Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON
n° 5668

Pavage des Polyominos et Bases de Grobner

Bodini Olivier

Research Report N° RR2001-51

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : `lip@ens-lyon.fr`

Pavage des Polyominos et Bases de Grobner

Bodini Olivier

Abstract

In this paper, we answer to a question of Grunbaum by proving that, for all set F of *polyominoes* (union of unit squares of a square lattice), we can find a $\mathbb{Z}$-tiling (*signed tile*) of polyominoes by copies of elements of F in polynomial time. We use for this the theory of generalised Grobner bases. For instance, we can algorithmicaly find again and extend results of Lagarias and Romero on the topic.

Keywords: Polyomino, Tiling, Standard Basis

Résumé

Nous montrons que, pour toute famille F de *polyomino* (union fini de cases d'une grille), le problème du $\mathbb{Z}$-pavage (*pavage signé*) des polycubes par des copies d'éléments de F peut être résolu en temps polynomial par l'usage de la théorie des bases de Grobner. Ceci répond à un problème posé par Grunbaum. De plus, nous pouvons ainsi retrouver et étendre de manière algorithmique les résultats obtenus par Lagarias et Romero dans ce domaine.

Mots-clés: Polyomino, Pavage, Base de Grobner

1 Introduction

Un *polycube en dimension d* (ou plus simplement un *polycube*) est une union finie de cubes unité dont les sommets sont sur les nœuds du réseau $\mathbb{Z}^d$. Soit P un polycube et F une famille de polycubes (*les paveurs*), un *$\mathbb{Z}$-pavage de P par F* est un placement de copies des paveurs pondérés par 1 ou -1 de telle sorte que tout cube de P est couvert par un poids total 1 et tout autre cube par un poids total nul. Evidement, un polycube pavable par une famille de paveurs est aussi $\mathbb{Z}$-pavable par cette famille. L'étude des $\mathbb{Z}$-pavages engendre donc des conditions nécessaires de pavabilité. J.H. Conway et J.C. Lagarias [4] ont étudié la notion de " signed tiling ", qui correspond, en dimension 2, à la définition de $\mathbb{Z}$-pavage. En particulier, ils obtiennent une condition nécessaire et suffisante pour qu'un polyomino (polycube en dimension 2) sans trou P soit $\mathbb{Z}$-pavable par une famille F de polyominos sans trou. Cette caractérisation présente néanmoins deux inconvénients; elle ne s'applique qu'aux polyominos sans trou, et elle repose sur une interprétation en termes d'appartenance d'un élément à un groupe de présentation. Ce problème est généralement ardu (voir Lagarias, Romano [10]). Nous proposons dans cette note une autre voie. Nous associons à tout polycube P de dimension d un polynôme à $n = 2d$ variables $X_1, ..., X_d, Y_1, ..., Y_d$, appelé *$P$-polynôme* que l'on notera Q_P. Nous montrons alors, qu'étant donnée une famille quelconque F de polycubes, un polycube P est $\mathbb{Z}$-pavable par F si et seulement si $Q_P \in \langle Q_{P'} \textit{ avec } P' \in E, X_1Y_1 - 1, ..., X_dY_d - 1\rangle_{\mathbb{Z}}$ où $\langle P_1, ..., P_q\rangle_{\mathbb{Z}}$ désigne l'idéal de $\mathbb{Z}[X_1, ..., X_n]$ engendré par les P_i. Nous proposons un énoncé analogue pour les *polyamants* (union finie de cellules triangulaires d'un réseau triangulaire) et les *polyhexes* (union finie de cellules hexagonales d'un réseau hexagonal). Nous porterons alors notre étude sur les moyens de déterminer quand un polynôme Q appartient à un idéal de $\mathbb{Z}[X_1, \ldots, X_n]$. Nous remontrons ici de manière élémentaire qu'il existe une famille finie F de polynômes telle qu'un polynôme Q appartient à un idéal I de $\mathbb{Z}$ si et seulement si Q est (en un sens que nous définirons) "divisible par la famille F". La famille F est ce que nous appellerons une *$\mathbb{Z}$-base* (ou *base de Grobner sur* $\mathbb{Z}$), elle ne dépend que de I. Les $\mathbb{Z}$-bases sont en fait une généralisation des bases de Grobner classiques; ces dernières furent introduites dans les années 65 par Buchberger [3] pour répondre à la question suivante : soit I un idéal de $\mathbb{C}[X_1, \ldots, X_n]$, comment déterminer si un polynôme appartient à I ?

Ceci nous amène à reconsidérer les arguments de coloration, outils très fréquemment utilisés dans la littérature pour donner des conditions nécessaires de pavabilité [7],[8],[9]. Nous définissons le concept de *coloration générale* d'une famille de paveurs F. Cette coloration regroupe à elle seule toutes les colorations généralisées définies par Conway-Lagarias [4]. De plus, la couleur générale d'un polycube P est nulle si et seulement si P est $\mathbb{Z}$-pavable par la famille F. Nous montrons ensuite qu'il est possible de déterminer la couleur générale d'un polycube par la seule connaissance des couleurs présentes sur son bord. Ceci présente une économie algorithmique substantielle dès lors qu'un polycube contient une boule de taille importante.

2 Définitions et préliminaires

Nous rappelons qu'étant donnés une subdivision S de $\mathbb{R}^d$ en cellules et A un anneau unitaire, une polycellule A-*pondérée* est une application P de S dans A à support fini. Pour toute cellule c, on appelle *poids* de P en c le nombre $P(c)$. L'espace P_A des polycellules A-pondérées a une structure naturelle de A-module libre. Les cellules de poids 1 forment clairement une base de P_A. On peut plonger canoniquement l'ensemble des polycellules dans le A-module des polycellules A-pondérées (en pondérant avec 1 les cellules couvertes par la polycellule et par 0 les autres cellules). Nous dirons alors qu'une polycellule A-pondérée P est A-*pavable* par une famille de paveurs A-pondérés si et seulement si P est une combinaison A-linéaire de translatés d'éléments de cette famille. Une conséquence immédiate de cette généralisation est que, si une polycellule P est pavable par une famille de paveurs E, alors la polycellule P est A-pavable par la famille E. Soient $P_1, ..., P_k$ des polynômes, nous noterons $\langle P_1, ..., P_k \rangle_A$ l'idéal de $A[X_1, ..., X_n]$ engendré par $P_1, ..., P_k$. On identifie naturellement le cube unité $(a_1, a_2, ..., a_d) + [0,1]^d$ de $\mathbb{R}^d$ au vecteur $(a_1, a_2, ..., a_d)$. De plus, étant donné un d-uplet $a = (a_1, ..., a_d) \in \mathbb{Z}^d$, on pose par convention $X^a = X_1^{\frac{a_1+|a_1|}{2}} ... X_d^{\frac{a_d+|a_d|}{2}} Y_1^{\frac{|a_1|-a_1}{2}} ... Y_d^{\frac{|a_d|-a_d}{2}}$ (on peut considérer en un sens que $Y_i = \frac{1}{X_i}$).

3 Le réseau cubique de $\mathbb{R}^d$

Pour tout polycube A-pondéré P, le polynôme :

$$Q_P = \sum_{a \in \mathbb{R}^d} P(a) X^a$$

de $A[X_1, ..., X_d, Y_1, ..., Y_d]$ est appelé P-*polynôme*. Par exemple, le polycube P en dimension 2 (polyomino) constitué des cases $(-1,0), (0,0), (1,0), (0,1)$ a pour P-polynôme $Q_P = X_1 + X_2 + Y_1 + 1$.

Lemme 3.1 *Pour le cas du réseau cubique de $\mathbb{R}^d$, l'espace P_A est isomorphe à :*

$$A[X_1, ..., X_d, Y_1, ..., Y_d] / \langle (X_1Y_1 - 1), ..., (X_dY_d - 1) \rangle_A.$$

preuve Il existe une unique application linéaire f de $A[X_1, ..., X_d, Y_1, ..., Y_d]$ dans P_A telle que :

$$f\left(X_1^{a_1} Y_1^{b_1} ... X_d^{a_d} Y_d^{b_d}\right)$$

est la cellule $(a_1 - b_1, ..., a_d - b_d)$ de poids 1. Il reste à montrer que $\ker(f) = \langle (X_1Y_1 - 1), ..., (X_dY_d - 1)\rangle_A$. Comme, en procédant par divisions successives par les $(X_1Y_1 - 1), ..., (X_dY_d - 1)$ dans les anneaux successifs

$$A[X_1, ..., X_{i-1}, X_{i+1}, ..., X_d, Y_1, ..., Y_d][X_i],$$

on peut écrire tout polynôme Q sous la forme $Q = R + \sum_{i=1}^{d} Q_i (X_iY_i - 1)$ avec R constitué uniquement de monômes de la forme X^a où $a \in \mathbb{Z}^d$ (c'est à dire sans présence simultanée de X_i et Y_i), on a que $f(Q)$ est le polycube vide, noté 0 (c'est à dire le polycube P de poids 0 sur tous les cubes de l'espace) si et seulement si $f(R) = 0$ (car $f(Q_i(X_iY_i - 1)) = 0$). De plus, il est clair que $f(R) = 0 \Leftrightarrow R = 0$ et que $R = 0 \Leftrightarrow Q \in \langle (X_1Y_1 - 1), ..., (X_dY_d - 1)\rangle_A$ donc $\ker(f) = \langle (X_1Y_1 - 1), ..., (X_dY_d - 1)\rangle_A$.

□

Lemme 3.2 *Soient E un ensemble de polycubes et A un anneau unitaire. Un polycube P est A-pavable par E si et seulement si*

$$Q_P \in \left\langle Q_{P'} \text{ avec } P' \in E, X_1Y_1 - 1, ..., X_dY_d - 1\right\rangle_A.$$

preuve

Par définition, un polycube P est A-pavable par E si et seulement s'il existe, pour tout $1 \leq i \leq t$, $\lambda_i \in A$, $P^i \in E$ et $a^i = \left(a_1^i, ..., a_d^i\right) \in \mathbb{Z}^d$ tels que $P = \sum_{i=1}^{t} \lambda_i P^i_{\left(a_1^i, ..., a_d^i\right)}$ où $P^i_{\left(a_1^i, ..., a_d^i\right)}$ désigne le translaté de P^i suivant le vecteur $\left(a_1^i, ..., a_d^i\right)$. On voit immédiatement que ceci est équivalent à $Q_P = \sum_{i=1}^{t} \lambda_i X^{a_i} Q_{P^i}$ dans

$$A[X_1, ..., X_d, Y_1, ..., Y_d] / \langle (X_1Y_1 - 1), ..., (X_dY_d - 1)\rangle_A$$

et donc P est A-pavable par E si et seulement si

$$Q_P \in \left\langle Q_{P'} \text{ avec } P' \in E, X_1Y_1 - 1, ..., X_dY_d - 1\right\rangle_A.$$

□

4 Le réseau hexagonal de $\mathbb{R}^2$

On appelle *hexagone unité fondamental*, que l'on note h, l'enveloppe convexe des points $(0,0), (0,1), \left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right), \left(0, \sqrt{3}\right), \left(1, \sqrt{3}\right)$. On note $[a_1, a_2]$ la cellule dont le coin inférieur gauche est le point $\left(3a_1 + \frac{3}{2}a_2, \frac{\sqrt{3}}{2}a_2\right)$ où $(a_1, a_2) \in \mathbb{Z}^2$, en d'autres termes $[a_1, a_2] = h_{\left(3a_1 + \frac{3}{2}a_2, \frac{\sqrt{3}}{2}a_2\right)}$ où $h_{\left(3a_1 + \frac{3}{2}a_2, \frac{\sqrt{3}}{2}a_2\right)}$

désigne le translaté de h suivant le vecteur $\left(3a_1+\frac{3}{2}a_2,\frac{\sqrt{3}}{2}a_2\right)$. On remarque alors que les cellules $[a_1,a_2]$ sont les cellules formées par le réseau hexagonal. Pour tout polyhexe A-pondéré P, on définit le *P-polynôme*

$$Q_P=\sum_{(a_1,a_2)\in\mathbb{Z}^2}P\left([a_1,a_2]\right)X^{(a_1,a_2)}$$

où $(a_1,a_2)\in\mathbb{Z}^2$.

Lemme 4.1 *Pour le cas du réseau hexagonal, l'espace P_A est isomorphe à*

$$A\left[X_1,X_2,Y_1,Y_2\right]/\left\langle\left(X_1Y_1-1\right),\left(X_2Y_2-1\right)\right\rangle_A.$$

preuve Il existe une unique application linéaire f de $A\left[X_1,X_2,Y_1,Y_2\right]$ dans P_A telle que : $f\left(X_1^{a_1}Y_1^{a_2}X_2^{a_3}Y_2^{a_4}\right)$ est la cellule $[a_1-a_2,a_3-a_4]$ de poids 1. f est surjective et $\ker(f)=\left\langle\left(X_1Y_1-1\right),\left(X_2Y_2-1\right)\right\rangle_A$ (même preuve que pour le lemme 3.1). $\square$

Lemme 4.2 *Soient E un ensemble de polyhexes et A un anneau unitaire. Un polyhexe P est A-pavable par E si et seulement si*

$$Q_P\in\left\langle Q_{P'}\text{ avec }P'\in E,X_1Y_1-1,X_2Y_2-1\right\rangle_A.$$

preuve La preuve est analogue à celle du lemme 3.2. $\square$

5 Le réseau triangulaire de $\mathbb{R}^2$

On appelle *triangle unité fondamental ayant la tête en haut*, que l'on note Δ, l'enveloppe convexe des points $(0,0),(0,1),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$ et *triangle unité fondamental ayant la tête en bas*, que l'on note ∇, l'enveloppe convexe des points

$$(0,1),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right),\left(\frac{3}{2},\frac{\sqrt{3}}{2}\right).$$

On note $[a_1,a_2]_\Delta$ le triangle ayant la tête en haut dont les coordonnées du coin inférieur gauche sont $(a_1+\frac{1}{2}a_2,\frac{\sqrt{3}}{2}a_2)$ où $(a_1,a_2)\in\mathbb{Z}^2$ et $[a_1,a_2]_\nabla$ le triangle ayant $[a_1,a_2]_\Delta$ à sa gauche. En d'autres termes, $[a_1,a_2]_\Delta=\Delta_{\left(a_1+\frac{1}{2}a_2,\frac{\sqrt{3}}{2}a_2\right)}$ et $[a_1,a_2]_\nabla=\nabla_{\left(a_1+\frac{1}{2}a_2,\frac{\sqrt{3}}{2}a_2\right)}$. On remarque alors que les cellules $[a_1,a_2]_\Delta$ et $[a_1,a_2]_\nabla$ sont les cellules formées par le réseau triangulaire.

Lemme 5.1 *Pour le cas du réseau triangulaire, l'espace P_A est isomorphe à*

$$A\left[X_1,X_2,Y_1,Y_2,Z\right]/\left\langle\left(X_1Y_1-1\right),\left(X_2Y_2-1\right),Z^2-1\right\rangle_A.$$

preuve L'unique application linéaire f de $A[X_1, X_2, Y_1, Y_2, Z]$ dans P_A telle que :

$$f\left(X_1^{a_1} Y_1^{a_2} X_2^{a_3} Y_2^{a_4} Z^{a_5}\right)$$

est la cellule $[a_1 - a_2, a_3 - a_4]_\Delta$ de poids 1 si a_5 est pair et la cellule $[a_1 - a_2, a_3 - a_4]_\nabla$ de poids 1 sinon. f est surjective et $\ker(f) = \left\langle (X_1Y_1 - 1), (X_2Y_2 - 1), Z^2 - 1 \right\rangle_A$ (la preuve est analogue à celle du lemme 3.1). $\square$

Pour tout polyamant A-pondéré P, on définit le *P-polynôme* :

$$Q_P = \sum_{(a_1,a_2)\in Z^2} P\left([a_1, a_2]_\Delta\right) X^{(a_1,a_2)} + \sum_{(a_1,a_2)\in Z^2} P\left([a_1, a_2]_\nabla\right) X^{(a_1,a_2)} Z.$$

Lemme 5.2 *Soient E un ensemble de polyamants et A un anneau unitaire. Un polyamant P est A-pavable par E si et seulement si*

$$Q_P \in \left\langle Q_{P'} \text{ avec } P' \in E, X_1Y_1 - 1, X_2Y_2 - 1, Z^2 - 1 \right\rangle_A.$$

preuve La preuve est analogue à celle du lemme 3.2. $\square$

Dès lors que l'on a un pavage périodique du plan, on peut définir la notion de polycellule (union finie de cellules du pavage) et il est alors possible de transcrire, par le même procédé que celui que l'on vient d'employer, le problème du A-pavage de polycellules par une famille de polycellules en termes d'appartenance à un idéal d'un anneau de polynôme sur A.

Nous nous intéressons dorénavant à l'étude spécifique des $\mathbb{Z}$-pavages, qui est à nos yeux le cas le plus intéressant. Nous allons montrer dans la section suivante qu'il est possible de répondre par un algorithme à la question : étant donnés un idéal I de $\mathbb{Z}[X_1, ..., X_n]$ et un polynôme P, P appartient-il à I ?

6 La division sur $\mathbb{Z}[X_1, ...X_n]$

Il nous faut définir préalablement un ordre total sur les monômes de $\mathbb{Z}[X_1, ..., X_n]$. Soit $\leq^*$ l'ordre lexicographique sur les n-uplets. Soit $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, nous noterons X^α le monôme $X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n}$. Alors on pose $X^\alpha \leq^* X^\beta$ si et seulement si $\alpha \leq^* \beta$. Nous vérifions aisément que $\leq^*$ est un ordre total sur les monômes de $\mathbb{Z}[X_1, ..., X_n]$ et que de plus, si nous avons $X^\alpha \leq^* X^\beta$, alors $X^{\alpha+\gamma} \leq^* X^{\beta+\gamma}$. Nous rappelons maintenant quelques termes courants dont nous avons besoin par la suite. Soit $P = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha$ un polynôme non nul de $\mathbb{Z}[X_1, ..., X_n]$:

Le *support* de P est : $S(P) = \{\alpha \in \mathbb{N}^n \textit{ tel que } a_\alpha \neq 0\}$. En particulier $S(P)$ est fini.

Le *multidegré* de P est : $m(P) = \max^*(\alpha \in S(P))$.

Le *coefficient dominant* de P est : $\mathrm{CD}(P) = a_{m(P)}$.

Le *monôme dominant* de P est : $\mathrm{MD}(P) = X^{m(P)}$.

Le *terme dominant* de P est : $\mathrm{TD}(P) = \mathrm{MD}(P).\mathrm{CD}(P)$.

Théorème 6.1 *Soit $F = (P_1, ..., P_s)$ un s-uplet de polynômes de $\mathbb{Z}[X_1, ..., X_n]$. Alors tout polynôme P de $\mathbb{Z}[X_1, ..., X_n]$ peut s'écrire de manière non unique : $P = (\sum_{k=1}^{s} Q_k P_k) + R$ où*
i) $Q_1, ..., Q_s, R \in \mathbb{Z}[X_1, ..., X_n]$.
ii) $R = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$ et $\forall \alpha \in S(R)$, $c_\alpha X^\alpha$ n'est divisible par aucun des $TD(P_1)$,..., $TD(P_s)$.

preuve La preuve découle immédiatement de l'algorithme de division généralisée suivant. □

Algorithme 6.2 *Algorithme de division généralisée On note tronc(a) la partie entière de a.*
Entrée : $(P_1, ..., P_s), P$
Sortie : $(a_1, ..., a_s), R$
$a_1 := 0, \ldots, a_s := 0, R := 0$
$Q := P$
Tant que $Q \neq 0$ Faire
$i := 1$
division := faux
Tant que ($i \leq s$ et division = faux) Faire
Si MD(P_i) divise MD(Q) et $|CD(P_i)| \leq |CD(Q)|$ Alors
$a_i := a_i + tronc(CD(Q)/CD(P_i))\,MD(Q)/MD(P_i)$
$Q := Q - (tronc(CD(Q)/CD(P_i))\,MD(Q)/MD(P_i)).P_i$
division := vrai
Sinon
$i := i + 1$
Fin si
Fin tant que
Si division := faux Alors
R := R+TD(Q)
Q := Q− TD(Q)
Fin si
Fin tant que
Imprimer $a_1, ..., a_s, R$

R est le *reste* de la division de P par $(P_1, ..., P_s)$, il sera noté $\overline{P}^{(P_1,...,P_s)}$. Cet algorithme revient en un sens à diviser "le plus possible" le polynôme P par $(P_1, ..., P_s)$ en respectant l'ordre que l'on s'est fixé sur les monômes.

Exemple 6.3 *Soient $P = X_1 X_2^2 + X_1 X_2 + X_2^2$, $(P_1 = X_2^2 - 1, P_2 = X_1 X_2 - 1)$. Alors on obtient en appliquant l'algorithme $P = P_1 \times (X_1 + 1) + P_2 + X_1 + 2$.*

Exemple 6.4 *En faisant la division de* $P = X_1X_2 - X_2^2$ *par* $(P_1 = X_1 - X_2, P_2 = X_1X_2 - 1)$, *on obtient* $\overline{P}^{(P_1,P_2)} = 0$. *Néanmoins, la division de* $P = X_1X_2 - X_2^2$ *par* $(P_1 = X_1X_2 - 1, P_2 = X_1 - X_2)$, *donne* $\overline{P}^{(P_1,P_2)} = -X_2^2+1$. *Ceci met en évidence que la division dépend de l'ordre de la famille de polynômes. Sous cette forme, la division ne permet pas de déterminer si un polynôme appartient à un idéal* I *de* $\mathbb{Z}[X_1, ..., X_n]$. *Nous rappelons que, dans* $\mathbb{R}[X]$, *un polynôme* $P \in \langle Q \rangle$ *si et seulement si* Q *divise* P. *Nous allons montrer que dans* $\mathbb{Z}[X_1, ..., X_n]$, *il existe* $Q'_1, ..., Q'_s$ *tels que* $P \in \langle Q_1, ..., Q_k \rangle$ *si et seulement si* P *est divisible par* $Q'_1, ..., Q'_s$.

7 Les idéaux monômiaux.

Nous allons utiliser un deuxième ordre sur $\mathbb{N}^n$. Etant donnés $\alpha, \beta \in \mathbb{N}^n$, on note $\alpha \leq \beta$, si pour tout $1 \leq i \leq n$, on a $\alpha_i \leq \beta_i$. L'ordre $\leq$ constitue donc un ordre partiel sur $\mathbb{N}^n$ (l'ordre terme à terme).

Définition 7.1 *I est un* idéal monômial *de* $\mathbb{Z}[X_1, ..., X_n]$ *s'il est engendré par une famille quelconque de monômes multipliés par une constante. En d'autres termes,* $I = \langle a_{\alpha,\delta} X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$.

Lemme 7.2 $\langle a_{\alpha,\delta} X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}} = \langle \mathit{pgcd}\,(a_{\gamma,\delta} ; \gamma \leq \alpha, \delta \in \mathbb{N})\, X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$ *où par convention on a posé* $\mathit{pgcd}\big((a_n)_{n\in\mathbb{N}}\big) = \mathit{pgcd}\,(a_n ; n \in \mathbb{N} \text{ et } a_i \neq 0)$ *et* $\mathit{pgcd}\,(\emptyset) = 0$.

preuve Si $cX^\beta \in \langle a_{\alpha,\delta} X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$ alors il est clair que :

$$cX^\beta \in \langle \mathrm{pgcd}\,(a_{\gamma,\delta} ; \gamma \leq \alpha, \delta \in \mathbb{N})\, X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}.$$

Réciproquement si $cX^\beta \in \langle \mathrm{pgcd}\,(a_{\gamma,\delta} ; \gamma \leq \alpha, \delta \in \mathbb{N})\, X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$ alors :

$$cX^\beta = \sum_{1 \leq i \leq s} Q_i \times \mathrm{pgcd}\,(a_{\gamma,\delta} ; \gamma \leq \alpha_i, \delta \in \mathbb{N})\, X^{\alpha_i}$$

et comme pour tout $1 \leq i \leq s$ il existe $t_i \in \mathbb{N}$, $u_1, ..., u_{t_i} \in \mathbb{Z}$ et $a_{\gamma_{i,j},\delta_{i,j}} \in \{a_{\gamma,\delta} ; \gamma \leq \alpha_i, \delta \in \mathbb{N}\}$ tels que : $\mathrm{pgcd}(a_{\gamma,\delta} ; \gamma \leq \alpha_i, \delta \in \mathbb{N}) = \sum_{1 \leq j \leq t_i} u_{i,j} a_{\gamma_{i,j},\delta_{i,j}}$,

on obtient $cX^\beta = \sum_{1 \leq i \leq s} Q_i \left(\sum_{1 \leq j \leq t_i} u_{i,j} a_{\gamma_{i,j},\delta_{i,j}} \right) X^{\alpha_i}$, soit

$$cX^\beta = \sum_{1 \leq i \leq s} \sum_{1 \leq j \leq t} a_{\gamma_{i,j},\delta_{i,j}} X^{\gamma_{i,j}} \left(u_{i,j} Q_i X^{\alpha_i - \gamma_{i,j}} \right),$$

donc $cX^\beta \in \langle a_{\alpha,\delta} X^\alpha ; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$. $\square$

Définition 7.3 *Pour tout idéal monômial*

$$I = \langle a_{\alpha,\delta} X^{\alpha}; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$$

de $\mathbb{Z}[X_1, ..., X_n]$*, on pose* $b_\alpha = pgcd(a_{\gamma,\delta}; \gamma \leq \alpha, \delta \in \mathbb{N})$*, donc* $I = \langle b_\alpha X^\alpha; \alpha \in \mathbb{N}^n \rangle_{\mathbb{Z}}$.
$\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^n\}$ *est appelé* base simple *de* I.

Remarque 7.4 *Soient* I *un idéal monômial et* $\{b_\alpha X^\alpha, \alpha \in \mathbb{N}^n\}$ *sa base simple. Les remarques suivantes sont des conséquences immédiates de la définition d'une base simple.*
i) Si $\alpha \leq \beta$*, alors on a* $b_\beta \mid b_\alpha$ *(en particulier* $b_\alpha \geq b_\beta$*).*
ii) $bX^\beta \in I$ *si et seulement si* $b_\beta \mid b$.
Si, pour $\alpha \in \mathbb{N}^n$*, il existe* $a \in \mathbb{Z} \backslash \{0\}$ *tel que* $aX^\alpha \in I$*, on obtient alors* $b_\alpha = \inf\{a_{\alpha,\delta} > 0; a_{\alpha,\delta} X^\alpha \in I\}$*, si ce n'est pas le cas alors* $b_\alpha = 0$*. En particulier, tout idéal monômial* I *possède une unique base simple.*

Lemme 7.5 *Soient* I *un idéal monômial et* $P \in \mathbb{Z}[X_1, ..., X_n]$*, nous avons les équivalences suivantes :*
i) $P \in I$.
ii) Tous les termes de P *appartiennent à* I.
iii) P *est une combinaison à coefficients entiers de monômes pondérés de* I.

preuve Il est clair que iii) $\Rightarrow$ ii) $\Rightarrow$ i). Il reste à montrer que i) $\Rightarrow$ iii), mais $P = \sum\limits_{\substack{\alpha \in \mathbb{N}^n \\ \delta \in \mathbb{N}}} P_{\alpha,\delta} a_{\alpha,\delta} X^\alpha$ et en développant les $P_{\alpha,\delta} a_{\alpha,\delta} X^\alpha$ et en regroupant les monômes, on a immédiatement la combinaison $\mathbb{Z}$-linéaire recherchée. $\square$

Corollaire 7.6 *Deux idéaux monômiaux sont identiques si et seulement s'ils ont les mêmes monômes pondérés.*

preuve Immédiat. $\square$

Théorème 7.7 *Soient* I *un idéal monômial et* $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^n\}$ *sa base simple, alors il existe un sous-ensemble fini* $B(I)$ *de* $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^n\}$ *qui engendre* I *et tel que* $aX^\alpha \in I \Leftrightarrow \exists bX^\beta \in B(I)$ *tel que* $bX^\beta \mid aX^\alpha$.

preuve Par récurrence sur le nombre n de variables. Pour $n = 1$, soit

$$I = \left\langle a_{i,j} X^i; i \in \mathbb{N}; j \in \mathbb{N} \right\rangle_{\mathbb{Z}}$$

un idéal monômial de $\mathbb{Z}[X_1]$, soit $\left\{b_i X^i; i \in \mathbb{N}\right\}$ la base simple de I. Comme $i \leq j$ implique $b_i \geq b_j$, la suite d'entiers naturels $(b_n)_{n \in \mathbb{N}}$ est stationnaire à partir d'un certain rang. Soit $i_{\min} = \inf\{i \in \mathbb{N} \text{ } tel \text{ } que \text{ } \forall j \geq i, b_j = b_i\}$, alors on a clairement que $I = \left\langle b_i X^i; i \leq i_{\min} \right\rangle_{\mathbb{Z}}$, $B(I) = \left\{b_i X^i; i \leq i_{\min}\right\}$ et $aX^i \in I \Leftrightarrow \exists bX^j \in B(I)$ tel que $bX^j \mid aX^i$. Supposons que la proposition "étant donné $I = \langle b_\alpha X^\alpha; \alpha \in \mathbb{N}^m \rangle_{\mathbb{Z}}$ où $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^m\}$ est la base simple de I, il existe un sous-ensemble fini $B(I)$ de $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^m\}$ qui engendre I et tel que $(aX^\alpha \in I) \Leftrightarrow \exists bX^\beta \in B(I)$ tel que $bX^\beta \mid aX^\alpha$ " soit vraie pour tout $m < n$. Soit $I = \langle a_{\alpha,\delta} X^\alpha; \alpha \in \mathbb{N}^n, \delta \in \mathbb{N} \rangle_{\mathbb{Z}}$ un idéal monômial de $\mathbb{Z}[X_1, ..., X_n]$ et $\{b_\alpha; \alpha \in \mathbb{N}^n\}$ sa base simple. Comme $\alpha \leq \beta$ implique $b_\alpha \geq b_\beta$, il existe $\alpha^{\min}$ un élément de $\mathbb{N}^n$ tel que $\forall \beta \geq \alpha^{\min}$, *on a* $b_\beta = b_{\alpha^{\min}}$. Pour tout $1 \leq i \leq n$ et tout $0 \leq \hat{\alpha}_i \leq \alpha_i^{\min}$, on pose

$$J_{i,\hat{\alpha}_i} = \langle b_\alpha X^\alpha |_{X_i=1}; \alpha = (\alpha_1, ..., \alpha_{i-1}, \hat{\alpha}_i, \alpha_{i+1}, \alpha_n) \rangle,$$

donc $J_{i,\hat{\alpha}_i} \in \mathbb{Z}[X_1, ..., X_{i-1}, X_{i+1}, ..., X_n]$ et

$$\{b_\alpha X^\alpha |_{X_i=1}; \alpha = (\alpha_1, ..., \alpha_{i-1}, \hat{\alpha}_i, \alpha_{i+1}, \alpha_n)\}$$

est une base simple de $J_{i,\hat{\alpha}_i}$. Par récurrence il existe un sous-ensemble fini $B(J_{i,\hat{\alpha}_i})$ de $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^n\}$ qui engendre $J_{i,\hat{\alpha}_i}$ et tel que $aX^\alpha \in J_{i,\hat{\alpha}_i} \Leftrightarrow \exists bX^\beta \in B(J_{i,\hat{\alpha}_i})$ tel que $bX^\beta \mid aX^\alpha$ Notons $A_{i,\hat{\alpha}_i} = a \in \mathbb{N}^n telque b_\alpha X^\alpha \in B_{i,\hat{\alpha}_i}$.

On va montrer que $I = I'$ avec $I' = \left\langle b_{\alpha^{\min}} X^{\alpha^{\min}}, b_\alpha X^\alpha; \alpha \in \bigcup_{1 \leq i \leq n} \bigcup_{0 \leq \hat{\alpha}_i \leq \alpha_i^{\min}-1} A_{i,\alpha_i} \right\rangle_{\mathbb{Z}}$.

Tout d'abord I' est engendré par le sous-ensemble fini $B(I') = \left\{ b_{\alpha^{\min}} X^{\alpha^{\min}}, b_\alpha X^\alpha; \alpha \in \bigcup_{1 \leq i \leq n} \bigcup_{0 \leq \hat{\alpha}_i \leq \alpha_i^{\min}-1} A_{i,\alpha_i} \right\}$ inclus dans $\{b_\alpha X^\alpha; \alpha \in \mathbb{N}^n\}$, donc $I \supset I'$. Montrons que $I \subset I'$. Par le corollaire 7.6, il suffit de montrer que, pour tout $aX^\alpha \in I$, on a $aX^\alpha \in I'$. Si $\alpha \geq \alpha^{\min}$, ceci est vérifié immédiatement. Sinon il existe $t \in \mathbb{N}$ tel que $\alpha_t < \alpha_t^{\min}$, alors par récurrence, il existe que $bX^{\alpha'} |_{X_t=1} \in B(J_{t,\alpha_t})$ tel que $bX^{\alpha'} |_{X_t=1}$ divise $aX^\alpha |_{X_t=1}$ mais alors $bX^{\alpha'} \in \left\langle b_\alpha X^\alpha;\ \alpha \in \bigcup_{1 \leq i \leq n} \bigcup_{0 \leq \hat{\alpha}_i \leq \alpha_i^{\min}-1} A_{i,\alpha_i} \right\rangle_{\mathbb{Z}}$ et $bX^{\alpha'}$ divise aX^α, donc $aX^\alpha \in I'$ et la proposition est démontrée pour n. □

Notation 7.8 *Soit I un idéal non réduit à 0, nous noterons*

$$TD(I) = a_{\alpha,\delta} X^\alpha \textit{ tel qu'il existe } P \in I \textit{ avec } TD(P) = a_{\alpha,\delta} X^\alpha.$$

Soit I un idéal non réduit à 0 alors il est clair que $\langle \mathrm{TD}(I) \rangle_{\mathbb{Z}}$ est un idéal monômial. Donc par le théorème 7.7, il existe $P_1, ..., P_t \in I$ tels que

$$\langle \mathrm{TD}(I) \rangle_{\mathbb{Z}} = \langle \mathrm{TD}(P_1), ..., \mathrm{TD}(P_t) \rangle_{\mathbb{Z}}$$

et $aX^\alpha \in \langle \mathrm{TD}(I) \rangle_{\mathbb{Z}}$ si et seulement s'il existe $i \in \mathbb{N}$; $1 \leq i \leq t$ tel que $\mathrm{TD}(P_i)$ divise aX^α.

Pour montrer le caractère fondamental du théorème 7.7, nous donnons comme corollaire le théorème de finitude de Hilbert suivant :

Théorème 7.9 *Soit I un idéal de $\mathbb{Z}[X_1, ..., X_n]$, alors I admet une base finie. En d'autres termes, il existe $t \in \mathbb{N}$ et $P_1, ..., P_t \in I$ tels que $I = \langle P_1, ..., P_t \rangle_{\mathbb{Z}}$.*

preuve Si I est réduit à 0, le théorème est immédiat. Soit I un idéal non réduit à 0, comme $\langle \mathrm{TD}\,(I)\rangle_{\mathbb{Z}}$ est un idéal monômial, il existe $P_1, ..., P_t \in I$ tels que $\langle \mathrm{TD}\,(I)\rangle_{\mathbb{Z}} = \langle \mathrm{TD}\,(P_1)\,, ..., \mathrm{TD}\,(P_t)\rangle_{\mathbb{Z}}$ et $aX^\alpha \in \langle \mathrm{TD}\,(I)\rangle_{\mathbb{Z}}$ si et seulement s'il existe $1 \leq i \leq t$ tel que $\mathrm{TD}(P_i)$ divise aX^α. Nous allons montrer que $I = \langle P_1, ..., P_t\rangle_{\mathbb{Z}}$. Tout d'abord $\langle P_1, ..., P_t\rangle_{\mathbb{Z}} \subset I$. Soit $P \in I$, en effectuant la division de P par $(P_1, ..., P_t)$, on a $P = (\sum\limits_{k=1}^{t} Q_k P_k) + R$ où $Q_1, ..., Q_t, R$ appartiennent à $\mathbb{Z}\,[X_1, ..., X_n]$, $R = \sum\limits_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$ et $\forall \alpha \in S\,(R)$, $c_\alpha X^\alpha$ n'est divisible par aucun des $\mathrm{TD}(P_1)$,...,$\mathrm{TD}(P_t)$. Donc le reste $R = P - (\sum\limits_{k=1}^{t} Q_k P_k)$ appartient à I. Si le reste R est différent de zéro alors $\mathrm{TD}\,(R) \in \langle \mathrm{TD}\,(I)\rangle_{\mathbb{Z}} = \langle \mathrm{TD}\,(P_1)\,, ..., \mathrm{TD}\,(P_t)\rangle_{\mathbb{Z}}$ et par hypothèse $\mathrm{TD}\,(R)$ est divisible par un des $\mathrm{TD}(P_i)$, ce qui contredit la définition du reste. Donc $R = 0$ et $\langle P_1, ..., P_t\rangle_{\mathbb{Z}} \supset I$. $\square$

Définition 7.10 *Un sous-ensemble fini $G = \{P_1, ..., P_t\}$ de polynômes est une* $\mathbb{Z}$-base *d'un idéal I si*
i) $\langle TD\,(I)\rangle_{\mathbb{Z}} = \langle TD\,(P_1)\,, ..., TD\,(P_t)\rangle_{\mathbb{Z}}$
ii) $aX^\alpha \in \langle TD\,(I)\rangle_{\mathbb{Z}}$ si et seulement s'il existe $1 \leq i \leq t$ vérifiant $TD(P_i)$ divise aX^α.

8 Propriétés et construction des $\mathbb{Z}$-bases

Soient $m_1, ..., m_s \in \mathbb{N}^n$, on rappelle que $\max^*(m_1, ..., m_s)$ désigne le maximum des m_i pour l'ordre lexicographique.

Proposition 8.1 *Soient $G = \{P_1, ..., P_t\}$ une $\mathbb{Z}$-base de I et $P \in \mathbb{Z}\,[X_1, ..., X_n]$. Il existe un unique $R \in \mathbb{Z}\,[X_1, ..., X_n]$ avec les propriétés suivantes :*
i) Aucun terme de R n'est divisible par l'un des $TD\,(P_1)\,, ..., TD\,(P_t)$.
ii) Il existe $Q \in I$ tel que $P = Q + R$.
En particulier R ne dépend pas de l'ordre dans lequel les P_i sont placés.

preuve i) et ii) découlent immédiatement de l'algorithme de division. Pour montrer l'unicité de R, il suffit de remarquer que si $P = Q_1 + R_1 = Q_2 + R_2$, alors $R_1 - R_2 \in I \backslash \{0\}$. Donc par la définition d'une $\mathbb{Z}$-base, $\mathrm{TD}\,(R_1 - R_2)$ est divisible par l'un des $\mathrm{TD}(P_i)$, mais ceci est impossible puisque aucun des monômes des restes R_1 et R_2 n'est divisible de $\mathrm{TD}(P_i)$. Donc $R_1 = R_2$. La fin du théorème est une conséquence de l'unicité de R. $\square$

Corollaire 8.2 *Soient $G = \{P_1, ..., P_t\}$ une $\mathbb{Z}$-base de I et $P \in \mathbb{Z}\,[X_1, ..., X_n]$. Alors $P \in I$ si et seulement si le reste de la division de P par G est zéro.*

preuve C'est une conséquence immédiate de l'unicité du reste. $\square$

Définition 8.3 *Soient P et Q deux polynômes non nuls de $\mathbb{Z}[X_1,...,X_n]$.*
i) Si $m(P)=\alpha$ et $m(Q)=\beta$, alors posons $\gamma=(\gamma_1,...,\gamma_n)$ où pour tout entier i, $\gamma_i=\max(\alpha_i,\beta_i)$. Le plus petit commun multiple *de TD(P) et TD(Q) est $ppcm(CD(P), CD(Q))X^\gamma$, et nous écrirons*

$$ppcm(TD(P), TD(Q)) = ppcm(CD(P), CD(Q))X^\gamma.$$

ii) On note $S(P,Q)$ le polynôme :

$$S(P,Q)=\frac{ppcm(TD(P), TD(Q))}{TD(P)}P-\frac{ppcm(TD(P), TD(Q))}{TD(Q)}Q.$$

iii) Soit $(u,v)\in\mathbb{N}\times\mathbb{Z}$ l'unique couple vérifiant :

$$CD(P)u+CD(Q)v=pgcd(CD(P), CD(Q))$$

avec u minimum. On définit alors $R(P,Q)=\dfrac{PuX^\gamma}{MD(P)}+\dfrac{QvX^\gamma}{MD(Q)}$.

Lemme 8.4 *Soient P et Q deux polynômes non nuls avec $m(P)=m(Q)=m$ et $c_1,c_2\in\mathbb{Z}$ tels que $m(c_1P+c_2Q)<m$, alors*

$$c_1P+c_2Q=\frac{c_1CD(P)}{ppcm(CD(P), CD(Q))}S(P,Q).$$

preuve Pour que les termes dominants de P et de Q s'annulent, il faut que $c_1=k\dfrac{\mathrm{ppcm}(\mathrm{CD}(P), \mathrm{CD}(Q))}{\mathrm{CD}(P)}$ et $c_2=-k\dfrac{\mathrm{ppcm}(\mathrm{CD}(P), \mathrm{CD}(Q))}{\mathrm{CD}(Q)}$, et comme, pour
$m(P)=m(Q)$, on a $S(P,Q)=\dfrac{\mathrm{ppcm}(\mathrm{CD}(P), \mathrm{CD}(Q))}{\mathrm{CD}(P)}P-\dfrac{\mathrm{ppcm}(\mathrm{CD}(P), \mathrm{CD}(Q))}{\mathrm{CD}(Q)}Q_j$,
le résultat s'ensuit. □

Lemme 8.5 *Soient P et Q deux polynômes non nuls avec $m(P)=m(Q)=m$, alors pour tous $c_1,c_2\in\mathbb{Z}$, il existe $k_1,k_2\in\mathbb{Z}$ tels que $c_1P+c_2Q=k_1R(P,Q)+k_2S(P,Q)$.*

preuve Prenons $k_1=\dfrac{c_1\mathrm{CD}(P)+c_2\mathrm{CD}(Q)}{\mathrm{pgcd}(\mathrm{CD}(P), \mathrm{CD}(Q))}$, alors $m(c_1P+c_2Q-k_1R(P,Q))<m$. Comme $R(P,Q)$ est une combinaison $\mathbb{Z}$-linéaire de P et Q et utilisant le lemme 8.4 on obtient $c_1P+c_2Q-k_1R(P,Q)=k_2S(P,Q)$ avec $k_2=\dfrac{\lambda\mathrm{CD}(P)}{\mathrm{ppcm}(\mathrm{CD}(P), \mathrm{CD}(Q))}$. □

Définition 8.6 *Un sous-ensemble $T=\{P_1,...,P_s\}$ de $\mathbb{Z}[X_1,...,X_n]$ vérifiant, pour tous i,j, l'existence d'un entier k tel que $P_k=R(P_i,P_j)$ sera dit est* stable *par R.*

Lemme 8.7 *Soit $T=\{P_1,...,P_s\}$ un sous-ensemble de $\mathbb{Z}[X_1,...,X_n]$ stable par R tel que pour tout $1\leq i\leq s$, $m(P_i)=m$. Si $m\left(\sum\limits_{i=1}^{s}c_iP_i\right)<m$ ($c_i\in\mathbb{Z}$), alors $\sum\limits_{i=1}^{s}c_iP_i$ est une combinaison $\mathbb{Z}$-linéaire des polynômes $S(P_i,P_j)$. De plus, chaque $S(P_i,P_j)$ a un multidegré strictement inférieur à m.*

preuve Par récurrence sur le cardinal s de T. Si $s=2$, cela résulte immédiatement du lemme 8.4. Supposons le lemme vérifié pour $s'<s$. Comme il existe k_1,k_2,P_t tels que $c_{s-1}P_{s-1}+c_sP_s=k_1P_t+k_2S(P_{s-1},P_s)$ (ceci résulte du lemme 8.5 et de la stabilité par R), $m\left(\sum\limits_{i=1}^{s-2}c_iP_i+k_1P_t+k_2S(P_{s-1},P_s)\right)<m$, donc $m\left(\sum\limits_{i=1}^{s-2}c_iP_i+k_1P_t\right)<m$. Mais par récurrence $\sum\limits_{i=1}^{s-2}c_iP_i+k_1P_t$ est une combinaison $\mathbb{Z}$-linéaire des polynômes $S(P_i,P_j)$ et comme $\sum\limits_{i=1}^{s}c_iP_i=\left(\sum\limits_{i=1}^{s-2}c_iP_i+k_1P_t\right)+k_2S(P_{s-1},P_s)$ le lemme est démontré. $\square$

Lemme 8.8 *Soit $T=\{P_1,...,P_s\}$ un sous-ensemble de $\mathbb{Z}[X_1,...,X_n]$ stable par R. Alors aX^α appartient à $\langle TD(P_1),...,TD(P_t)\rangle\mathbb{Z}$ si et seulement s'il existe i tel que $TD(P_i)$ divise aX^α.*

preuve Soit $aX^\alpha=\sum\limits_{t\leq s}Q_t\mathrm{TD}(P_{i_t})$, on va faire une récurrence sur le nombre s de polynôme dans T. Pour $s=1$, $aX^\alpha=Q_1\mathrm{TD}(P_{i_1})$, on a clairement que $\mathrm{TD}(P_i)$ divise aX^α. Pour $s=2$, $aX^\alpha=Q_1\mathrm{TD}(P_{i_1})+Q_2\mathrm{TD}(P_{i_2})$, On prend Q_1, Q_2 tels que $m(Q_1)+m(Q_2)$ soit minimum parmi les Q_1, Q_2 qui forment aX^α par combinaison linéaire. Alors :

$$aX^\alpha=\mathrm{TD}(Q_1)\,\mathrm{TD}(P_{i_1})+\mathrm{TD}(Q_2)\,\mathrm{TD}(P_{i_2})$$

et

$$\mathrm{MD}(\mathrm{TD}(Q_1)\,\mathrm{TD}(P_{i_1}))=\mathrm{MD}(\mathrm{TD}(Q_2)\,\mathrm{TD}(P_{i_2}))=\ X^\alpha,$$

donc $aX^\alpha=(\mathrm{CD}(Q_1)\,\mathrm{CD}(P_{i_1})+\mathrm{CD}(Q_2)\,\mathrm{CD}(P_{i_2}))\,X^\alpha$ et on a $\mathrm{MD}(P_{i_1})\mid X^\alpha$ et $\mathrm{MD}(P_{i_2})\mid X^\alpha$ on en conclut que $\mathrm{MD}(R(P_{i_1},P_{i_2}))\,|X^\alpha$. De plus, comme

$$\mathrm{CD}(R(P_{i_1},P_{i_2}))=\mathrm{pgcd}(\mathrm{CD}(P_{i_1}),\mathrm{CD}(P_{i_2}))\,,$$

on a donc :

$$\mathrm{CD}(R(P_{i_1},P_{i_2}))\mid\ (\mathrm{CD}(Q_1)\,\mathrm{CD}(P_{i_1})+\mathrm{CD}(Q_2)\,\mathrm{CD}(P_{i_2}))$$

il en résulte que $\mathrm{TD}(R(P_{i_1},P_{i_2}))\mid aX^\alpha$ et $R(P_{i_1},P_{i_2})=P_t$ car T est stable par R. Supposons que, pour tout $a'X^{\alpha'}=\sum\limits_{t<s}Q'_t\mathrm{TD}\left(P_{i'_t}\right)$, il existe i tel

que $\mathrm{TD}(P_i)$ divise $a'X^{\alpha'}$. Montrons que, si $aX^\alpha = \sum_{t\leq s} Q_t \mathrm{TD}\left(P_{i_t}\right)$, alors il existe i tel que $\mathrm{TD}(P_i)$ divise aX^α. On prend les Q_i tels que $\sum_i m\left(Q_i\right)$ soit minimum parmi les Q_i qui forment aX^α par combinaison linéaire. Alors $aX^\alpha = \sum_{t\leq s} \mathrm{TD}\left(Q_t\right) \mathrm{TD}\left(P_{i_t}\right)$ et pour tout t, $\mathrm{MD}\left(\mathrm{TD}\left(Q_t\right)\mathrm{TD}\left(P_{i_t}\right)\right) = X^\alpha$. Donc $aX^\alpha - \mathrm{TD}\left(Q_s\right)\mathrm{TD}\left(P_{i_s}\right) = a'X^\alpha = \sum_{t<s} \mathrm{TD}\left(Q_t\right)\mathrm{TD}\left(P_{i_t}\right)$ et par récurrence il existe $P \in T$ tel que $\mathrm{TD}(P)$ divise $a'X^\alpha$. Mais alors $aX^\alpha = \mathrm{TD}\left(Q_s\right)\mathrm{TD}\left(P_{i_s}\right) + a'X^\alpha = \mathrm{TD}\left(Q_s\right)\mathrm{TD}\left(P_{i_s}\right) + kX^\beta \mathrm{TD}\left(P\right)$ et par hypothèse de récurrence, il existe $P' \in T$ tel que $\mathrm{TD}(P')$ divise aX^α. $\square$

Théorème 8.9 *Soient I un idéal et $G = \{P_1, ..., P_t\}$ une famille génératrice de I stable par R telle que pour toute paire $i \neq j$, le reste de la division de $S\left(P_i, P_j\right)$ par G (ordonné de manière quelconque) est nul alors G est une $\mathbb{Z}$-base de I.*

preuve Soit $P \in I$, on veut montrer que si le reste de la division de $S\left(P_i, P_j\right)$ par G est nul pour tous $i \neq j$ alors $\mathrm{TD}(P) \in \left\langle \mathrm{TD}\left(P_1\right), ..., \mathrm{TD}\left(P_t\right)\right\rangle_{\mathbb{Z}}$ et il existe $1 \leq i \leq t$ tel que $\mathrm{TD}(P_i)$ divise $\mathrm{TD}(P)$. $P = \left(\sum_{k=1}^{t} Q_k P_k\right)$ donc $m\left(P\right) \leq \max^*\left(m\left(P_i Q_i\right)\right)$. Parmi toutes les expressions de P comme combinaison linéaire de P_i ($P = \left(\sum_{k=1}^{t} Q_k P_k\right)$), il en existe une (au moins) telle que $\max^*\left(m\left(P_i Q_i\right)\right) = m$ soit minimum pour l'ordre lexicographique. Nous allons montrer que nécessairement $m\left(P\right) = m$. Si tel est le cas, $m\left(P\right) = \max^*\left(m\left(P_i Q_i\right)\right)$ et donc $\mathrm{TD}(P)$ appartient à $\left\langle \mathrm{TD}\left(P_1\right), ..., \mathrm{TD}\left(P_t\right)\right\rangle_{\mathbb{Z}}$. Procédons par l'absurde. Supposons que $m\left(P\right) < m$. On peut réécrire P comme suit : $P = \sum_{m(P_iQ_i)=m} Q_i P_i + \sum_{m(P_iQ_i)<m} Q_i P_i$, donc :

$$P = \sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i + \sum_{m(P_iQ_i)=m} (Q_i - \mathrm{TD}(Q_i))P_i + \sum_{m(P_iQ_i)<m} Q_i P_i \tag{1}$$

et comme $m\left(P\right) < m$, on a nécessairement $m\left(\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i\right) < m$. Mais $\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i = \sum_{m(P_iQ_i)=m} \mathrm{CD}(Q_i)\mathrm{MD}\left(Q_i\right)P_i$ vérifie les hypothèses du lemme 8.7 avec $c_i = \mathrm{CD}\left(Q_i\right)$ et $T = \left\{\mathrm{MD}\left(Q_i\right)P_i \textit{ tel que } m\left(P_iQ_i\right) = m\right\}$, donc

$\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i$ est une combinaison $\mathbb{Z}$-linéaire des polynômes

$$S\left(\mathrm{MD}\left(Q_j\right)P_j, \mathrm{MD}\left(Q_k\right)P_k\right) = X^{m-\gamma_{j,k}} S\left(P_j, P_k\right)$$

où $\gamma_{i,j}$ est le plus petit exposant tel que $\mathrm{MD}(P_i)$ et $\mathrm{MD}(P_j)$ divise $X^{\gamma_{i,j}}$. Donc il existe des constantes $c_{j,k} \in \mathbb{Z}$ telles que $\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i = \sum_{j,k} c_{j,k} X^{m-\gamma_{j,k}} S(P_j, P_k)$. Or $S(P_j, P_k) = \sum_{i=1}^{t} Q_{i,j,k} P_i$ où $Q_{i,j,k} \in \mathbb{Z}[X_1, ..., X_n]$ car le reste de la division de $S(P_j, P_k)$ par G est zéro. L'algorithme de division donne de plus que $m(Q_{i,j,k}P_i) \leq m(S(P_j, P_k))$. On peut écrire $X^{m-\gamma_{j,k}} S(P_j, P_k) = \sum_{i=1}^{t} Q'_{i,j,k} P_i$ où $Q'_{i,j,k} = X^{m-\gamma_{j,k}} Q_{i,j,k}$ et donc $m\left(Q'_{i,j,k}P_i\right) \leq m\left(X^{m-\gamma_{j,k}} S(P_j, P_k)\right) < m$. Donc $\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i = \sum_{j,k} c_{j,k} X^{m-\gamma_{j,k}} S(P_j, P_k) = \sum_{j,k} c_{j,k} \left(\sum_i Q'_{i,j,k} P_i\right) = \sum_i Q''_i P_i$ et pour tout i, $m(Q''_i P_i) < m$. Finalement, en substituant $\sum_{m(P_iQ_i)=m} \mathrm{TD}(Q_i)P_i$ par $\sum_i Q''_i P_i$ dans (1), on a P sous forme d'une combinaison linéaire des P_i avec $m(Q''_i P_i) < m$, ce qui contredit la minimalité de m. $\square$

Algorithme 8.10 *Soit $I = \langle P_1, ..., P_t \rangle_z$ un idéal non trivial de $\mathbb{Z}[X_1, ..., X_n]$, l'algorithme suivant construit une base finie de I stable par R en moins de t itérations.*
Entrée : $F := (P_1, ..., P_t)$
Sortie : une base $G := \{Q_1, ..., Q_s\}$ stable par R
$G := F$
Répéter $G' := G$
Pour chaque paire $\{P, Q\}$, $P \neq Q$ dans G' Faire
Si il n'existe pas $Q' \in G'$ tel que $Q' = R(P, Q)$
alors $G := G \cup \{R(P, Q)\}$
Fin si
Fin pour
Jusqu'à $G := G'$
Imprimer G.

preuve Il est clair que l'algorithme s'arrête quand G est stable par R. De plus $R(P, Q) \in I$, donc G est bien une base de I. Il reste à montrer que l'algorithme s'arrête au bout d'au plus t boucles. Mais $\mathrm{CD}(R(P, Q))$ divise le pgcd de $\mathrm{CD}(P)$ et $\mathrm{CD}(Q)$ et donc au niveau de la $t^{\text{ième}}$ itération $\mathrm{CD}(R(P, Q))$ divise $\mathrm{pgcd}(\mathrm{CD}(P_i), 1 \leq i \leq |G|)$, avec un peu d'attention on montre alors qu'il existe $Q' \in G'$ tel que Q' divise $R(P, Q)$. $\square$

Notation 8.11 *Soit $F := (P_1, ..., P_t)$ une suite de polyominos, on note* Complété(F) *le résultat de l'algorithme précédent.*

Algorithme 8.12 *Soit* $I = \langle P_1, ..., P_t \rangle_{\mathbb{Z}}$ *un idéal non trivial. Une* $\mathbb{Z}$*-base peut être construite en un nombre fini d'étapes par l'algorithme suivant :*
Entrée : $F := (P_1, ..., P_t)$
Sortie : une $\mathbb{Z}$*-base* $G := \{Q_1, ..., Q_s\}$
$G := F$
Répéter $G' := G$
Pour chaque paire $\{P, Q\}$, $P \neq Q$ *dans* G' *Faire*
S *:= reste de la division de* $S(P, Q)$ *par* G'
Si $S \neq 0$
alors G *:= Complété(*$G \cup \{S\}$*)*
Fin si
Fin pour
Jusqu'à $G = G'$
Imprimer G.

preuve Il est clair que, quand l'algorithme s'arrête, G est une $\mathbb{Z}$-base. Il reste à montrer que l'algorithme est fini. Si S est non nul, alors

$$\langle \mathrm{TD}\,(G) \rangle_{\mathbb{Z}} \subset \langle \mathrm{TD}\,(\text{Complété}\,(G \cup \{S\})) \rangle_{\mathbb{Z}}\,,$$

nous allons montrer que nous avons une inclusion stricte. En effet, S est un reste non nul d'une division par G. $\mathrm{TD}(S)$ n'est pas divisible par les termes dominants de G. Donc $\mathrm{TD}\,(S) \notin \langle \mathrm{TD}\,(G) \rangle_{\mathbb{Z}}$ et $\mathrm{TD}\,(S) \in \langle \mathrm{TD}\,(\text{Complété}\,(G \cup \{S\})) \rangle_{\mathbb{Z}}$. Donc la suite des $\langle \mathrm{TD}\,(G) \rangle_{\mathbb{Z}}$ obtenue en faisant tourner l'algorithme est une suite strictement croissante. Comme $\mathbb{Z}\,[X_1, ..., X_n]$ est nœthérien, toute suite croissante infinie d'idéaux est stationnaire. Donc l'algorithme est fini. $\square$

Remarque 8.13 *Bien que l'obtention d'une* $\mathbb{Z}$*-base soit effective par l'algorithme 8.12, le temps d'exécution de celui-ci peut se révéler particulièrement long, ce qui met en péril l'efficacité générale d'un tel procédé.*

Remarque 8.14 *Il est clair que si l'on remplace* $\mathbb{Z}$ *par un anneau euclidien calculable les résultats précédents se transcrivent immédiatement.*

Revenons maintenant au problème de $\mathbb{Z}$-pavage.

Exemple 8.15 *Etudions le cas élémentaire du* $\mathbb{Z}$*-pavage des polycubes par des dominos (ensemble de 2 cubes de dimension* n *collés par une face de dimension* $n-1$*). La transcription du problème en termes de* $\mathbb{Z}$*-base donne : Un polycube* P *est* $\mathbb{Z}$*-pavable par des dominos si et seulement si* Q_P *est divisible par*

$$\{Y_1 - 1, ..., Y_d - 1, X_1 - 1, ..., X_d - 1\}$$

(qui est clairement une $\mathbb{Z}$*-base de l'idéal associé aux dominos). Donc* P *est* $\mathbb{Z}$*-pavable par des dominos si et seulement il a autant de cubes blancs que noirs (pour la coloration en échiquier de l'espace).*

Il paraît maintenant intéressant d'introduire la notion suivante :

Définition 8.16 *Soient E, E' et C des familles de polycubes, E et E' sont des A-*palettes *(A est un anneau unitaire)* équivalentes sur *C si et seulement si $\forall P \in C$, P est A-pavable par E si et seulement si P est A-pavable par E'.*

La notion de $\mathbb{Z}$-base permet pour toute famille de polycubes E de trouver une nouvelle famille E' (famille associée à la $\mathbb{Z}$-base) qui soit une $\mathbb{Z}$-palette équivalente à E pour l'ensemble des polycubes qui soit bien plus pratique dans le sens où celle-ci possède un algorithme de pavage simple (qui découle de l'algorithme de division).

9 Relations entre les différents types de pavage.

Nous nous proposons de montrer dans cette partie, l'importance que peut jouer la géométrie algébrique dans la théorie des pavages. Nous proposons à cet effet des résultats analogues à ceux obtenus indépendamment par Barnes [1] mais une optique différente qui nous permet dorénavant une approche algorithmique par les bases de Grobner. Nous montrons que, dans un sens, toutes les colorations classiques (voir définition ci-dessous) découlent des points d'une variété algébrique associée à l'ensemble des paveurs. Dans la dernière section, nous définirons de manière un peu différente la notion de couleur et proposerons une élégante condition nécessaire et suffisante pour qu'un polycube soit $\mathbb{C}$-pavable (resp. $\mathbb{Z}$-pavable) par un ensemble de paveurs. Les résultats suivants sont applicables moyennant modifications aux polyhexes et aux polyamants.

Soit E une famille de polycubes, on note $I_{E,K}$ l'idéal

$$\langle Q_P; P \in E, X_1Y_1 - 1, ..., X_dY_d - 1\rangle_K$$

où K est un corps. Nous employons dans ce chapitre des résultats classiques sur les bases de Grobner. Nous renvoyons le lecteur non spécialiste au livre Ideals,varieties and algorithms de D. Cox, J. Little, D. O'Shea [3].

Commençons par un résultat élémentaire d'algèbre commutative :

Théorème 9.1 *Soient $Q \in \mathbb{Q}[X_1, ..., X_n]$ et $Q_1, ..., Q_s \in \mathbb{Q}[X_1, ..., X_n]$ alors les propositions suivantes sont équivalentes :*
i) $Q \in \langle Q_1, ..., Q_s\rangle_{\mathbb{C}}$
ii) $Q \in \langle Q_1, ..., Q_s\rangle_{\mathbb{R}}$
iii) $Q \in \langle Q_1, ..., Q_s\rangle_{\mathbb{Q}}$

preuve Il est clair que iii) $\Rightarrow$ ii) $\Rightarrow$ i). Montrons que i) $\Rightarrow$ iii). L'algorithme de Buchberger de construction des bases de Grobner permet d'affirmer qu'il existe une base de Grobner $Q\prime_1, \ldots, Q\prime_t$ où $Q\prime_1, \ldots, Q\prime_t$ appartiennent à $\mathbb{Q}[X_1, ..., X_n]$ donc $Q \in \langle Q_1, ..., Q_s\rangle_{\mathbb{C}}$ si et seulement s'il existe $Q''_1, \ldots, Q''_t$

appartenant à $\mathbb{C}[X_1,...,X_n]$ tels que $Q = \sum_{i=1}^{t} Q'_i Q''_i$, mais en développant les monômes de $Q''_i = \sum_{\alpha\in\mathbb{N}^n} a_{i,\alpha} X^\alpha$ on obtient $Q = \sum_{i=1}^{t} \sum_{\alpha\in\mathbb{N}^n} a_{i,\alpha} X^\alpha Q_i$ et les monômes à coefficients irrationnels s'annulent car $Q \in \mathbb{Q}[X_1,...,X_n]$. Donc en prenant $Q'''_i = \sum_{\substack{\alpha\in\mathbb{N}^n \\ a_{i,\alpha}\in Q}} a_{i,\alpha} X^\alpha$, on a $Q = \sum_{i=1}^{t} Q'_i Q'''_i$. $\square$

Théorème 9.2 *Soient P un polycube et E une famille de polycubes, les propositions suivantes sont équivalentes :*
i) P est $\mathbb{Q}$-pavable par E.
ii) P est $\mathbb{R}$-pavable par E.
iii) P est $\mathbb{C}$-pavable par E.

preuve La preuve est une conséquence facile du théorème 9.1. $\square$

Théorème 9.3 *Soient P un polycube et $E = \{P_1,...,P_s\}$ une famille de polycubes. P est $\mathbb{C}$-pavable par E si et seulement s'il existe un entier m dépendant de $P_1,...,P_s$ et P tels que mP (la superposition de m copies de P) est $\mathbb{Z}$-pavable par E.*

preuve Il est clair que si mP est $\mathbb{Z}$-pavable par E alors P est $\mathbb{C}$-pavable par E. Montrons la réciproque. Si P est $\mathbb{C}$-pavable par E, le théorème précédent implique que P est $\mathbb{Q}$-pavable par E, donc il existe des polynômes Q_i à coefficients rationnels tels que $Q_P = \sum_{i=1}^{s} Q_i Q_{P_i} + \sum_{i=1}^{d} Q_{s+i}(X_i Y_i - 1)$. Mais si l'on prend m le ppcm des dénominateurs de tous les coefficients des Q_i, mQ_P est donc une combinaison $\mathbb{Z}[X_1,...,X_d,Y_1,...,Y_d]$-linéaire. Or $mQ_P = Q_{mP}$ et donc mP est $\mathbb{Z}$-pavable par E. $\square$

La détermination de la constante m est effective par l'algorithme de construction des $\mathbb{Z}$-bases, néanmoins cette constante peut se révéler particulièrement grande (2^{2^d} où d est le degré maximum des polynômes).

10 Coloration dans un corps K.

Dans toute cette section K désigne un corps.

Définition 10.1 *Soit E un ensemble de K-paveurs. Une E-*coloration *est une forme K-linéaire χ de $K[X_1,...,X_d,Y_1,...,Y_d]/\langle X_1Y_1-1,...,X_dY_d-1\rangle_K$ telle que, pour tout $P\in E$ et tout $\alpha\in\mathbb{Z}^d$, on a $\chi(X^\alpha Q_P) = 0$.*

Définition 10.2 *Soit χ une coloration. Un polycube est* équilibré *pour la coloration χ si $\chi(Q_P) = 0$.*

Définition 10.3 *Soit E une famille de polycubes. L'ensemble des E-colorations forme un K-espace vectoriel C_E que l'on appellera* espace des E-colorations.

Lemme 10.4 *Soit E une famille de polycubes, alors C_E est isomorphe à*

$$(K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K})^*.$$

(On note F^* le dual de F).

preuve
Il existe un isomorphisme naturel entre les formes linéaires de

$$K[X_1, ..., X_d, Y_1, ..., Y_d]/\langle X_1Y_1 - 1, ..., X_dY_d - 1\rangle_K$$

s'annulant sur $\langle Q_P; P \in E\rangle_K$ et les formes linéaires de $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$.
□

Théorème 10.5 *Un polycube P est K-pavable par E si et seulement si $\forall \chi \in C_E$, on a $\chi(Q_P) = 0$.*

preuve Il est clair que la condition « $\forall\chi \in C_E$, on a $\chi(Q_P) = 0$ » est une condition nécessaire pour que P soit K-pavable (car Q_P est une combinaison linéaire des $Q_{P'}$, $P' \in E$). Supposons que P ne soit pas K-pavable, donc $Q_P \notin I_{E,K}$, ce que l'on peut encore écrire $Q_P \neq 0$ dans $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$. Soit B une base de $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$ dont Q_P est un des éléments (elle existe par le théorème de la base incomplète) alors on définit une forme K-linéaire λ de $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$ par $\lambda(Q_P) = 1$, pour tout $Q \in B$, $Q \neq Q_P$, $\lambda(Q) = 0$. Par isomorphisme, il existe donc $\chi \in C_E$ tel que $\chi(Q_P) \neq 0$. □

On note de manière classique $V(I)$ la variété algébrique associée à l'idéal I .

Lemme 10.6 *Soit K un corps algébriquement clos. Le cube unité fondamental $(0, \ldots, 0)$ est K-pavable par une famille E de polycubes si et seulement si $V(I_{E,K}) = \emptyset$.*

preuve D'après la version faible du théorème des zéros de Hilbert, on a $V(I_{E,K}) = \emptyset \Leftrightarrow 1 \in I_{E,K}$. □

Lemme 10.7 *Soit K un corps algébriquement clos, soit E une famille de polycubes. Supposons que $V(I_{E,K}) = \emptyset$. Prenons $x = (x_1, ..., x_{2d}) \in V(I_{E,K})$, alors la forme linéaire χ_x de $K[X_1, ..., X_d, Y_1, ..., Y_d]/\langle X_1Y_1 - 1, ..., X_dY_d - 1\rangle_K$ définie par $\forall\alpha \in \mathbb{Z}^d$, $\chi_x(X^\alpha) = x^\alpha$ (on rappelle que X^a est le monôme $X_1^{\frac{a_1+|a_1|}{2}} ... X_d^{\frac{a_d+|a_d|}{2}} Y_1^{\frac{|a_1|-a_1}{2}} ... Y_d^{\frac{|a_d|-a_d}{2}}$ et $x^\alpha = x_1^{\alpha_1} ... x_d^{\alpha_d}$) est une E-coloration.*

preuve Pour tout $P \in E$, $\chi_x(Q_P) = 0$, car $x = (x_1, ..., x_{2d})$ annule tous les Q_P. $\square$

Corollaire 10.8 *Soit K un corps algébriquement clos. Le cube unité fondamental* $(0, \ldots, 0)$ *est K-pavable par E une famille de polycubes si et seulement si* $\dim(C_E) = 0$.

preuve

Si $(0, ..., 0)$ est K-pavable, toute E-coloration χ vérifie $\chi(1) = 0$, donc la coloration χ est la E-coloration nulle. Réciproquement, d'après le lemme 10.6, si $(0, ..., 0)$ n'est pas K-pavable par E alors $V(I_{E,K}) \neq \emptyset$, et donc par le lemme 10.7, $\dim(C_E) > 0$. $\square$

Théorème 10.9 *Soient K un corps algébriquement clos et E une famille de polycubes, on suppose que $|V(I_{E,K})| = v$ est fini, alors les conditions suivantes sont équivalentes :*
i) $I_{E,K}$ est un idéal radical.
ii) Pour tout $x \in V(I_{E,K})$, les colorations χ_x forment une base de C_E.

preuve Supposons que l'idéal $I_{E,K}$ est radical.
Soit f l'application linéaire de $K[X_1, ..., X_d, Y_1, ..., Y_d]$ dans K^v :

$$f(Q) = \left(Q\left(x^1\right), ..., Q\left(x^v\right)\right)$$

où les x^i sont les éléments de la variété. Par le théorème des zéros de Hilbert, on a que $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$ est isomorphe à K^v. Donc $\dim(C_E) = v$ car C_E est isomorphe à $(K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K})^*$ qui est lui-même isomorphe à $K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}$ dont la dimension est v puisque isomorphe à K^v. Or les v colorations χ_x sont libres, donc elles forment une base de l'espace des colorations. Maintenant supposons que les colorations χ_x forment une base de C_E, alors on a

$$v = \dim(K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K}) \geq \dim\left(K[X_1, ..., X_d, Y_1, ..., Y_d]\Big/\sqrt{I_{E,K}}\right) = v.$$

donc $\dim(K[X_1, ..., X_d, Y_1, ..., Y_d]/I_{E,K})$ est égale à

$$\dim\left(K[X_1, ..., X_d, Y_1, ..., Y_d]\Big/\sqrt{I_{E,K}}\right)$$

et donc $I_{E,K} = \sqrt{I_{E,K}}$. $\square$

11 Racines multiples et colorations différentielles.

La théorie de la géométrie algébrique permet d'étendre la définition de racine multiple d'un polynôme à une variable au champ des polynômes à plusieurs variables. Soit Δ le K-espace vectoriel engendré par les vecteurs de base

$\left(\frac{\partial}{\partial X_1}\right)^{a_1} ... \left(\frac{\partial}{\partial X_n}\right)^{a_n}$ pour tous $a_1, ..., a_n$ appartenant à $\mathbb{N}$. C'est un sous-espace vectoriel des formes linéaires de $K[X_1, ..., X_n]$. Un élément de cet espace est appelé un *opérateur différentiel.* Soit $D \in \Delta$ alors le degré de D est le degré du polynôme associé à D (il est clair que l'on peut associer bijectivement à tout élément $\left(\frac{\partial}{\partial X_1}\right)^{a_1} ... \left(\frac{\partial}{\partial X_n}\right)^{a_n}$ de la base le monôme $X_1^{a_1}...X_n^{a_n}$). Soit I un idéal, si $x \in V(I)$, on définit *l'espace de multiplicité en* x,M_x, par : $M_x = \{D \in \Delta,\ Q \in I \Rightarrow DQ\,|_x = 0\}$. C'est un sous-espace non nul de Δ. La *multiplicité* d'un élément $x \in V(I)$ est par définition la dimension de M_x. Soit E une famille de polycubes. Pour tout $x \in V(I_{E,K})$ et pour tout $D \in M_x \backslash \{0\}$, on appelle *coloration différentielle* $\chi_D :\ P \mapsto DP\,|_x$. On vérifie sans peine que χ_D est bien une E-coloration.

Théorème 11.1 *Soient K un corps algébriquement clos et E une famille de polycubes. On suppose que $|V(I_{E,K})| = v$ est fini, alors* $\dim(C_E) = \sum_{x \in V(I_{E,K})} \dim(M_x)$. *De plus, si* $\left\{D_x^1, ..., D_x^{\dim(M_x)}\right\}$ *est une base de* M_x, *alors* $\bigcup_{x \in V(I_{E,K})} \bigcup_{i=1}^{\dim(M_x)} \left\{\chi_{D_x^i}\right\}$ *constitue une base de l'espace des E-colorations.*

preuve C'est la transcription d'un résultat classique de géométrie algébrique. □

12 Propriétés des bases de Grobner de $I_{E,K}$.

Nous allons montrer que l'on peut déterminer les bases de Grobner et la variété associées à l'idéal $I_{E,K}$ par des calculs sur $K[X_1, ..., X_d]$.

Propriété 12.1 *Soit $E = \{P_1, ..., P_s\}$ une famille de polycubes et soit $\{Q_1, ..., Q_h\}$ une base de Grobner (resp. une $\mathbb{Z}$-base) de $I_{E,K}$ pour l'ordre lexicographique $Y_1 > ... > Y_d > X_1 > ... > X_d$. Posons $B = \{Q_1, ..., Q_h\} \cap \mathbb{Z}[X_1, ..., X_d]$ alors, si un polycube P appartient au cadrant $\mathbb{R}_+^d$, $Q_P \in I_{E,K} \Leftrightarrow \overline{Q_P}^B = 0$ (pour la division dans $K[X_1, ..., X_d]$, (resp. dans $\mathbb{Z}[X_1, ..., X_d]$).*

preuve Immédiat, car dans la division n'apparaît aucun terme comportant des Y_i. □

Propriété 12.2 *En gardant les notations de la propriété 12.1, soient K un corps algébriquement clos et $E = \{P_1, ..., P_s\}$ une famille de polycubes, $(x_1, ..., x_d, y_1, ..., y_d) \in V(I_{E,K})$ si et seulement si $(x_1, ..., x_d) \in V(\langle B \rangle_K)$, $\prod_{i=1}^{d} x_i \neq 0$ et pour tout $1 \leq i \leq d$, on a $x_i = \frac{1}{y_i}$.*

preuve $\langle B\rangle_K$ est le d^{ieme} idéal d'élimination de $\langle Q_{P_1},...,Q_{P_k},X_1Y_1-1,...,X_dY_d-1\rangle_K$ pour l'ordre $Y_1>...>Y_d>X_1>...>X_d$. Donc les éléments de

$$V\left(\langle Q_{P_1},...,Q_{P_k},X_1Y_1-1,...,X_dY_d-1\rangle_K\right)$$

sont obtenus par extension des éléments de $V\left(\langle B\rangle_K\right)$. Les extensions ne sont réalisables que si $\prod_{i=1}^{d} x_i \neq 0$ et dans ce cas, on a pour tout $1\leq i\leq d$, $x_i=\frac{1}{y_i}$.
$\square$

13 Colorations générales.

Définition 13.1 *Soient E une famille de polycubes et*

$$B=\{Q_1,...,Q_h,X_1Y_1-1,...,X_dY_d-1\}$$

*une base de Grobner de $I_{E,\mathbb{C}}$ (resp. une $\mathbb{Z}$-base de $I_{E,\mathbb{Z}}$) . On appelle $\mathbb{C}$-*coloration générale $\chi_{E,\mathbb{C}}$ *(resp. $\mathbb{Z}$-*coloration générale $\chi_{E,\mathbb{Z}}$*) l'application de $\mathbb{C}[X_1,...,X_d,Y_1,...,Y_d]$ dans $\mathbb{C}[X_1,...,X_d,Y_1,...,Y_d]/I_{E,\mathbb{C}}$ (resp. de $\mathbb{Z}[X_1,...,X_d,Y_1,...,Y_d]$ dans $\mathbb{Z}[X_1,...,X_d,Y_1,...,Y_d]/I_{E,\mathbb{Z}}$) qui à Q associe $\bar{Q}^B$.*

Théorème 13.2 *Un polycube P est $\mathbb{C}$-pavable (resp. $\mathbb{Z}$-pavable) par une famille de polycubes $E=\{P_1,...,P_s\}$ si et seulement si $\chi_{E,\mathbb{C}}(P)=0$ (resp. $\chi_{E,\mathbb{Z}}(P)=0$).*

preuve Immédiat. $\square$

Remarque 13.3 *Si la dimension de $\mathbb{C}[X_1,...,X_d,Y_1,...,Y_d]/I_{E,\mathbb{C}}$ est finie, alors l'espace vectoriel $\mathbb{C}[X_1,...,X_d,Y_1,...,Y_d]/I_{E,\mathbb{C}}$ est isomorphe à $\bigoplus_{x\in V(I_{E,\mathbb{C}})} M_x$. De plus si l'on note, pour $1\leq i\leq \dim(C_E)$, π_i la projection sur la i^{eme} coordonnée, alors pour $1\leq i\leq \dim(C_E)$ les formes linéaires $\pi i\circ\chi_{E,\mathbb{C}}$ sont des E-colorations qui forment une base de C_E. En particulier, si la dimension de $\mathbb{C}[X_1,...,X_d,Y_1,...,Y_d]/I_{E,\mathbb{C}}$ est finie et égale au cardinal de $V(I_{E,\mathbb{C}})$ on sait que $I_{E,\mathbb{C}}$ est un idéal radical. Dans ce cas P est $\mathbb{C}$-pavable si et seulement si Q_P s'annule sur la variété $V(I_{E,\mathbb{C}})$.*

14 Applications au pavage des polycubes par des briques.

Notation 14.1 *Soient $1\leq i\leq d$ et $y\in\mathbb{C}$, on note H_y^i l'hyperplan affine*

$$\left\{x\in\mathbb{C}^d; x_i=y\right\}.$$

Lemme 14.2 *Soit* $E = \{1 \times ... \times 1 \times a_j \times 1 \times ... \times 1\}$ *où* a_j *est à la* j^{eme} *position (en d'autres termes* E *n'est constituée que d'une barre). La variété* $V(I_{E,\mathbb{C}})$ *qui lui est associée est*

$$\left\{ (x_1, ..., x_d, y_1, ..., y_d) ; (x_1, ..., x_d) \in \bigcup_{k=1}^{a_j - 1} H^j_{e^{\frac{2i\pi k}{a_j}}} \text{ et } y_k = \frac{1}{x_k} \text{ pour } 1 \leq k \leq d \right\}.$$

preuve On a $Q_{1\times...\times a_j\times...\times 1} = \frac{X_j^{a_j}-1}{X_j-1}$; or $\frac{x_j^{a_j}-1}{x_j-1} = 0$ si et seulement si $(x_1, ..., x_d) \in \bigcup_{k=1}^{a_j-1} H^j_{e^{\frac{2i\pi k}{a_j}}}$ donc $V\left(\left\langle \frac{X_j^{a_j}-1}{X_j-1} \right\rangle_{\mathbb{C}}\right) = \bigcup_{k=1}^{a_j-1} H^j_{e^{\frac{2i\pi k}{a_j}}}$, le lemme découle alors de la propriété 12.2. □

Lemme 14.3 *Soit* V_i *la variété associée à la barre* $1 \times ... \times 1 \times a_i \times 1 \times ... \times 1$ *alors la variété* V *associée à la brique* $a_1 \times ... \times a_d$ *vérifie* $V = \bigcup_{i=1}^{d} V_i$. *Donc* P *est* $\mathbb{C}$*-pavable par* $p_1 \times ... \times p_n$ *si et seulement si* P *est* $\mathbb{C}$*-pavable par* $p_1 \times 1 \times ... \times 1$ *et* $\mathbb{C}$*-pavable par* $1 \times p_2 \times ... \times 1$ *et* ... *et* $\mathbb{C}$*-pavable par* $1 \times ... \times 1 \times p_n$.

preuve En effet $Q_{a_1\times...\times a_j\times...\times a_d} = \prod_{i=1}^{d} \frac{X_i^{a_i}-1}{X_i-1}$, donc $\prod_{i=1}^{d} \frac{x_i^{a_i}-1}{x_i-1} = 0$ si et seulement s'il existe j tel que $\frac{x_j^{a_j}-1}{x_j-1} = 0$. Ce qui implique $V = \bigcup_{i=1}^{d} V_i$. □

Lemme 14.4 *Soit* $E = \{P_1, ..., P_k\}$ *une famille de paveurs et soit, pour* $1 \leq i \leq k$, V_i *la variété associée au paveur* P_i, *alors la variété* V *associée à* E *vérifie* $V = \bigcap_{i=1}^{k} V_i$.

preuve Cela découle immédiatement de la propriété suivante: $V(\langle Q_1, ..., Q_s \rangle_{\mathbb{C}}) = \bigcap_{i=1}^{s} V(\langle Q_i \rangle_{\mathbb{C}})$. □

Corollaire 14.5 *Soit* $E = \{P_1, ..., P_k\}$ *une famille de briques. Si*

$$(x_1, ..., x_d, y_1, ..., y_d) \in V(I_{E,\mathbb{C}})$$

alors $(x_1, ..., x_d)$ *appartient à une combinaison finie d'unions et d'intersections d'hyperplans de* $\mathbb{C}^n$ *et* $y_i = \frac{1}{x_i}$, *pour* $1 \leq i \leq d$.

preuve Immédiat. □

Les lemmes 14.2, 14.3, 14.4 permettent de déterminer rapidement la variété associée à une famille finie de briques. En utilisant le lemme suivant :

Lemme 14.6 *Soit* $E = \{P_1, ..., P_k\}$ *une famille de briques alors* $I_{E,\mathbb{C}}$ *est un idéal radical.*

On obtient alors :

Théorème 14.7 *Un polycube* P *est* $\mathbb{C}$*-pavable par* E *si et seulement si* Q_P *s'annule sur la variété .*

Le théorème suivant permet de trouver un critère de $\mathbb{Z}$-pavabilité par des briques :

Théorème 14.8 *(Barnes [1]) Soit* $E = \{P_1, ..., P_k\}$ *une famille de briques.* P *est* $\mathbb{C}$*-pavable par* E *si et seulement si* P *est* $\mathbb{Z}$*-pavable par* E.

Exemple 14.9 *On cherche un critère de* $\mathbb{Z}$*-pavage des polyominos par* $2 \times 3, 3 \times 4$*, on détermine* $V(I_{E,\mathbb{C}})$ *en utilisant les lemmes 14.2, 14.3, 14.4. On trouve que*

$$(x_1, x_2, y_1, y_2) \in V\left(I_{E,\mathbb{C}}\right)$$

si et seulement si $(x_1, x_2) \in (\{-1\} \times \{-1, i, -i\}) \bigcup \left(\{j, j^2\}^2\right)$, $y_1 = \frac{1}{x_1}$ *et* $y_2 = \frac{1}{x_2}$. *Donc un polyomino* P *est* $\mathbb{Z}$*-pavable si et seulement si* Q_P *s'annule pour les 7 valeurs de* $V(I_{E,\mathbb{C}})$.

Pavages	Ideaux	Bases de Grobner	Variétés
P est $\mathbb{C}$-pavable par F	$Q(P) \in I_F$	$Q(P)$ est divisible par une base de Grobner de I_F	Si I_F est radical $Q(P)$ s'annule sur V_F
P est $\mathbb{C}$-pavable par F_1 et $\mathbb{C}$-pavable par F_2	$Q(P) \in I_{F_1} \cap I_{F_2}$		Si I_F est radical $Q(P)$ s'annule sur $V_{F_1} \cup V_{F_2}$
P est $\mathbb{C}$-pavable par $F_1 \cup F_2$	$Q(P) \in I_{F_1} + I_{F_2}$		Si I_F est radical $Q(P)$ s'annule sur $V_{F_1} \cap V_{F_2}$

15 Tableau

We give in the sequel a tabular where we have computed the standard basis for the "small" polyominoes, and for the three-in-line pohexes. Respectively, we mention on each line : the dominoes, the three-in-line trominoes, the L-trominoes, the T-tetrominoes, the L-tetrominoes, S-tetrominoes and the tribones.

(*) We use the order on the monomial induces by $y_1 > y_2 > x_1 > x_2$. We only write the polynomials of the basis which belong to $\mathbb{Z}[x_1, x_2]$.

16 $\mathbb{Z}$-tilability and boundary conditions

In the paper of Conway and Lagarias, it is possible to know if a polymino P has a $\mathbb{Z}$-tiling by only having informations on the boundary of P. In this section, we prove that we have the same fact. We do not need to compute

P-polynomials	(*) Standard Basis	General Coloration and condition of $\mathbb{Z}$-tilability
x_1+1, x_2+1	x_1+, x_2+1	black and white balanced
$x_1^2+x_1+1$, $x_2^2+x_2+1$	$x_1^2+x_1+1$, $x_2^2+x_2+1$	(j,j),(j,j^2) (j^2,j),(j^2,j^2)
x_1+x_2+1, $x_1x_2+x_1+1$, $x_1x_2+x_2+1$, $x_1x_2+x_1+x_2$	x_1-1, x_2-1, 3	the number of squares is a multiple of 3
$x_1^2+x_1x_2+x_1+1$, $x_1^2x_2+x_1x_2+x_1+x_2$, $x_1x_2+x_2^2+x_2+1$, $x_1x_2^2+x_1x_2+x_1+x_2$	x_1+3, x_2+3, 8	when assigning 5 on the white squares and 1 on the black squares, the sum of values on the squares of the polyomino is a multiple of 8
$x_1^2+x_1+x_2+1$, $x_1x_2^2+x_1x_2+x_1+1$, $x_1x_2^2+x_1x_2+x_1+x_2^2x_1x_2^2+x_2^2+x_2+1$, $x_1+x_2^2+x_2+1$, $x_1^2x_2+x_1x_2+x_2+1$, $x_1^2x_2+x_1^2+x_1x_2+x_2$, $x_1^2x_2+x_1^2+x_1+1$	x_2^2-1, $4x_2-4$, x_1+x_2+2	no simple criterion
$x_1x_2^2+x_1x_2+x_2+1$, $x_1^2+x_1x_2+x_1+x_2$, $x_1^2x_2+x_1x_2+x_1+1$, $x_1x_2+x_1+x_2^2+x_2$	$x_1^2-x_2^2$, $x_1x_2+x_1+x_2^2+x_2 2x_2^2-2$, $x_2^3-x_2^2-x_2+1$	no simple criterion
$x_1^2+x_1+1$, $x_2^2+x_2+1$, $x_1^2+x_1x_2+x_2^2$	$3x_1+3x_2+3$, $x_2^2+x_2+1$, $x_1^2-2x_1-3x_2-2$, $x_1x_2+2x_1+2x_2+1$	no simple criterion

the remainder of Q_P, but only the remainder of a polynomial associated to the boundary of P.

17 Remplissage équitable et couleur sur le bord.

Soit $G\left(V,E\right)$ graphe simple d-régulier et $f: V \to \{1,...n\}$ une coloration des sommets en n couleurs, on note $\tilde{G}$ le digraphe symétrique orienté $\tilde{G}\left(V,\tilde{E}\right)$ avec $(x,y) \in \tilde{E}$ et $(y,x) \in \tilde{E}$ si $\{x,y\} \in E$. Soit H un sous-graphe induit de G, un sommet x de H est dit *sur le bord* de H si le degré de x dans H est strictement inférieur à d. H est dit *équitablement rempli* si quels que soient $1 \le i \le n$ et $1 \le j \le n$, on a :

$$\left|f^{-1}(i) \cap V\left(H\right)\right| = \left|f^{-1}(j) \cap V\left(H\right)\right|.$$

L'ensemble A_s des *arcs sortants de* H est l'ensemble des arcs $(x,y) \in E(\tilde{G})$ tels que $x \in H$ et $y \in G \backslash H$. On note, pour $1 \le i \le n$, ε_i le i-ème vecteur de la base canonique de $\mathbb{R}^n$. On définit le *vecteur couleur* de x de la manière suivante :

$$v\left(x\right) = \sum_{(x,y)\ arc\ sortant\ de\ x} (\varepsilon_{f(x)} - \varepsilon_{f(y)}).$$

Proposition 17.1 *Soit H un sous-graphe induit de G. Si les deux propositions suivantes sont vérifiées :*
i) pour tout $1 \le i \le n$ tous les sommets de G de couleur i ont le même vecteur couleur v_i.
ii) $\sum\limits_{i=1}^{n} v_i = \vec{0}$ et $\langle v_1, ...v_n\rangle$ de codimension 1.
Alors H est équitablement rempli si et seulement si $\sum\limits_{(x,y)\in A_s} \left(\varepsilon_{f(x)} - \varepsilon_{f(y)}\right) = 0$.

preuve On a $\sum\limits_{(x,y)\in A_s} \left(\varepsilon_{f(x)} - \varepsilon_{f(y)}\right) = \sum\limits_{x\in H} v(x)$ car si x et y appartiennent à H, les contributions des arcs (x,y) et (y,x) s'annulent. De plus, on a

$$\sum_{x\in H} v(x) = \sum_{1\le i\le n} \left(\left|f^{-1}(i) \cap H\right|.v_i\right)$$

car $v(x) = v_i$ si x est de couleur i. On en déduit que

$$\sum_{1\le i\le n} \left(\left|f^{-1}(i) \cap H\right|.v_i\right) = \sum_{(x,y)\in A_s} \left(\varepsilon_{f(x)} - \varepsilon_{f(y)}\right). \tag{2}$$

Maintenant, H est équitablement rempli si et seulement si pour, $1 \le i \le n$ et $1 \le j \le n$, on a $\left|f^{-1}(i) \cap H\right| = \left|f^{-1}(j) \cap H\right| = k$ donc par ii) si et seulement si $\sum\limits_{1\leq i\leq n}\left(\left|f^{-1}(i)\cap H\right|.v_i\right)=k\sum\limits_{1\leq i\leq n}v_i=0$. En utilisant (2), H est équitablement rempli si et seulement si $\sum\limits_{(x,y)\in A_s}\left(\varepsilon_{f(x)}-\varepsilon_{f(y)}\right)=0$. $\square$

18 Applications à la caractérisation des polycubes $\mathbb{C}$-pavables ($\mathbb{Z}$-pavables) par une famille de polycubes.

Théorème 18.1 *Soient P un polycube et x appartenant à la variété associée aux paveurs $P_1,\ldots,P_k$. On suppose que la $(P_1,\ldots,P_k)$-coloration χ_x vérifie*

$$\chi_x\left(\sum_{i=1}^{d}(X_i+Y_i)\right)\neq 2d.$$

Alors $\chi_x(Q_P)=0$ si et seulement si $\sum\limits_{(c_1,c_2)\in S}\left(\chi_x(Q_{c_1})-\chi_x(Q_{c_2})\right)=0$ où (c_1,c_2) appartient à S si c_1 est un cube de P et c_2 un cube ayant une face en commun avec b_1 et n'appartenant pas à P.

preuve Soient χ une coloration et X^a un monôme, on note

$$v_\chi(X^a)=\sum_{i=1}^{d}\left(\chi(X^a)-\chi(X^aX_i)\right)+\sum_{i=1}^{d}\left(\chi(X^a)-\chi(X^aY_i)\right).$$

On a $\sum\limits_{(c_1,c_2)\in S}\left(\chi_x(Q_{c_1})-\chi_x(Q_{c_2})\right)=\sum\limits_{c\in P}v_{\chi_x}(Q_c)$ car si c et c' appartiennent à P, les contributions des arcs (c,c') et (c',c) s'annulent. De plus, on a $\sum\limits_{c\in P}v_{\chi_x}(Q_c)=\sum\limits_{c\in P}\sum\limits_{(c,c')\in S}\left(\chi_x(Q_c)-\chi_x(Q_{c'})\right)=\left(2d-\chi_x\left(\sum\limits_{i=1}^{d}(X_i+Y_i)\right)\right)\chi_x(Q_P)$.
Comme

$$\chi_x\left(\sum_{i=1}^{d}(X_i+Y_i)\right)\neq 2d,$$

$\chi(Q_P)=0$ si et seulement si $\sum\limits_{(c_1,c_2)\in S}\left(\chi(Q_{c_1})-\chi(Q_{c_2})\right)=0$. $\square$

Corollaire 18.2 *Un polycube P est $\mathbb{Z}$-pavable par une famille E de briques si et seulement s'il est équitablement rempli pour les colorations associées à la variété déterminée par la famille E.*

preuve En effet, l'idéal associé à une famille de briques est un idéal radical. Donc un polycube P est $\mathbb{C}$-pavable par une famille E de briques si et seulement s'il est équitablement rempli pour les colorations associées à la variété déterminée par la famille E. De plus, par le théorème de Barnes [1], nous savons que P est $\mathbb{C}$-pavable par une famille E de briques si et seulement P est $\mathbb{Z}$-pavable par une famille E de briques. Le théorème s'ensuit. $\square$

Théorème 18.3 *Soient P un polycube et $\chi_{E,\mathbb{Z}}$ la $\mathbb{Z}$-coloration générale (resp. $\chi_{E,\mathbb{C}}$ la $\mathbb{C}$-coloration générale) associée aux paveurs $P_1, \ldots, P_k$. On suppose que*

$$\chi_{E,\mathbb{Z}}\left(\sum_{i=1}^{d}(X_i + Y_i)\right) - 2d$$

(resp. $\chi_{E,\mathbb{C}}\left(\sum_{i=1}^{d}(X_i + Y_i)\right) - 2d$) n'est pas un diviseur de zéro. Dans ce cas, $\chi_{E,\mathbb{Z}}(Q_P) = 0$ si et seulement si $\sum_{(c_1,c_2)\in S}(\chi_{E,\mathbb{Z}}(Q_{c_1}) - \chi_{E,\mathbb{Z}}(Q_{c_2})) = 0$ où (c_1, c_2) appartient à S si c_1 est un cube de P et c_2 un cube ayant une face en commun avec c_1 et n'appartenant pas à P.

preuve Nous faisons la preuve pour les $\mathbb{Z}$-colorations générales. L'autre cas se traite de façon identique. Soit $\chi_{E,\mathbb{Z}}$ la $\mathbb{Z}$-coloration générale, on note

$$v_{\chi_{E,\mathbb{Z}}}(X^a) = \sum_{i=1}^{d}(\chi_{E,\mathbb{Z}}(X^a) - \chi_{E,\mathbb{Z}}(X^a X_i)) + \sum_{i=1}^{d}(\chi_{E,\mathbb{Z}}(X^a) - \chi_{E,\mathbb{Z}}(X^a Y_i)).$$

On a $\sum_{(c_1,c_2)\in S}(\chi_{E,\mathbb{Z}}(Q_{c_1}) - \chi_{E,\mathbb{Z}}(Q_{c_2})) = \sum_{c\in P} v_{\chi_{E,\mathbb{Z}}}(Q_c)$ car, si des cubes c et c' appartiennent à P, les contributions des couples (c, c') et (c', c) s'annulent. De plus, on a $\sum_{c\in P} v_{\chi_{E,\mathbb{Z}}}(Q_c) = \sum_{c\in P}\sum_{(c,c')\in S}(\chi_{E,\mathbb{Z}}(Q_c) - \chi_{E,\mathbb{Z}}(Q_{c'})) = \left(2d - \chi_{E,\mathbb{Z}}\left(\sum_{i=1}^{d}(X_i + Y_i)\right)\right)\chi_{E,\mathbb{Z}}(Q_P)$. Comme $\chi_{E,\mathbb{Z}}\left(\sum_{i=1}^{d}(X_i + Y_i)\right) - 2d$ n'est pas un diviseur de zéro, $\chi_{E,\mathbb{Z}}(Q_P) = 0$ si et seulement si $\sum_{(c_1,c_2)\in S}(\chi_{E,\mathbb{Z}}(Q_{c_1}) - \chi_{E,\mathbb{Z}}(Q_{c_2})) = 0$. $\square$

References

[1] F.W. Barnes, Algebraic theory of brick packing 2, Discrete Mathematics 42 (1982) 129-144.

[2] L. Bougé, M. Cosnard, Recouvrement d'une pièce trapézoïdale par des dominos, *C. R. Acad. Paris*, t. 315, Série I, p. 221-226, 1992.

[3] B. Buchberger, Introduction to Grobner basis, Logic of computation (Marktoberdorf 95) 35-66, NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci.,157, Springer Berlin (1997).

[4] J.H Conway, J.C. Lagarias, Tiling with polyominoes and combinatorial group theory, J.C.T. Series A 53 (1990) 183-208.

[5] D. Cox, J. Little, D. O'Shea, Ideals,varieties and algorithms, 2nde edition, Undergraduate Text in Mathematics, Springer Verlag, New York (1997) XV 536 pp.

[6] P. Duchet, C. Payan, Modélisation combinatoire et Méthodologie de le recherche, cours de 3ème cycle, Université Grenoble 1, 1997.

[7] S. W. Golomb, Tiling with polyominoes, J.C.T. Series A 1 (1966) 280-296.

[8] S. W. Golomb, Polyominoes which tile rectangles, J.C.T. Series A 51 (1989) 117-124.

[9] D.A. Klarner, Packing a rectangle with congruent n-ominoes, J.C.T. Series A 7 (1969) 107-115.

[10] J.C. Lagarias, D.S. Romano, A polyomino tiling problem of Thruston and its configurational entropy, J.C.T. Series A 63 (1993) 338-358.