,x*y^2-x],plex(x,y,z),'c');
```

$$\left[x^2 y-1, x y^2-x, -y+x^2, y^2-1\right] \tag{7.1.5}$$

Dans "CLO.1", p.92, exercice 2a, avec l'ordre lexicographique avec priorité au degré.

```
> algorithmeBuchberger([x^2*y-1,x*y^2-x],grlex(x,y,z),'c');
```

$$\left[x^2 y-1, x y^2-x, -y+x^2, y^2-1, y-x^2\right] \tag{7.1.6}$$

Dans "CLO.1", p.92, exercice 2a, avec l'ordre lexicographique inversé avec priorité au degré.

```
> algorithmeBuchberger([x^2*y-1,x*y^2-x],tdeg(x,y,z),'c');
```

$$\left[x^2 y-1, x y^2-x, -y+x^2, y^2-1, y-x^2\right] \tag{7.1.7}$$

Dans "CLO.1", p.92, exercice 2c, avec l'ordre lexicographique.

```
> algorithmeBuchberger([x-z^4,y-z^5],plex(x,y,z),'c');
```

$$\left[x-z^4, y-z^5\right] \tag{7.1.8}$$

Dans "CLO.1", p.92, exercice 2c, avec l'ordre lexicographique avec priorité au degré.

```
> algorithmeBuchberger([x-z^4,y-z^5],grlex(x,y,z),'c');
```

$$\left[x-z^4, y-z^5, -x z+y, -x^2+z^3 y, y^2 z^2-x^3\right] \tag{7.1.9}$$

Dans "CLO.1", p.92, exercice 2c, avec l'ordre lexicographique inversé avec priorité au degré.

```
> algorithmeBuchberger([x-z^4,y-z^5],tdeg(x,y,z),'c');
```

$$\left[x-z^4, y-z^5, -x z+y, -x^2+z^3 y, y^2 z^2-x^3\right] \tag{7.1.10}$$

▼ Algorithme de Buchberger pour sous-Modules

Procédure qui construit une base de Groebner d'un sous-module, selon un ordre fixé sur les variables et une position déterminée, d'après la première version de l'algorithme de Buchberger.

```
> algoBuchbergerModule:=proc(sModule,tOrd,ordre,compteur)
  local sp,G,cpt,L,i,j,s,n,c;

  G:=sModule;
  cpt:=0;
  c:=compteur;
  L:=[];
  if (nops(G)<>1) then

  while cpt<nops(G) do
    for i from 1 to (nops(G)-1) do
      for j from i+1 to nops(G) do

        s:=expand(spModule(G[i],G[j],tOrd,ordre));
        L:=expand(algoDivisionModule(s,G,tOrd,ordre,c));
```

```
      n:=op(nops(L),L);

      if n<>0 then
        G:=[op(G),n];
       else
        cpt:=cpt+1;
      end if;

    end do;
  end do;

end do;
return(G);

else
  return(G);

fi;
end proc:
```

exemples

Dans "CLO.2", p.203. exercice 3, avec l'ordre lexicographique et POT.

```
> algoBuchbergerModule([[x*y+4*x,0,y^2],[0,y-1,x-2]],plex(x,y),
  POT,'c');
```

$$[[x\,y+4\,x,\,0,\,y^2],\,[0,\,y-1,\,x-2]] \tag{8.1.1}$$

Dans "CLO.2", p.203. exercice 3, avec l'ordre lexicographique et TOP.

```
> algoBuchbergerModule([[x*y+4*x,0,y^2],[0,y-1,x-2]],plex(x,y),
  TOP,'c');
```

$$[[x\,y+4\,x,\,0,\,y^2],\,[0,\,y-1,\,x-2]] \tag{8.1.2}$$

Exemple au hasard et testé dans CoCoA, avec l'ordre lexicographique inversé avec priorité au degré et TOP.

```
> algoBuchbergerModule([[x^2,y,z],[0,x*y,2*y^2+3*x],[x*y*z,x-2,
  z^2]],tdeg(x,y,z),TOP,'c');
```

$$[[x^2,\,y,\,z],\,[0,\,x\,y,\,2\,y^2+3\,x],\,[y\,x\,z,\,x-2,\,z^2],\,[0,\,-x^2+2\,x+z\,y^2,\,-z^2\,x+y\,z^2],\,[0,\,x^3-2\,x^2,\,z^2\,x^2-x\,z^2\,y+2\,z\,y^3+3\,y\,x\,z]] \tag{8.1.3}$$

Exemple au hasard et testé dans CoCoA, avec l'ordre lexicographique inversé avec priorité au degré et POT.

```
> algoBuchbergerModule([[x^2,y,z],[0,x*y,2*y^2+3*x],[x*y*z,x-2,
```

```
   z^2]],tdeg(x,y,z),POT,'c');
```

$$[[x^2, y, z], [0, xy, 2y^2+3x], [yxz, x-2, z^2], [0, -x^2+2x+zy^2, -z^2x + yz^2], [0, x^3-2x^2, z^2x^2-xz^2y+2zy^3+3yxz], [0, 0, -4xy^2-6x^2-z^2x^2y + xy^2z^2-2zy^4-3xzy^2+2x^2y^2+3x^3]] \quad (8.1.4)$$

Base de Groebner minimale et réduite

Base de Groebner minimale

Procédure qui construit une base de Groebner minimale d'un idéal, pour un ordre fixé sur les variables.

```
> bgMinimale:=proc(ideal,tOrd,compteur)
  local bg,bgMin,i,j,q,lt,ind,indice,c;

  c:=compteur;

  bg:=algorithmeBuchberger(ideal,tOrd,c);

  lt:=[];
  for i from 1 to nops(bg) do
    lt:=[op(lt),LT(bg[i],tOrd)];
    c:=c+1;
  end do;

  ind:=[];
  for i from 1 to (nops(lt)-1) do
    for j from i+1 to nops(lt) do
      if (divide(lt[i],lt[j],'q')) then
        ind:=[op(ind),i];
      elif (not(divide(lt[i],lt[j],'q')) and divide(lt[j],lt[i],
'q')) then
        ind:=[op(ind),j];
      fi;
    end do;
  end do;

  indice:=Reverse(convert(convert(ind,set),list));

  for i from 1 to nops(indice) do
    bg:=subsop(indice[i]=NULL,bg);
  end do;
```

```
bgMin:=[];
for i from 1 to nops(bg) do
  bgMin:=[op(bgMin),bg[i]/LeadingCoefficient(LT(bg[i],tOrd),
tOrd)];
  c:=c+1;
end do;

return(bgMin);

end proc:
```

Base de Groebner réduite

Procédure qui contruit une base de Groebner réduite d'un idéal, pour un ordre fixé sur les variables.

```
> bgReduite:=proc(ideal,tOrd,compteur)
local bgRed,bgMin,i,r,c;

c:=compteur;

bgMin:=bgMinimale(ideal,tOrd,c);

for i from 1 to nops(bgMin) do

  r:=expand(algorithmeDivision(bgMin[i],subsop(i=NULL,bgMin),
tOrd,c));

  if r<>0 then
    bgMin:=subsop(i=r,bgMin);
  end if;

end do;

bgRed:=bgMin;

return(bgRed);

end proc:
```

exemples

Prendre un idéal pour voir un exemple.

```
> unassign('ideal'); ideal:=[x^3-2*x*y,x^2*y-2*y^2+x];
```

$$ideal := [x^3 - 2xy, x^2y - 2y^2 + x] \tag{9.3.1}$$

Calcul d'une base de Groebner minimale de l'idéal avec la procédure bgMinimale.

```
> bgMinimale(ideal,grlex(x,y),'c');
```

$$\left[x^2, y^2 - \frac{1}{2}x, xy\right] \tag{9.3.2}$$

Calcul d'une base de Groebner réduite de l'idéal avec la procédure bgRéduite.

```
> bgReduite(ideal,grlex(x,y),'c');
```

$$\left[x^2, y^2 - \frac{1}{2}x, xy\right] \tag{9.3.3}$$

Commande de Maple qui retourne une base de Groebner réduite, par défaut.

```
> Basis(ideal,grlex(x,y));
```

$$[2y^2 - x, xy, x^2] \tag{9.3.4}$$

Dans "CLO.1", p. 92, exercice 2a, avec l'ordre lexicographique avec priorité au degré.

```
> bgMinimale([x^2*y-1,x*y^2-x],grlex(x,y,z),'c');
```

$$[y^2 - 1, -y + x^2] \tag{9.3.5}$$

```
> bgReduite([x^2*y-1,x*y^2-x],grlex(x,y,z),'c');
```

$$[y^2 - 1, -y + x^2] \tag{9.3.6}$$

```
> Basis([x^2*y-1,x*y^2-x],grlex(x,y,z));
```

$$[y^2 - 1, -y + x^2] \tag{9.3.7}$$

Dans "CLO.1", p. 92, exercice 2b, avec l'ordre lexicographique avec priorité au degré.

```
> bgMinimale([x^2+y,x^4+2*x^2*y+y^2+3],grlex(x,y,z),'c');
```

$$[1] \tag{9.3.8}$$

```
> bgReduite([x^2+y,x^4+2*x^2*y+y^2+3],grlex(x,y,z),'c');
```

$$[1] \tag{9.3.9}$$

```
> Basis([x^2+y,x^4+2*x^2*y+y^2+3],grlex(x,y,z));
```

$$[1] \tag{9.3.10}$$

Dans "CLO.1", p. 92, exercice 2c, avec l'ordre lexicographique.

```
> bgMinimale([x-z^4,y-z^5],plex(x,y,z),'c');
```

$$[x - z^4, y - z^5] \tag{9.3.11}$$

```
> bgReduite([x-z^4,y-z^5],plex(x,y,z),'c');
```

$$[x - z^4, y - z^5] \tag{9.3.12}$$

```
> Basis([x-z^4,y-z^5],plex(x,y,z));
```

$$[y - z^5, x - z^4] \tag{9.3.13}$$

▼ Base de Groebner minimale et réduite pour sous-Module

▼ Base de Groebner minimale pour sous-modules

Procédure qui contruit une base de Groebner minimale d'un sous-module, pour un ordre fixé sur les variables et une position déterminée.

```
> bgMinModule:=proc(sModule,tOrd,ordre,compteur)
  local bg,bgMin,e,i,j,k,m,n,q,lt,ind,indice,Lc,la,c;

  c:=compteur;
  e:=vE(nops(sModule[1]));

  bg:=algoBuchbergerModule(sModule,tOrd,ordre,c);

  lt:=[];
  for i from 1 to nops(bg) do
    lt:=[op(lt),LTM(bg[i],tOrd,ordre)];
    c:=c+1;
  end do;

  ind:=[];
  for i from 1 to (nops(lt)-1) do
    for j from i+1 to nops(lt) do
      if (siDivise(lt[i],lt[j])) then
        ind:=[op(ind),i];
      elif (not(siDivise(lt[i],lt[j])) and siDivise(lt[j],lt[i])
  ) then
        ind:=[op(ind),j];
      fi;
    end do;
  end do;

  indice:=Reverse(convert(convert(ind,set),list));

  for i from 1 to nops(indice) do
    bg:=subsop(indice[i]=NULL,bg);
  end do;

  Lc:=[];
  for j from 1 to nops(bg) do
    Lc:=[op(Lc),LeadingCoefficient( LTM( bg[j],tOrd,ordre ),
```

```
tOrd )];
end do;

la:=[];
for n from 1 to nops(Lc) do
  for m from 1 to nops(Lc[n]) do
    if Lc[n][m]<>0 then
      la:=[op(la),m];
    fi;
  od;
od;

for k from 1 to nops(la) do
  bg[k][la[k]]:=bg[k][la[k]]/Lc[k][la[k]];
od;

return(bg);
end proc:
```

Base de Groebner réduite pour sous-modules

Procédure qui contruit une base de Groebner réduite d'un sous-module, pour un ordre fixé sur les variables et une position déterminée.

```
> bgRedModule:=proc(sModule,tOrd,ordre,compteur)
local bgRed,bgMin,i,n,r,c,eN;

c:=compteur;
eN:=vNul(nops(sModule[1]));

bgMin:=bgMinModule(sModule,tOrd,ordre,c);

for i from 1 to nops(bgMin) do

  n:=expand(algoDivisionModule(bgMin[i],subsop(i=NULL,bgMin),
tOrd,ordre,c));
  r:=op(nops(n),n);

  if r<>0 then
    bgMin:=subsop(i=r,bgMin);
  end if;

end do;
```

```
bgRed:=bgMin;

return(bgRed);

end proc:
```

▼ exemples

Exemple de calcul de base de Groebner minimale d'un sous-module donné, avec l'ordre lexicographique et POT.

```
> bgMinModule([[x*y+4*x,0,y^2],[0,y-1,x-2]],plex(x,y),POT,'c');
```

$$[[x\,y+4\,x,\,0,\,y^2],\,[0,\,y-1,\,x-2]] \tag{10.3.1}$$

Exemple de calcul de base de Groebner minimale d'un sous-module donné, avec l'ordre lexicographique et TOP.

```
> bgMinModule([[x*y+4*x,0,y^2],[0,y-1,x-2]],plex(x,y),TOP,'c');
```

$$[[x\,y+4\,x,\,0,\,y^2],\,[0,\,y-1,\,x-2]] \tag{10.3.2}$$

Exemple de calcul de base de Groebner réduite d'un sous-module donné, avec l'ordre lexicographique et POT.

```
> bgRedModule([[0,x*y,2*y^2+3*x],[0,-x^2+2*x+y^2*z,-z^2*x+z^2*y]
  ,[0,-y^3*z,4*y^2+6*x+z^2*y*x-2*x*y^2-3*x^2],[0,0,-4*x*y^2-6*
  x^2-z^2*x^2*y+z^2*y^2*x-2*y^4*z-3*y^2*z*x+2*x^2*y^2+3*x^3]],
  plex(x,y,z),POT,'c');
```

$$\left[[0,\,x\,y,\,2\,y^2+3\,x],\,[0,\,x^2-2\,x-z\,y^2,\,-z^2\,x+y\,z^2],\,[0,\,z\,y^3,\,4\,y^2+6\,x\right. \tag{10.3.3}$$
$$+x\,z^2\,y-2\,x\,y^2-3\,x^2],\,\left[0,\,0,\,-\frac{2}{3}\,y^4\,z-\frac{4}{3}\,x\,y^2-x\,z\,y^2-2\,x^2-\frac{1}{3}\,z^2\,x^2\,y+\frac{2}{3}\,x^2\,y^2\right.$$
$$\left.\left.+x^3\right],\,[0,\,0,\,y^2\,z^2]\right]$$

Exemple de calcul de base de Groebner réduite d'un sous-module donné, avec l'ordre lexicographique et TOP.

```
> bgRedModule([[0,x*y,2*y^2+3*x],[0,-x^2+2*x+y^2*z,-z^2*x+z^2*y]
  ,[0,-y^3*z,4*y^2+6*x+z^2*y*x-2*x*y^2-3*x^2],[0,0,-4*x*y^2-6*
  x^2-z^2*x^2*y+z^2*y^2*x-2*y^4*z-3*y^2*z*x+2*x^2*y^2+3*x^3]],
  plex(x,y,z),TOP,'c');
```

$$\left[[0,\,x\,y,\,2\,y^2+3\,x],\,[0,\,x^2-2\,x-z\,y^2,\,-z^2\,x+y\,z^2],\,\left[0,\,-z\,y^3,\,-\frac{4}{3}\,y^2-2\,x-\frac{1}{3}\,x\,z^2\,y\right.\right. \tag{10.3.4}$$
$$\left.\left.+\frac{2}{3}\,x\,y^2+x^2\right],\,[0,\,0,\,y^2\,z^2],\,[0,\,z^3\,y^5,\,0]\right]$$

Exemple de calcul de base de Groebner minimale d'un sous-module donné, avec l'ordre lexicographique avec priorité au degré et TOP.

```
> bgMinModule([[x*y+4*x,0,y^2],[0,y-1,x]],grlex(x,y,z),TOP,'c');
```

$$[[x\,y+4\,x, 0, y^2], [0, y-1, x]] \tag{10.3.5}$$

Exemple de calcul de base de Groebner réduite d'un sous-module donné, avec l'ordre lexicographique avec priorité au degré et TOP.

```
> bgRedModule([[x*y+4*x,0,y^2],[0,y-1,x]],grlex(x,y,z),TOP,'c');
```

$$[[x\,y+4\,x, 0, y^2], [0, y-1, x]] \tag{10.3.6}$$

▼ Idéaux égaux

Procédure qui vérifie si deux ensembles de polynômes engendrent un même idéal, pour un ordre fixé sur les variables.
Les idéaux seront égaux si et seulement si la base de Groebner réduite est la même.

```
> memesIdeaux:=proc(ideal1,ideal2,tOrd,compteur)
  local c;

  c:=compteur;

  if (convert(bgReduite(ideal1,tOrd,c),set)=convert(bgReduite
  (ideal2,tOrd,c),set)) then
    return(true);
  else
    return(false);
  fi;

  end proc:
```

▼ exemples

Prendre deux ensembles de polynômes pour voir un exemple.

```
> ex:=[x^2+y,x^4+2*x^2*y+y^2+3];
  ideal;
```

$$ex := [x^2+y, x^4+2\,x^2\,y+y^2+3]$$
$$[x^3-2\,x\,y, x^2\,y-2\,y^2+x] \tag{11.1.1}$$

On voit que ces deux ensembles de polynômes n'engendrent pas le même idéal, pour les trois ordres.

```
> memesIdeaux(ex,ideal,plex(x,y,z),'c');
```

false (11.1.2)

```
> memesIdeaux(ex,ideal,grlex(x,y,z),'c');
```

false (11.1.3)

```
> memesIdeaux(ex,ideal,tdeg(x,y,z),'c');
```

false (11.1.4)

Exemple où deux ensembles de polynômes engendrent le même idéal, pour les trois ordres.

```
> memesIdeaux([x^2*y-1,x*y^2-x],[x^2-y,y^2-1],plex(x,y,z),'c');
```

true (11.1.5)

```
> memesIdeaux([x^2*y-1,x*y^2-x],[x^2-y,y^2-1],grlex(x,y,z),'c');
```

true (11.1.6)

```
> memesIdeaux([x^2*y-1,x*y^2-x],[x^2-y,y^2-1],tdeg(x,y,z),'c');
```

true (11.1.7)

Exemple où deux ensembles de polynômes n'engendrent pas le même idéal avec l'ordre lexicographique, mais qui engendrent le même idéal avec l'ordre lexicographique avec priorité au degré et l'ordre lexicographique inversé avec priorité au degré.

```
> memesIdeaux([x^2*y-z*x^2+x*y-1,x^2*y-z*x^2+x*z-1],[x*y-1,x*z
  -1,y-z],plex(x,y,z),'c');
```

false (11.1.8)

```
> memesIdeaux([x^2*y-z*x^2+x*y-1,x^2*y-z*x^2+x*z-1],[x*y-1,x*z
  -1,y-z],grlex(x,y,z),'c');
```

true (11.1.9)

```
> memesIdeaux([x^2*y-z*x^2+x*y-1,x^2*y-z*x^2+x*z-1],[x*y-1,x*z
  -1,y-z],tdeg(x,y,z),'c');
```

true (11.1.10)

▼ Base minimale

Procédure qui permet de trouver une base minimale à partir d'un ensemble donné de générateurs, en éliminant les éléments superflus, selon un ordre fixé sur les variables.

```
> baseMinimale:=proc(ensemble,tOrd,compteur)
  local ens,i,L,trouve,longueur,c;

  c:=compteur;
  ens:=ensemble;

  trouve:=false;
  i:=1;

  while not trouve do
    L:=subsop(i=NULL,ens);
    longueur:=nops(ens);
```

```
    if memesIdeaux(ens,L,tOrd,c) then
      ens:=L;
      i:=1;
    else
      i:=i+1;
    fi;

    if (i>=longueur) then
      trouve:=true;
    fi;

  end do;

  return(ens);

  end proc:
```

▼ exemples

D'un ensemble de polynômes quelconque formant une base, trouvons une base minimale, selon l'ordre lexicographique avec priorité au degré.

```
> baseMinimale([x,x^2,y^3,x*y,x*z^2,z],grlex(x,y,z),'c');
```

$$[x, y^3, z] \tag{12.1.1}$$

On voit bien que cette base ne peut pas être plus minimale qu'elle ne l'est déjà, c'est donc une base minimale, selon l'ordre lexicographique avec priorité au degré.

```
> baseMinimale([x,y^3,z],grlex(x,y,z),'c');
```

$$[x, y^3, z] \tag{12.1.2}$$

Exemple de calcul d'une base minimale.

```
> ydeal:=[x^2+1,x+z,x+y^2+1];
```

$$ydeal := [x^2+1, x+z, x+y^2+1] \tag{12.1.3}$$

Calculons une base de Groebner de notre idéal, selon l'ordre lexicographique.

```
> G:=algorithmeBuchberger(ydeal,plex(x,y,z),'c');
```

$$G := [x^2+1, x+z, x+y^2+1, 1+z^2, 1+zy^2+z, z-y^2-1, 1+z^2] \tag{12.1.4}$$

Calculons une base de Groebner minimale de notre idéal, selon l'ordre lexicographique.

```
> bm:=bgMinimale(ydeal,plex(x,y,z),'c');
```

$$bm := [x+y^2+1, -z+y^2+1, 1+z^2] \tag{12.1.5}$$

Calculons une base de Groebner réduite de notre idéal, selon l'ordre lexicographique.

```
> br:=bgReduite(ydeal,plex(x,y,z),'c');
```

$$br := \left[x + y^2 + 1, -z + y^2 + 1, 1 + z^2\right] \tag{12.1.6}$$

Calculons une base minimale de notre base de Groebner du départ, pour voir que notre base de Groebner n'était pas une base minimale de Groebner.
Dans cet exemple, on voit que la base minimale de Groebner est la même que la base de Groebner minimale, selon l'ordre lexicographique, mais ce n'est pas toujours le cas.

```
> Bmin:=baseMinimale(G,plex(x,y,z),'c');
```

$$Bmin := [x + y^2 + 1, z - y^2 - 1, 1 + z^2] \tag{12.1.7}$$

Intersection d'idéaux

procédures utiles pour l'intersection d'idéaux

Procédure permettant de calculer tI + (1−t)J pour deux idéaux I et J.

```
> algoT:=proc(ideal1,ideal2)
    return([op(expand(t*ideal1)),op(expand((1-t)*ideal2))]);
  end proc:
```

Procédure qui vérifie si un terme contient la variable "t" et si oui, retire le polynôme contenant ce terme.

```
> sansT:=proc(liste)
  local i,j,L,ind,indice;

  indice:=[];
  L:=[];

  for i from 1 to nops(liste) do
    if has(expand(op(i,liste)),t) then
      indice:=[op(indice),i];
    fi;
  od;

  ind:=Reverse(indice);

  L:=liste;

  for j from 1 to nops(ind) do
    L:=subsop(op(j,ind)=NULL,L);
  od;
  return(L);
```

```
  end proc:
```

Procédure qui prend un ensemble de variables et place la variable "t" en premier.

```
> varOrdre:=proc(ordre)
  local ordret;
    return(t,op(ordre));
  end proc:
```

Procédure qui prend un ordre sur les variables et le retourne avec la variable "t" en premier.

```
> tordre:=proc(ordre)
  local om,var;
    om:=op(0,ordre);
    var:=varOrdre(ordre);
    return(om(var));
  end proc:
```

En prenant l'ordre lexicographique sur les variables x,y,z, on obtient l'ordre lexicographique sur les variables t,x,y,z.

```
> tordre(plex(x,y,z));
```

$$plex(t, x, y, z) \tag{13.1.1}$$

Intersection

Procédure qui calcule l'intersection de deux idéaux donnés, en retournant l'ensemble des polynômes qui appartiennent à la fois aux deux idéaux, selon un ordre fixé sur les variables.

```
> Intersection:=proc(ideal1,ideal2,tOrd,compteur)
  local ideal,bg,bgST,c,ordre,mat,matT,nbLignes,nbColonnes,
  retour1,retour2;

  c:=compteur;

  if op(0,tOrd)=matrix then

    mat:=op(tOrd);

    nbLignes:=nops(mat[1]);
    nbColonnes:=nops(mat[2]);
```

$$\left[(x+3y)\,(x-5y)\,\left(x^2+y\right)^3\,(x+y)^4\right] \tag{13.3.4}$$

La commande de Maple qui calcule l'intersection de deux idéaux nous donne la même chose.

```
> factor(Intersect(<pI>,<pJ>));
```

$$\left\langle -(x+3y)\,(x-5y)\,\left(x^2+y\right)^3\,(x+y)^4\right\rangle \tag{13.3.5}$$

On peut définir un ordre, nous-même, qui place la variable "t" en premier.

```
> Matrix([[1,0,0],[0,1,1],[0,0,1],[0,1,0]]);
```

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \tag{13.3.6}$$

```
> ordreT:=''matrix''([[1,1],[0,1],[1,0]],[x,y]);
```

$$ordreT := (\text{'matrix'})([[1,1],[0,1],[1,0]],[x,y]) \tag{13.3.7}$$

```
> Intersection([pI],[pJ],ordreT,'c');
```

$$\begin{aligned}&[68x^3y^6-2x^{11}y+17x^{10}y^2+186x^3y^7+68x^9y^3-x^6y^3-2x^5y^4+17y^5x^4+97y^4x^8 \\ &+62y^5x^7+186y^6x^5+62y^8x+15y^6x^6+45y^7x^4 \\ &+45y^8x^2-3x^{10}y-6x^9y^2-3x^8y^2-6x^7y^3-x^{12}+15y^9+51y^3x^8+204y^4x^7 \\ &+51y^4x^6+204y^5x^5+291y^5x^6+291y^6x^4+97y^7x^2]\end{aligned} \tag{13.3.8}$$

On retrouve la même intersection pour nos deux idéaux.

```
> factor(%);
```

$$\left[-(x+3y)\,(x-5y)\,\left(x^2+y\right)^3\,(x+y)^4\right] \tag{13.3.9}$$

Exemple de calcul d'intersection entre deux idéaux.

```
> Intersection([x*z,y*z],[z],plex(x,y,z),'c');
```

$$[yz, xz] \tag{13.3.10}$$

La commande de Maple qui calcule l'intersection de deux idéaux nous donne la même chose.

```
> Intersect(<x*z,y*z>,<z>);
```

$$\langle yz, xz\rangle \tag{13.3.11}$$

Ordres monomiaux

Ordre sur les variables de monômes des polynômes.

Définition d'ordres par des matrices.

```
> ordre1:=''matrix''([[1,1,1,1,1],[1,2,0,0,0]],[x,y,z,w,t]):
```

```
> ordre2:=''matrix''([[1,0,1,1,1],[1,2,0,0,0]],[x,y,z,w,t]):
```

Exemples où on trouve le monôme dominant d'un polynôme donné, selon les deux ordres qu'on a définit.

```
> p:=5*x^3*y+x^2*w^2*t+5*x^3*y*z*t-2*x*z*w^2*t^2+3*y^2*w^3*t;
  LeadingMonomial(p,ordre1);
  LeadingMonomial(p,ordre2);
```

$$p := 5\,y\,x^3 + x^2\,w^2\,t + 5\,x^3\,y\,z\,t - 2\,x\,z\,w^2\,t^2 + 3\,y^2\,w^3\,t$$

$$x^3\,y\,z\,t$$

$$x\,z\,w^2\,t^2 \qquad (14.1)$$

```
> q:=-2*x*z*w^3*t+3*y^2*w^3*t;
  LeadingMonomial(q,ordre1);
  LeadingMonomial(q,ordre2);
```

$$q := -2\,x\,z\,w^3\,t + 3\,y^2\,w^3\,t$$

$$y^2\,w^3\,t$$

$$x\,z\,w^3\,t \qquad (14.2)$$

```
> LeadingMonomial(x^3*y^2*z+x^2*w^4,ordre1);
  LeadingMonomial(x^3*y^2*z+x^2*w^4,ordre2);
```

$$z\,y^2\,x^3$$

$$x^2\,w^4 \qquad (14.3)$$

```
> r:=5*x^3*y+x^2*w^2*t-2*x*z*w^3*t+3*y^2*w^3*t;
  LeadingMonomial(r,ordre1);
  LeadingMonomial(r,ordre2);
```

$$r := 5\,y\,x^3 + x^2\,w^2\,t - 2\,x\,z\,w^3\,t + 3\,y^2\,w^3\,t$$

$$y^2\,w^3\,t$$

$$x\,z\,w^3\,t \qquad (14.4)$$

Le monôme dominant du polynôme suivant n'est pas déterminé par la matrice donnée dans la définition de l'ordre 1, dans ce cas (il semble que) Maple complète la matrice en morceaux de matrice identitée, autrement dit, Maple (semble) utiliser l'ordre lexicographique en cas d'égalité avec les deux premières lignes.

```
> LeadingMonomial(z^2*w^4+t^4*w^2,ordre1);
```

$$z^2\,w^4 \qquad (14.5)$$

```
> LeadingMonomial(x^2*y^2*z+x^3*w^2,ordre1);
```

$$z\,x^2\,y^2 \qquad (14.6)$$

Même si la matrice a autant de lignes que de variables, si Maple n'a pas de quoi décider, il va prendre l'ordre lexicographique pour décider.

```
> LeadingMonomial(x^3*y^2+x^2*y^3,'matrix'([[1,1],[0,0]]),[x,y]));
```

$$x^3\,y^2 \qquad (14.7)$$

```
    retour1:=[[1,seq(0,j=1..nbColonnes)],seq([0,op(mat[1][j])],
  j=1..nbLignes)];
    retour2:=[t,op(mat[2])];
    matT:=(retour1,retour2);

    ordre:='matrix'(matT);

  else
    ordre:=tordre(tOrd);

  end if;

  ideal:=algoT(ideal1,ideal2);
  bg:=Basis(ideal,ordre);
  bgST:=sansT(bg);

  return(expand(bgST));

  compteur:=c;

  end proc:
```

exemples

Dans "CLO.1", p.186, exemple, avec l'ordre lexicographique.

```
> pI:=expand((x+y)^4*(x^2+y)^2*(x-5*y));
```

$$pI := -14\,y^4x^3 + x^9 - 5\,y^7 - 26\,x^6y^3 - 19\,x^5y^4 - 38\,y^5x^3 - 19\,xy^6 - 5\,y^5x^4 - x^8y - 14\,y^2x^7 - 10\,x^2y^6 + 2\,yx^7 + y^2x^5 - 2\,x^6y^2 - x^4y^3 - 28\,x^5y^3 - 52\,y^4x^4 - 26\,y^5x^2 \qquad (13.3.1)$$

```
> pJ:=expand((x+y)*(x^2+y)^3*(x+3*y));
```

$$pJ := x^8 + 4\,yx^7 + 3\,x^6y + 12\,y^2x^5 + 3\,x^4y^2 + 12\,y^3x^3 + x^2y^3 + 4\,xy^4 + 3\,x^6y^2 + 9\,x^4y^3 + 9\,x^2y^4 + 3\,y^5 \qquad (13.3.2)$$

On trouve l'intersection des idéaux pI et pJ.

```
> Intersection([pI],[pJ],plex(x,y),'c');
```

$$[-68\,x^3y^6 + 2\,x^{11}y - 17\,x^{10}y^2 - 186\,x^3y^7 - 68\,x^9y^3 + x^6y^3 + 2\,x^5y^4 - 17\,y^5x^4 - 97\,y^4x^8 - 62\,y^5x^7 - 186\,y^6x^5 - 62\,y^8x - 15\,y^6x^6 - 45\,y^7x^4 - 45\,y^8x^2 + 3\,x^{10}y + 6\,x^9y^2 + 3\,x^8y^2 + 6\,x^7y^3 + x^{12} - 15\,y^9 - 51\,y^3x^8 - 204\,y^4x^7 - 51\,y^4x^6 - 204\,y^5x^5 - 291\,y^5x^6 - 291\,y^6x^4 - 97\,y^7x^2] \qquad (13.3.3)$$

En factorisant, on voit mieux.

```
> factor(%);
```

```
> LeadingMonomial(x^3*y^2+x^2*y^3,'matrix'([[1,1],[0,1]],[x,y]));
```

$$x^2 y^3 \tag{14.8}$$

La matrice doit avoir, au moins, autant de colonnes que le polynôme a de variables, sinon, ça ne fonctionne pas.

```
> LeadingMonomial(p,'matrix'([[1,1,1,1],[1,2,0,0]],[t,w,x,y,z]));
Error, (in type/ShortMonomialOrder) improper op or subscript
selector
```

La matrice doit avoir, au plus, autant de colonnes que le polynôme a de variables, sinon, ça ne fonctionne pas.

```
> LeadingMonomial(p,'matrix'([[1,1,1,1,1],[1,2,0,0,0]],[t,w,x,y]))
  ;
Error, (in type/ShortMonomialOrder) improper op or subscript
selector
```

Ordres monomiaux décrit par une matrice à coefficients positifs

Représentation des ordres par des matrices

Représentation de l'ordre lexicographique (plex), par une matrice 2 x 2.

```
> matLEX:=Matrix([[1,0],[0,1]]);
```

$$matLEX := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{15.1.1}$$

Représentation de l'ordre lexicographique avec priorité au degré (grlex), par une matrice 2 x 2.

```
> matGRLEX:=Matrix([[1,1],[1,0]]);
```

$$matGRLEX := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{15.1.2}$$

Représentation de l'ordre lexicographique inversé avec priorité au degré (grevlex), par une matrice 2 x 2.

```
> matGREVLEX:=Matrix([[1,1],[0,-1]]);
```

$$matGREVLEX := \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \tag{15.1.3}$$

exemples

Illustrons, par des exemples, le fait que tout ordre monomial sur Q^n, qui peut être décrit par une matrice n x n, peut aussi être décrit par une matrice à coefficients positifs.
Voyons comment trouver une telle matrice à coefficients positifs à partir d'une matrice d'un ordre monomial quelconque de façon à obtenir une matrice dont tous les coefficients sont positifs.
(Rappelons qu'une telle matrice est faite de n lignes indépendantes et de n colonnes dont le premier élément non nul à partir du haut est strictement positif.)

Procédure qui décrit l'ordre lexicographique inversé avec priorité au degré par une matrice n x n.

```
> mGREVLEX:=proc(n)
  Matrix(n,n,(i,j)->
   if (i=1) then 1
   elif (i=n-j+2) then -1
   else 0
   end if)
  end proc:
```

Matrice 2 x 2 qui décrit l'ordre lexicographique inversé avec priorité au degré, directement de sa définition.

```
> a:=mGREVLEX(2);
```

$$a := \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \tag{15.2.1}$$

Matrice 5 x 5 qui d'écrit l'ordre lexicographique inversé avec priorité au degré.

```
> A:=mGREVLEX(5);
```

$$A := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix} \tag{15.2.2}$$

Procédure qui décrit une matrice triangulaire inférieure d'ordre n x n, dont les éléments diagonaux sont tous des 1, donc strictement positifs.

```
> mTRIANG:=proc(n)
  Matrix(n,n,(i,j)->
   if (i>=j) then 1
   else 0
   end if)
  end proc:
```

Matrice 2 x 2 triangulaire inférieure, dont les éléments diagonaux sont tous des 1, donc strictement positifs.

```
> p:=mTRIANG(2);
```

$$p := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{15.2.3}$$

Matrice 5 x 5 triangulaire inférieure, dont les éléments diagonaux sont tous des 1, donc strictement positifs.

```
> P:=mTRIANG(5);
```

$$P := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{15.2.4}$$

Remarquons qu'on a déjà vu qu'une matrice B = P.A obtenue d'une matrice A, d'un ordre monomial, multipliée par une matrice P, triangulaire inférieure, dont les éléments diagonaux sont strictement positifs, est à nouveau une matrice B, d'un ordre monomial. (Dans "ROB.1", p. 57, tutoriel 9b.)

```
> B:=P.A;
```

$$B := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{15.2.5}$$

Dans le cas où n = 2, on peut voir c'est aussi la matrice qui décrit l'ordre lexicographique avec priorité au degré.

```
> b:=p.a;
```

$$b := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{15.2.6}$$

La matrice P est loin d'être unique.
On peut toujours prendre les éléments diagonaux de P égaux à 1, car tout multiplier les éléments d'une ligne par une constante strictement positive
ne change pas l'ordre décrit et laisse un élément strictement positif sur la diagonale.

Ainsi, si on raisonne ensuite sur chaque ligne et qu'on prend les entiers les plus petits possible qui vont donner des éléments positifs dans P.A, on obtient

```
> p1GREVLEX:=proc(n)
  Matrix(n,n,(i,j)->
   if ((i=j) or (j=1)) then 1
   else 0
   end if)
  end proc:
```

Matrice 2 x 2.

```
> p1:=p1GREVLEX(2);
```

$$p1 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{15.2.7}$$

Matrice 5 x 5.

```
> P1:=p1GREVLEX(5);
```

$$P1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{15.2.8}$$

```
> N1:=P1.A;
```

$$N1 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{15.2.9}$$

On obtient encore une matrice qui décrit l'ordre lexicographique avec priorité au degré, lorsque n = 2.

```
> n1:=p1.a;
```

$$n1 := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{15.2.10}$$

▼ Présentations de Modules

▼ Présentations

Procédure qui calcule une présentation de module.

```
> Presentation:=proc(ideal,tOrd,compteur)
  local G,c,cpt,comp,ct,bg,matbg,i,j,k,l,m,s,a,Laij,Sij,mSij,
  mat,estNul;

  G:=ideal;
  c:=compteur;
  cpt:=0;
  comp:=0;
  Laij:=[];
  mat:=[];
  k:=1;

  bg:=algorithmeBuchberger(G,tOrd,c);
  matbg:=convert(bg,Matrix);

  if (nops(bg)<>1) then
    while cpt<nops(bg) do

      for i from 1 to (nops(bg)-1) do
        for j from i+1 to nops(bg) do

          s:=expand(SPolynomial(bg[i],bg[j],tOrd));
          a:=expand(algorithmeDivisionLong(s,bg,tOrd,c));

          Laij:=[op(Laij),a[1..(nops(a)-1)]];

          ct:=0;
          estNul:=false;

          for l from 1 to nops(a) do
```

```
          if a[l]=0 then
            ct:=ct+1;
          end if;
        end do;
        if ct=nops(a) then
          estNul:=true;
        end if;

        Sij:=expand(PPCM([bg[i],bg[j]],tOrd)/LT(bg[i],tOrd)*vE
(nops(bg))[i]-PPCM([bg[i],bg[j]],tOrd)/LT(bg[j],tOrd)*vE(nops
(bg))[j]-Laij[k]);

        k:=k+1;

        mSij:=Transpose(convert(Sij,Matrix));

        if (expand((matbg.mSij)[1,1])<>0) or (estNul=true)
then
          null; ## ce n'est pas une syzygie
        else
          mat:=[op(mat),mSij];
        end if;

        if op(nops(a),a)<>0 then
          bg:=[op(bg),op(nops(a),a)];
          comp:=comp+1;
        else
          cpt:=cpt+1;
        end if;

      end do;
    end do;

  end do;

  return(Matrix(mat));

else
  return(Matrix(mat));
fi;

end proc:
```

▼ exemples

Dans "CLO.2", p. 237, selon l'ordre lexicographique.

```
> g[1]:=x^2-x;
  g[2]:=x*y;
  g[3]:=y^2-y;
  ideal1:=[g[1],g[2],g[3]];
```

$$g_1 := x^2 - x$$

$$g_2 := x\,y$$

$$g_3 := y^2 - y$$

$$ideal1 := \left[x^2 - x, x\,y, y^2 - y\right] \tag{16.2.1}$$

```
> bg1:=algorithmeBuchberger(ideal1,plex(x,y,z),'c');
```

$$bg1 := \left[x^2 - x, x\,y, y^2 - y\right] \tag{16.2.2}$$

```
> mbg1:=convert(bg1,Matrix);
```

$$mbg1 := \begin{bmatrix} x^2 - x & x\,y & y^2 - y \end{bmatrix} \tag{16.2.3}$$

```
> mp1:=Presentation(ideal1,plex(x,y),'c');
```

$$mp1 := \begin{bmatrix} y & y^2 - y & 0 \\ 1 - x & y - 1 & y - 1 \\ 0 & -x^2 & -x \end{bmatrix} \tag{16.2.4}$$

Vérification.

```
> [expand((mbg1.mp1)[1,1]),expand((mbg1.mp1)[1,2]),expand((mbg1.
  mp1)[1,3])];
```

$$[0, 0, 0] \tag{16.2.5}$$

Dans "BOUCH.1", exemple 4.1, la quadratique elliptique, selon l'ordre lexicographique.

```
> h[1]:=x^2-x*z-w*y;
  LT(h[1],plex(w,x,y,z));
```

$$h_1 := x^2 - x\,z - w\,y$$

$$-w\,y \tag{16.2.6}$$

```
> h[2]:=y*z-w*x-w*z;
  LT(h[2],plex(w,x,y,z));
```

$$h_2 := y\,z - w\,x - w\,z$$

$$-w\,x \tag{16.2.7}$$

L'idéal.

```
> ideal2:=[h[1],h[2]];
```

$$ideal2 := \left[x^2 - x\,z - w\,y,\ y\,z - w\,x - w\,z\right] \tag{16.2.8}$$

La base de Groebner calculée selon l'ordre lexicographique.

```
> bg2:=algorithmeBuchberger(ideal2,plex(w,x,y,z),'c');
```

$$bg2 := \left[x^2 - x\,z - w\,y,\ y\,z - w\,x - w\,z,\ -x^3 + z\,y^2 + z^2\,x,\ -x^2\,y\,z + w\,z\,y^2 + x\,z^2\,y\right] \tag{16.2.9}$$

La même base de Groebner, mais sous forme de matrice, pour les besoin du calcul suivant.

```
> mbg2:=convert(bg2,Matrix);
```

$$mbg2 := \begin{bmatrix} x^2 - x\,z - w\,y & y\,z - w\,x - w\,z & -x^3 + z\,y^2 + z^2\,x & -x^2\,y\,z + w\,z\,y^2 + x\,z^2\,y \end{bmatrix} \tag{16.2.10}$$

```
> mp2:=Presentation(ideal2,plex(w,x,y,z),'c');
```

$$mp2 := \begin{bmatrix} -x - z & -x^3 + z\,y^2 + z^2\,x & 0 \\ y & 0 & x\,z - x^2 \\ -1 & x\,z - x^2 + w\,y & w \\ 0 & 0 & -1 \end{bmatrix} \tag{16.2.11}$$

Vérication.

```
> [expand((mbg2.mp2)[1,1]),expand((mbg2.mp2)[1,2]),expand((mbg2.
  mp2)[1,3])];
```

$$[0, 0, 0] \tag{16.2.12}$$