Table des matières

Introduction

Le but de cette présente étude est la mise en relief de la particularité de la base de Gröbner des idéaux toriques. Cette base est très intéressante pour les idéaux polynômiaux grâce à ses propriétés particulières. Pour cela, on peut signaler entre autres que la base de Gröbner d'un idéal I engendre cet idéal et de plus, elle a un reste unique dans l'algorithme de division dans un anneau de polynôme $\mathbb{K}[X_1, \ldots, X_n]$ sans tenir compte l'ordre qu'on procède à ladite division. Outre, elle donne une esquisse simple de l'existence des solutions d'un système d'équation polynomiale en utilisant le Nullstellensatz de Hilbert. Quant à l'importance de la base de Gröbner des idéaux toriques, les principales contributions de cette étude se concentrent sur le fait qu'elle contient les minimaux successifs de Minkowski, et qu'on peut déterminer la borne de son degré en choisissant un ordre polynomial.

Pour cela, notre travail se divise en quatre parties. La première partie contient des rappels sur les relations d'ordre et les propriétés des A - modules. La deuxième partie sera réservée à la construction de la variété torique par le biais d'un cône σ. C'est dans cette partie que nous donnerons les notions de la variété affine et la corrélation entre les idéaux et ces variétés. Ensuite, la troisième partie s'intéresse sur la base de Gröbner et son application notamment sur les idéaux et sur les systèmes d'équation polynomiale. Finalement, nous verrons dans la dernière partie les spécificités de la base de Gröbner des idéaux toriques.

Chapitre 1

Ordre et module

1.1 Ordre

Soient E et F deux ensembles.

Définition 1.1.1.

Une *relation binaire* définie sur E est une propriété définie par

$$x\mathcal{R}y \Rightarrow (x, y) \in E \times E.$$

Définition 1.1.2.

Une relation binaire $\leqslant$ définie sur E est dite un *préordre* si elle est :

- reflexive : $x \leqslant x, \forall x \in E$
- transitive : $(x \leqslant y \text{ et } y \leqslant z) \Rightarrow x \leqslant z$

Une *relation d'ordre* ou ordre partiel est un *préordre antisymétrique*, c'est-à-dire si on a de plus

$$(x \leqslant y \text{ et } y \leqslant x) \Rightarrow x = y$$

Exemple 1.1.3.

- La relation de la divisibilité "|" est un ordre partiel sur $\mathbb{N}^*$. Dans ce cas $(E, |)$ est dit *partiellement ordonné*.

– La relation $<$ définie par $\forall (x,y) \in \mathbb{Z}^2,\ x < y \Leftrightarrow y - x \in \mathbb{N}^*$ n'est pas une relation d'ordre, car la relation n'est pas reflexive.

Dans toute la suite, $\leqslant$ désignera un ordre partiel.

Notations.

Soit $A \subseteq E$, pour tout $x \in E$, on note :

$$U(x, \leqslant) := \{y \in E/\ x \leqslant y\} \tag{1.1}$$

$$D(x, \leqslant) := \{y \in E/\ y \leqslant x\} \tag{1.2}$$

$$U_A(x, \leqslant) := \{y \in A/ x \leqslant y\} \tag{1.3}$$

$$D_A(x, \leqslant) := \{y \in A/\ y \leqslant x\} \tag{1.4}$$

On les notera respectivement $U(x)$ et $D(x)$ s'il n'y aura pas d'ambiguité.

Définition 1.1.4.

$(E, \leqslant)$ est dit un ensemble totalement ordonné si pour tout $x \in E$, pour tout $y \in E$;

$$y \in U(x) \text{ ou } y \in D(x) \tag{1.5}$$

Une telle relation est dite *ordre total* sur E.

Exemple 1.1.5.

$(\mathbb{R}, \leqslant)$ est totalement ordonné.

Définitions 1.1.6.

On dit que deux éléments x, y de E sont $\leqslant$-*comparables* ou tout simplement comparables s'ils vérifient (1.5). Ils sont $\leqslant$-incomparables (ou incomparables) s'ils ne sont pas comparables.

Soit $A \subseteq E$. A est dit *chaîne* (resp. *antichaîne*) si tout $x, y \in A, x, y$ sont $\leqslant$-comparables (resp. $\leqslant$-incomparables).

Définitions 1.1.7.

Un ordre partiel $\leqslant$ est dit *fondé* si l'ensemble

$$\mathrm{Min}_{\leqslant}(A) := \{x \in A/\ D_A(x; \leqslant)\backslash\{x\} = \varnothing\} \neq \varnothing \tag{1.6}$$

pour tout sous ensemble non vide de E ; Autrement dit, $\leqslant$ est fondé si tout sous ensemble non vide de E admet au moins un élément minimal. Cette relation d'ordre est dite :

- *non fondée*, si elle n'est pas fondée
- *étroite* si $\mathrm{Min}_{\leqslant}(A)$ est fini pour tout $A \subseteq E$, avec $A \neq \varnothing$
- *bel ordre* si $\leqslant$ est à la fois étroit et fondé
- *bon ordre* si $\leqslant$ est à la fois total et fondé. Dans ce cas, $(E, \leqslant)$ est dit *bien ordonné*.
- *linéaire* si $(E, \leqslant)$ est une chaîne.

Théorème 1.1.8.

$\leqslant$ est fondé sur E si et seulement si toute suite strictement décroissante $(x_i)_{i\in\mathbb{N}}$ d'elements de E est finie.

Preuve.

$(\Rightarrow)$: Supposons qu'il existe une suite strictement décroissante $(x_i)_{i\in\mathbb{N}}$ d'éléments de E qui n'est pas finie. Posons $X = \{x_i/\ i \in \mathbb{N}\} \subseteq E$. Alors $\mathrm{Min}_{\leqslant}(X) = \varnothing$ et $\leqslant$ est ainsi non fondé sur E.

$(\Leftarrow)$: Supposons qu'il existe $A \subseteq E$ tel que $A \neq \varnothing$ et $\mathrm{Min}_{\leqslant}(A) = \varnothing$. Donc
$\forall x \in A, D_A(x, \leqslant) \neq \varnothing$

Soit $x_0 \in A$, donc il existe $x_1 \in A$ tel que $x_1 \leqslant x_0$, et de la même façon il existe $x_2 \in A$ tel que $x_2 \leqslant x_1 \leqslant x_0$. En continuant cette procédure, on peut avoir une suite strictement décroissante d'éléments de E :

$$x_0 \geqslant x_1 \geqslant x_2 \geqslant ... \geqslant x_n \geqslant ...\text{pour tout } n \in \mathbb{N}$$

□

Lemme 1.1.9.

$\leqslant$ est étroit sur E si et seulement si $(E, \leqslant)$ n'admet pas d'antichaîne infinie.

Preuve.

Supposons que $\leqslant$ est étroit et soit A une antichaîne de $(E, \leqslant)$.
On a $\mathrm{Min}_{\leqslant}(A) = A$ car pour tout $x, y \in A$, x et y sont incomparables d'après la définition 1.1.6. Comme $\leqslant$ est étroit, donc A est fini.

Réciproquement, soit $A \neq \varnothing$ et $A \subseteq E$. $\mathrm{Min}_{\leqslant}(A)$ est une antichaîne de E, d'où $\mathrm{Min}_{\leqslant}A$ est fini et $\leqslant$ est ainsi étroit. □

Définition 1.1.10.

Un ordre partiel $\leqslant'$ de E est dit une *extension de* $\leqslant$ si on a :

$$x \leqslant y \Rightarrow x \leqslant' y, \text{ pour tout } x, y \in E$$

Théorème 1.1.11.

Les assertions suivantes sont équivalentes :

1. *$\leqslant$ est un bel ordre*
2. *Pour toute suite $(x_i)_{i\in\mathbb{N}}$ d'éléments distincts de E, on peut trouver deux indices $i < j$ tel que $x_i \leqslant x_j$.*

Preuve.

$1 \Rightarrow 2$ Soit $(x_i)_{i\in\mathbb{N}}$ une suite d'éléments distincts de E tel que pour tout $i, j \in \mathbb{N}$, x_i et x_j sont incomparables. Ainsi, $X = \{x_i / \ i \in \mathbb{N}\}$ est une antichaîne infinie de E et par suite, $\leqslant$ n'est pas étroit sur E, donc ce n'est pas un bel ordre De plus, s'il existe une suite strictement décroissante d'éléments distincts de E, alors $\leqslant$ n'est pas fondé sur E (cf théorème 1.1.8), donc ce n'est plus un bel ordre.
$2 \Rightarrow 1$ Si $\leqslant$ n'est pas fondé alors il y a une suite infinie $(x_i)_{i\in\mathbb{N}} \subseteq E$ strictement décroissante (cf ; théorème 1.1.8).
Si $\leqslant$ n'est pas étroit, il existe une antichaîne infinie A de $(E, \leqslant)$.

Soit $x : \begin{array}{ccc} \mathbb{N} & \longrightarrow & A \\ n & \longmapsto & x_n \end{array}$ une application injective alors x_n et x_m sont incomparables, pour tout $n \neq m$ □

Lemme 1.1.12.

Soit $\leqslant'$ une extension de $\leqslant$.

Si x et y sont $\leqslant'$-incomparables, alors ils sont $\leqslant$-incomparables.

Preuve.

C'est la contraposée de la définition : $x \leqslant y \Rightarrow x \leqslant' y$. □

Proposition 1.1.13.

Soit $\leqslant'$ une extension de l'ordre partiel $\leqslant$:

1. *si $\leqslant'$ est fondé, alors $\leqslant$ est fondé ;*
2. *si $\leqslant$ est étroit, alors $\leqslant'$ est étroit ;*
3. *si $\leqslant$ est bel ordre, alors $\leqslant'$ l'est aussi.*

Preuve.

1. Supposons que $\leqslant$ n'est pas fondé. Soit $\varnothing \neq A \subseteq E$ tel que $\mathrm{Min}_{\leqslant}(A) = \varnothing$. Donc pour tout $x \in A$, il existe $y \in A$; tel que $y \in D_A(x, \leqslant)$ par suite $y \in D_A(x, \leqslant')$; ainsi $\mathrm{Min}_{\leqslant'}(A) = \varnothing$ et $\leqslant'$ n'est pas fondé.
2. Supposons que $\leqslant$ est étroit. Or x et y sont $\leqslant$ -incomparables s'ils sont $\leqslant'$-incomparables (cf lemme 1.1.12). Donc une antichaîne infinie dans $(E, \leqslant')$ l'est aussi dans $(E, \leqslant)$. Comme $\leqslant$ est étroit, $(E, \leqslant)$ n'admet pas d'antichaîne infinie (cf. lemme 1.1.9). Donc $(E, \leqslant')$ n'admet non plus d'antichaîne infinie. D'où d'après ce même lemme, $\leqslant'$ est étroite.
3. Soit $(x_i)_{i \in \mathbb{N}}$ une suite d'éléments distincts de E. Comme $(E, \leqslant)$ est un bel ordre, il existe i, j tels que $i < j$ et $x_i \leqslant x_j$, (cf théorème 1.1.11) par conséquent $x_i \leqslant' x_j$. Ainsi, $\leqslant'$ est un bel ordre.

□

Lemme 1.1.14.

Soit $A \subseteq E$ une antichaîne de $(E, \leqslant)$. Soit $a \in A$, alors l'ordre partiel $\leqslant$ admet une extension $\leqslant'$ tel que $\{a\} = Min_{\leqslant'} A$.

Preuve.

Sous les hypothèses du lemme, en notant $B = A\backslash\{a\}$ et $\leqslant'$ la relation sur E définie par :

$$U'(x) = \begin{cases} U(x) \cup U(B) & \text{si } a \in U(x) \\ U(x) & \text{sinon} \end{cases}$$

avec $U(B) = \bigcup_{x \in B} U(x)$. La relation $\leqslant'$ est un ordre partiel sur E. De plus, c' est une extension de $\leqslant$ car $U(x) \subseteq U'(x)$ pour tout $x \in E$ (cf [Ram 02]. lemme 1.16).

Et pour la deuxième partie du lemme, soit y un élément quelconque de B. Comme $y \in U(y)$, $y \in U(B)$ et par suite $B \subseteq U(a) \cup U(B)$. De plus $a \in U(a)$, donc $U'(a) = U(a) \cup U(B)$. Ainsi, $y \in U'(a)$ pour tout $y \in A\backslash\{a\}$. Par conséquent, $a \leqslant' y$ pour tout $y \in A\backslash\{a\}$, donc $y \notin \mathrm{Min}_{\leqslant'}(A)$ et on conclut que $\{a\} = \mathrm{Min}_{\leqslant'}(A)$. □

Proposition 1.1.15.

Tout ordre partiel $\leqslant$ admet une extension linéaire.

Preuve.

Notons X l'ensemble de toutes les extensions $\leqslant'$ de l'ordre partiel $\leqslant$. X est non vide (car $\leqslant \in X$). Définissons sur X une relation d'inclusion, pour deux éléments $\leqslant'$ et $\leqslant''$ de X par

$$\leqslant' \subseteq \leqslant'' \Leftrightarrow U(x, \leqslant') \subseteq U(x, \leqslant'') \tag{1.7}$$

Soit une chaîne $\{\leqslant_i\}_{i \in I}$ de $(X, \subseteq)$. Alors pour chaque $x \in E$, la chaîne d'ensembles $(U_E(x, \leqslant_i))_{i \in I}$ admet un majorant $U(x, \leqslant') = \bigcup_{i \in I} U(x_i \leqslant_i)$. Donc $(X, \subseteq)$ est inductif et il admet ainsi un élément maximal $\leqslant_m$ (d'après le lemme de Zorn).

Supposons que $\leqslant_m$ n'est pas linéaire. Soit (a, b) un couple de E tel que a et b sont $\leqslant_m$-incomparables. Donc $\{a, b\}$ est une antichaîne de E et d'après le lemme

1.1.14, il existe une extension $\leqslant'_m$ de $\leqslant_m$ tel que $\{a\} = \text{Min}_{\leqslant'_m}\{a, b\}$

Par suite : $\leqslant'_m \in X$ et alors $U(x, \leqslant_m) \subseteq U(x, \leqslant'_m)$, donc $\leqslant_m \subseteq \leqslant'_m$, qui contredit la maximalité de $\leqslant_m$. D'où $\leqslant_m$ est une extension linéaire de $\leqslant$. □

1.2 Monoïdes et modules

1.2.1 Monoïdes

On appelle *monoïde*, un ensemble muni d'une opération de composition interne associative et d'un élément neutre. Par exemple $(\mathbb{N}, +, 0)$ est un monoïde.

1.2.2 Modules

Soit K un anneau commutatif unitaire. Un *K-modules M* est un monoïde commutatif muni d'une loi d'addition $+$ et d'une loi de multiplication de $K \times M$ à valeurs dans M qui satisfait aux axiomes suivants :
$\alpha.(x + y) = \alpha.x + \alpha.y$
$(\alpha + \beta).x = \alpha.x + \beta.x$
$\alpha.(\beta.x) = (\alpha.\beta).x$
$1.x = x$
Pour tout $x \in M$, il existe x' tel que $x + x' = 0$ (0 est l'élément neutre de M) pour tout $\alpha, \beta \in K$ et $x, y \in M$)

Définition 1.2.1.
Soient E et F deux K modules. Une fonction f est dite *K-linéaires* de E vers F, si

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y), \forall x, y \in E \text{ et } \alpha, \beta \in K.$$

Définition 1.2.2.
Soit M un K-module. On appelle K-sous module de M, toute partie M' tel que :

$$M' \text{ est un sous monoïde de } (M,+)$$
$$x \in M',\ \alpha \in K \text{ impliquent } \alpha x \in M'$$

Si K était un corps, alors on dit que M est un K-sous espace vectoriel.

Définition 1.2.3.

Soient M un K-module et $M_1, ..., M_p$ des K-sous modules de M, on dit qu'ils sont *linéairement indépendants* si l'application

$$\begin{array}{rccl} f: & M_1 \times ... \times M_p & \longrightarrow & M \qquad\qquad \text{est bijective} \\ & (x_1, ..., x_p) & \longmapsto & x_1 + ... + x_p \end{array}$$

On note alors $M = M_1 \oplus M_2 \oplus ... \oplus M_p$ et on dit que M est une *somme directe* de $M_1, ..., M_p$.

Proposition 1.2.4.

Si $M = M_1 \oplus M_2 \oplus ... \oplus M_p$, alors tout $x \in M$ s'écrit de façon unique sous la forme $x = x_1 + ... + x_p$ avec $x_i \in M_i,\ 1 \leqslant i \leqslant p$.

Proposition et définitions 1.2.5.

Notons V_i l'application de M vers $\bigoplus_{i=1}^{p} M_i$ telle que $V_i : x \mapsto x_i$. Alors V_i est linéaire et que $V_i \circ V_i = V_i$,

V_i est appelé la projection sur M_i parallèlement à $\bigoplus_{\substack{j=1 \\ j \neq i}}^{p} M_j$

Un endomorphisme V d'un K-module M est un projecteur si $V \circ V = V$.

Proposition 1.2.6.

Soient $V_1, ..., V_p$ des endomorphismes d'un module M vérifant :

(i)

$$V_j \circ V_i = \begin{cases} V_i & si\ i = j \\ 0 & si\ i \neq j \end{cases} \tag{1.8}$$

(ii)

$$V_1 + ... + V_p = Id_M$$

Alors :

1. *Les V_i sont des projecteurs*
2. $M = \overset{p}{\underset{i=1}{\oplus}} V_i(M)$

Une telle décomposition de Id_M est dite décomposition de l'unité en une famille orthogonale de projecteurs.

Preuve.

1. Soit : $i = \{1, ..., p\}$

   On a $V_i \circ V_i = V_i$ d'après (1.8)

2. Par hypothèse $V_1 + ... + V_p = Id_M$. Donc $(V_1 + ... + V_p)(M) = Id_M(M)$. Alors $V_1(M) + \cdots + V_p(M) = M$. De plus, si $x \in \bigcap_{i=1}^{p} V_i(M)$, alors pour tout i, il existe $x_i \in M$ tel que $V_i(x_i) = x$. Soit $i \neq j$, on a $V_j \circ V_i(x_i) = V_j(x) = 0$, par suite $x \in \bigcap_{i=1}^{p} \operatorname{Ker} V_i$. Or $V_i \circ V_i(x_i) = V_i[V_i(x_i)] = V_i(x)$ et d'après (1.8) : $V_i \circ V_i(x_i) = V_i(x_i)$.

   Ainsi, $V_i(x) = V_i(x_i) = x$ et comme $x \in \operatorname{Ker} V_i$, $V_i(x) = 0$. Donc $x = 0$.

□

1.3 Les modules de type fini

Définition 1.3.1.

Soit A un $\mathbb{Z}$-module. La famille $(e_i)_{i \in I}$ est une base de A si pour tout $a \in A$, il existe des $\lambda_i \in \mathbb{Z}$ tels que $a = \sum_{i \in I} \lambda_i e_i$. On dit que A est libre si et seulement si A admet une base. Il est de *type fini* s'il admet une famille génératrice finie.

Théorème 1.3.2.

Soit A un $\mathbb{Z}$-module libre de type fini.Alors toutes les bases de A ont le même cardinal.

Preuve.

Soit $(a_1, ..., a_n)$ une base de A.

Considérons l'homomorphisme surjectif de groupe :

$$\begin{array}{rccc} \Phi : & A & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^n \\ & a = \sum_{i \leqslant n} \alpha_i a_i & \longmapsto & (\overline{\alpha_1}; ...; \overline{\alpha_p}) \end{array}$$

$A/2A$ est un F_2- espace vectoriel. En effet $(A/2A, +)$ est un groupe abélien et on vérifie le seul axiome non trivial

$$\text{pour tout } \lambda, \mu \in F_2, (\lambda + \mu)x = \lambda x + \mu x$$

si $\lambda = 1 = \mu$ on a

$$(1+1)\overline{x} = 2\overline{x} = \overline{0} \text{ et } \overline{x} + \overline{x} = 2\overline{x} = \overline{0}$$

De plus, on a : $\begin{aligned} \text{Ker } \Phi &= \{a \in A / \Phi(a) = 0\} \\ &= \left\{ \sum_{i=1}^{n} \alpha_i a_i / \alpha_i = 2\beta_i, \beta_i \in \mathbb{Z} \right\} \\ &= \left\{ \sum_{i=1}^{n} 2\beta_i a_i / \beta_i \in \mathbb{Z} \right\} \\ &= \left\{ 2\sum_{i=1}^{n} \beta_i a_i / \beta_i \in \mathbb{Z} \right\} \\ &= 2A \end{aligned}$

Comme Φ est surjective, $\Phi(A) = (\mathbb{Z}/2\mathbb{Z})^n$ et par suite $A/2A \simeq (\mathbb{Z}/2\mathbb{Z})^n$ donc $A/2A$ est de dimension n. Ce qui détermine n de manière unique. □

1.4 Completion d'une famille libre en une base

Lemme 1.4.1.

Soit $(\lambda_1, ..., \lambda_n) \in \mathbb{Z}^n (n \geqslant 2)$, *tel que* $pgcd(\lambda_1; ...; \lambda_n) = 1$.

Alors il existe $(\alpha_{i,j})_{\substack{1\leqslant i\leqslant n\\ 2\leqslant j\leqslant n}} \in \mathbb{Z}^{(n-1)n}$ *telle que :*

$$\begin{vmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} = 1$$

Preuve.

On raisonne par récurrence sur n.

Si $n = 2$, comme $pgcd(\lambda_1, \lambda_2) = 1$, il existe $(m, n) \in \mathbb{Z}^2$ tel que $\lambda_1 m - n\lambda_2 = 1$ c'est-à-dire $\begin{vmatrix} \lambda_1 & n \\ \lambda_2 & m \end{vmatrix} = 1$ Supposons que l'affirmation soit vraie jusqu'au rang $n-1$

Notons $d = pgcd(\lambda_1, ..., \lambda_{n-1})$ et $\mu_i = \dfrac{\lambda_i}{d}$ pour $1 \leqslant i \leqslant n-1$.

On a $pgcd(\mu_1; ...; \mu_{n-1}) = 1$ Soit donc $(\alpha_{i,j})_{1\leqslant i\leqslant n-1, 2\leqslant j\leqslant n-1}$ telle que

$$\begin{vmatrix} \mu_1 & \alpha_{12} & \dots & \alpha_{1(n-1)} \\ \mu_2 & \alpha_{22} & \dots & \alpha_{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n-1} & \alpha_{(n-1)2} & \dots & \alpha_{(n-1)(n-1)} \end{vmatrix} = 1$$

On sait que d et λ_n sont premiers entre eux. Ainsi, il existe $(k, \ell) \in \mathbb{Z}^2$ tel que

$$kd + \ell\lambda_n = 1$$

On a

$$\begin{vmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1(n-1)} & \ell\mu_1 \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2(n-1)} & \ell\mu_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_{n-1} & \alpha_{(n-1)2} & \dots & \alpha_{(n-1)(n-1)} & \ell\mu_{n-1} \\ \lambda_n & 0 & \dots & 0 & k \end{vmatrix}$$

$$= (-1)^{n-1}\left[\lambda_n \begin{vmatrix} \alpha_{12} & \dots & \alpha_{1(n-1)} & \ell\mu_1 \\ \alpha_{22} & \dots & \alpha_{2(n-1)} & \ell\mu_2 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{n-1\,2} & \dots & \alpha_{(n-1)(n-1)} & \ell\mu_{n-1} \end{vmatrix} + (-1)^{n-1}k \begin{vmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1(n-1)} \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \alpha_{(n-1)2} & \dots & \alpha_{(n-1)(n-1)} \end{vmatrix}\right]$$

$$= (-1)^{n-1}\left[\lambda_n\, \ell \begin{vmatrix} \alpha_{12} & \dots & \alpha_{1(n-1)} & \mu_1 \\ \alpha_{22} & \dots & \alpha_{2(n-1)} & \mu_2 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{(n-1)2} & \dots & \alpha_{(n-1)(n-1)} & \mu_{n-1} \end{vmatrix} + (-1)^{n-1}kd \begin{vmatrix} \mu_1 & \alpha_{12} & \dots & \alpha_{1(n-1)} \\ \mu_2 & \alpha_{22} & \dots & \alpha_{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n-1} & \alpha_{(n-1)2} & \dots & \alpha_{(n-1)(n-1)} \end{vmatrix}\right]$$

$$= (-1)^{n-1}\left[(-1)^{n-1}\lambda_n\ell + (-1)^{n-1}kd\right]$$

$$= \lambda_n l + kd$$

$$= 1$$ □

Proposition 1.4.2.

Soit $\lambda = (\lambda_1, ..., \lambda_n) \in \mathbb{Z}^n$ *tel que* $pgcd(\lambda_1; ...; \lambda_n) = 1$. *Alors, il existe* $(a_i)_{1 \leqslant i \leqslant n-1} \in (Z^n)^{n-1}$ *tel que* $(\lambda, a_1, ..., a_{n-1})$ *soit une* $\mathbb{Z}$*-base de* $\mathbb{Z}^n$.

Preuve.

Posons $M = \begin{pmatrix} \lambda_1 & \alpha_{12} & ... & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & ... & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}$

$\det(M) = 1$ d'après le lemme 1.4.1

Posons M' la comatrice de M et ${}^tM'$ la transposée de sa comatrice.

On a :

$$({}^tM')M = (\det(M))I_n = I_n$$

On en déduite que $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Notons $\xi_i \in \mathcal{M}_{n1}(\mathbb{Z})$ tel que $(\xi_i)_j = \delta_{ij}$ Dans ce cas :

$$MX = \xi_i \Leftrightarrow X = M^{-1}\xi_i \in \mathcal{M}_{n1}(\mathbb{Z})$$

Donc $\xi_i = \sum_{j=1}^{n} X_j C_j$ où C_j est la j-ième colonne de la matrice M. Ainsi $(C_j)_{1 \leqslant j \leqslant n}$ est génératrice de $\mathbb{Z}^n$ et libre car de bon cardinal. □

Définition 1.4.3.

Soient :

- K un anneau commutatif intègre
- M un K-module unitaire

1. Un élément $m \in M$ est dit *élément de torsion* s'il existe $a \in K^*$ tel que $am = 0$
2. L'ensemble de tous les éléments de torsion de M constitue un K-sous-module de M appelé *sous module de torsion* de M, noté M_{tor}
3. Lorsque $M = M_{tor}$, on dit que M est un *module de torsion*
4. Au cas où $M_{tor} = \{0\} \neq M$, on dit que M est *sans torsion*. Dans ce cas, pour $m \in M$, $a \in K^*$; on a :

$$a.m = 0 \Rightarrow m = 0$$

Théorème 1.4.4 (Quotients sans torsion de $\mathbb{Z}^n$).

Soit G un sous groupe de $\mathbb{Z}^n$ tel que $\mathbb{Z}^n/G$ soit sans torsion.

Alors il existe $k \in \mathbb{N}$ tel que $\mathbb{Z}^n/G \simeq \mathbb{Z}^k$.

Preuve.

On raisonne par récurrence sur n.

Si $n = 1$, alors G est le groupe nul et $k = 1$. En effet, on sait que les quotients de $\mathbb{Z}$

sont les $\mathbb{Z}/n\mathbb{Z}$ qui sont cycliques dès que $n > 1$.

Supposons que cette affirmation soit vraie jusqu'au rang $n-1$. Soit G un sous groupe, supposé non nul de $\mathbb{Z}^n$ tel que $\mathbb{Z}^n/G$ soit sans torsion. Soit $\lambda \in G$, $\lambda \neq 0$ avec $\lambda = (\lambda_1, ..., \lambda_n)$. Soit $d = \text{pgcd}(\lambda_1, ..., \lambda_n)$. Alors $\mu = \left(\dfrac{\lambda_i}{d}\right)_{i\in\mathbb{N}} \in G$.

En effet, sinon, on aurait en notant $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n/G$ l'homomorphisme surjectif canonique, $\varphi(\mu) \neq \overline{0}$ et $d\varphi(\mu) = \overline{0}$. On peut alors compléter μ en une base $(a_i)_{1\leqslant i\leqslant n}$ où $a_1 = \mu$ d'après la proposition 1.4.2.

Considérons

$$\begin{array}{rccc} \psi : & \mathbb{Z}^{n-1} & \longrightarrow & \mathbb{Z}^n/G \\ & (x_2, ..., x_n) & \longmapsto & \varphi\left(\displaystyle\sum_{i=2}^{n} x_i a_i\right) \end{array}$$

Cet homomorphisme est bien défini et surjectif car $\mu \in G$. En effet si
$X_1 = (x_2^{(1)}; \ldots; x_n^{(1)})$, $X_2 = (x_2^{(2)}; ...; x_n^{(2)})$ tel que $X_1 = X_2$. On a

$$\sum_{i=2}^{n} x_i^{(1)} a_i = \sum_{i=2}^{n} x_i^{(2)} a_i$$

et si $y \in \mathbb{Z}^n/G$ alors $y = (\overline{y}_1, ..., \overline{y}_n)$. Donc il existe $(y_1, ..., y_n)$ tel que

$$\begin{aligned} \varphi(y_1, ..., y_n) &= y \\ &= \varphi\left(\sum_{i=1}^{n} \alpha_i a_i\right) \\ &= \varphi\left(\sum_{i=2}^{n} \alpha_i a_i\right) + \varphi(\alpha_1 \mu) \\ &= \varphi\left(\sum_{i=2}^{n} \alpha_i a_i\right) + \alpha_1 \varphi(\mu) \end{aligned}$$

Or $\mu \in G$ donc ψ est surjectif.

Ainsi $\mathbb{Z}^{n-1}/\text{Ker } \psi \simeq \mathbb{Z}^n/G$. Or $\mathbb{Z}^{n-1}/\text{Ker } \psi$ est sans torsion. En effet, posons θ un isomorphisme de $\mathbb{Z}^{n-1}/\operatorname{Ker}\psi$ dans $\mathbb{Z}^n/G$. Soit $\overline{m} \in \mathbb{Z}^{n-1}/\operatorname{Ker}\psi$ tel que $\alpha\overline{m} = \overline{0}$ avec $\alpha \in \mathbb{Z}^*$.

On a $\theta(\alpha\overline{m}) = \overline{0} = \alpha\theta(\overline{m})$, avec $\theta(\overline{m}) \in \mathbb{Z}^n/G$.

Par hypothèse, $\mathbb{Z}^n/G$ est sans torsion, donc $\theta(\overline{m}) = \overline{0}$. Or θ est injective, c'est-à-dire

$\mathrm{Ker}\,\theta = \{\overline{0}\}$, on en déduit que $\overline{m} = \overline{0}$.

Enfin, l'hypothèse de récurrence nous permet de conclure le résultat. □

Théorème 1.4.5.

Tout $\mathbb{Z}$-module de type fini et sans torsion est libre.

Preuve.

Soit M un $\mathbb{Z}$-module de type fini et sans torsion et soit $(a_i)_{1\leqslant i\leqslant n}$ une famille génératrice de M. Considérons l'application φ définie par :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \longrightarrow & M \\ & \lambda = (\lambda_1, ..., \lambda_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} \lambda_i a_i \end{array}$$

Par définition φ est surjective, donc $M \simeq \mathbb{Z}^n/\mathrm{Ker}\varphi \simeq \mathbb{Z}^k$ d'après le théorème 1.4.4. Soient $(e_i)_{1\leqslant i\leqslant k}$ la base canonique de $\mathbb{Z}^k$ et f est un isomorphisme de $\mathbb{Z}^k$ sur M, alors $(f(e_i))_{1\leqslant i\leqslant k}$ est une $\mathbb{Z}$-base de M □

Théorème 1.4.6.

Soient p un nombre premier et A un $\mathbb{Z}$-module libre de type fini, alors A/pA est un anneau fini non nul.

Preuve.

Le fait que A/pA soit un anneau est acquis dès la construction de A/pA.

Pour montrer qu'il est fini non nul, il suffit de montrer que $(A/pA) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ si rg $A = n$ c'est-à-dire $< a_1, ..., a_n >= A$.

Considérons l'homomorphisme surjectif

Posons :

$$\begin{array}{rccc} \psi : & A & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^n \\ & \sum \lambda_i a_i & \longmapsto & (\overline{\lambda}_1, \overline{\lambda}_2, ..., \overline{\lambda}_n) \end{array}$$

On a $\mathrm{Ker}\,\psi = pA$ et comme ψ est surjective, $A/pA \simeq (\mathbb{Z}/pZ)^n$ □ □

Chapitre 2

Variété torique

2.1 Cônes

Définition 2.1.1.

Un ensemble non vide d'un espace Euclidien est dit *cône convexe* si

$$\lambda x + \mu y \in C \ \forall x, y \in C \text{ et } \lambda, \mu \geqslant 0$$

Soient maintenant :

$N \simeq \mathbb{Z}^n$ un réseau (module libre de rang n), $M = \text{Hom}\ (N, \mathbb{Z})$ son dual

Nous noterons

$N_{\mathbb{R}} = N \otimes \mathbb{R} \simeq \mathbb{R}^n$ le $\mathbb{R}$-espace vectoriel associé à N ; $M_{\mathbb{R}} = \mathcal{L}(\mathbb{R}^n, \mathbb{R})$ le $\mathbb{R}$-espace vectoriel associé à M.

Définition 2.1.2.

On appelle *cône rationnel polyédral fortement convexe* un sous ensemble σ de $\mathbb{N}_{\mathbb{R}}$ tel qu'il existe une famille fini $(a_i)_{i \in I}$ d'éléments de N telle que

$$\sigma \ = \sum_{i \in I} \mathbb{R}^+ a_i = \{\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_s a_s / \ \alpha_i \in \mathbb{R}_+ \text{ pour } 1 \leqslant i \leqslant s\}$$

et

$$\sigma \cap (-\sigma) = \{0\}$$

Dans ce cas, on dit que σ est de type fini et on le note $\sigma =< a_1, ..., a_s >$

La *dimension* de σ est définie comme la dimension de l'espace vectoriel réel engendré par les points du cône σ.

On définit le produit $\mathbb{R}$-bilinéaire canonique sur $M_{\mathbb{R}} \times N_{\mathbb{R}}$ par :

$$<,>: M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}(\text{ par exemple le produit usuel de } \mathbb{R}^n)$$

Notons $\sigma^* = \{v \in M_{\mathbb{R}} :< v, x >\geqslant 0, \forall x \in \sigma\} \subseteq M_{\mathbb{R}}$

$$\sigma^{\perp} = \{v \in M_{\mathbb{R}} :< v, x >= 0, \forall x \in \sigma\} \subseteq M_{\mathbb{R}}$$

le dual et l'orthogonal respectifs du cône σ

Définition 2.1.3.

On dit que $\tau \subset \sigma$ est une *face de* σ (on notera $\tau \leqslant \sigma$) s'il est possible de trouver $v \in \sigma^*$ tel que $\tau = \sigma \cap \{v\}^{\perp}$.

$\tau =< a_1, ..., a_k >$ est dit *simplicial* de dimension k si les $a_i (i = 1, ..., k)$ sont linéairement indépendants.

Proposition 2.1.4.

Soit σ un cône de dimension n. Les faces de σ de dimension $p < n$ sont exactement les cônes engendrés par la famille $\{a_1, ..., a_p\}$ de cardinal p.

Preuve.

On a $\sigma = \{\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_n a_n,\ \alpha_i \geqslant 0,\ a_i \in \mathbb{Z}^n \text{pour } 1 \leqslant i \leqslant n\}$

Comme $\tau \leqslant \sigma$, si $x \in \tau$, alors $x \in \sigma$.

Donc il existe $(\alpha_i)_{1 \leqslant i \leqslant m[x]}$ tel que $x = \sum_{i=1}^{m[x]} \alpha_i a_i$ avec $\alpha_i \geqslant 0$ pour tout $1 \leqslant i \leqslant m[x]$ et $m[x] \leqslant n$

Ainsi chaque élément de τ s'écrit de cette façon.

Prenons $m = \sup\{m[x]/x \in \tau\}$

alors, on a

$$\tau = \{\alpha_1 a_1 + ... + \alpha_m a_m : \alpha_i \geqslant 0, a_i \in \mathbb{Z}^n \text{ pour } 1 \leqslant i \leqslant n\}$$

□

Proposition 2.1.5.

Le dual d'un cône est un cône.

Preuve.

On a

$$\sigma^* = \{v \in M_{\mathbb{R}} :< v, x >\geqslant 0, \forall x \in \sigma\}$$

Notons e_k^* l'application

$$\begin{array}{lccc} e_k^* : & \mathbb{R}^n & \longrightarrow \mathbb{R} & \text{pour tout } 1 \leqslant k \leqslant n \\ (x_1, ..., x_k, ..., x_n) & \longmapsto & e_k^*(x_1, ..., x_k, ..., x_n) = x_k & \end{array}$$

Prenons $x \in \sigma$, on a

$$x = \alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_n e_n$$

où

$$\begin{array}{rcl} e_i = & (0, \quad ..., \quad 0, & 1, \qquad 0, ..., \quad 0) \\ & & \uparrow \\ & & i^{eme} \quad \text{rang} \end{array}$$

donc

$$x = e_1^*(x)e_1 + e_2^*(x)e_2 + ... + e_n^*(x)e_n$$

Soit maintenant $v \in \sigma^*$, on a :

$$v(x) = v(e_1)e_1^*(x) + v(e_2)e_2^*(x) + ... + v(e_n)e_n^*(x)$$

Alors $v = \beta_1 e_1^* + \beta_2 e_2^* + ... + \beta_n e_n^*$ avec $\beta_i = v(e_i) \quad 1 \leqslant i \leqslant n$

Par suite

$$\sigma^* = \{\beta_1 e_1^* + \beta_2 e_2^* + ... + \beta_n e_n^*; \beta_i \geqslant 0 \text{ pour } 1 \leqslant i \leqslant n\}$$

□

Proposition 2.1.6.

Soient deux cônes σ et δ. Alors

i) $((\sigma)^*)^* \simeq \sigma$

ii) $\sigma = ((\sigma)^\perp)^\perp$

iii) $\sigma^\perp + \delta^\perp \subseteq (\sigma \cap \delta)^\perp$

iv) $(\sigma + \delta)^\perp = \sigma^\perp \cap \delta^\perp$

Preuve.

i) Prenons l'homomorphisme

$$\begin{array}{rcl} \theta : \ \sigma & \longrightarrow & (\sigma^*)^* \\ x & \longmapsto & \theta_x : \ \sigma^* \longrightarrow \mathbb{R} \\ & & f \longmapsto \theta_x(f) = f(x) \end{array}$$

Soit x tel que $\theta_x = 0$, alors on a nécessairement $x = 0$

Donc $\ker\theta = \{0\}$ et θ est ainsi injective. Par suite, θ est bijective.

ii) Il suffit de remarquer que :

$$\sigma^\perp = \{v \in M_{\mathbb{R}}, < v, x >= 0, \text{ pour tout } x \in \sigma\}$$

$$(\sigma^\perp)^\perp = \{x \in \sigma, < v, x >= 0, \text{ pour tout } v \in \sigma^\perp\}$$

iii) D'abord, il est nécessaire de remarquer que si $\sigma \subset \delta$, alors $\delta^\perp \subset \sigma^\perp$

On a :

$$\sigma \cap \delta \subseteq \sigma, \text{ implique } \sigma^\perp \subseteq (\sigma \cap \delta)^\perp$$

$$\sigma \cap \delta \subseteq \delta, \text{ implique } \delta^\perp \subseteq (\sigma \cap \delta)^\perp$$

Ainsi $\sigma^\perp + \delta^\perp \subseteq (\sigma \cap \delta)^\perp$

iv) D'une part, on a : $\sigma \subseteq \sigma + \delta$ et $\delta \subseteq \sigma + \delta$. Alors on a $(\sigma + \delta)^\perp \subseteq \sigma^\perp$ et $(\sigma + \delta)^\perp \subseteq \delta^\perp$, ainsi $(\sigma + \delta)^\perp \subseteq \sigma^\perp \cap \delta^\perp$

Réciproquement, soit $v \in \sigma^\perp \cap \delta^\perp$ et $x \in \sigma + \delta$.

Alors, il existe $y \in \sigma$ et $z \in \delta$ tel que $x = y + z$. Ainsi,

$$< v, x >=< v, y > + < v, z >= 0$$

Donc, $v \in (\sigma + \delta)^{\perp}$ et on a par suite $\sigma^{\perp} \cap \delta^{\perp} \subseteq (\sigma + \delta)^{\perp}$. D'où l'égalité voulue.

□

2.2 Variétés affines

Définition 2.2.1.

Soit k un corps et $f_1, ..., f_s \in k[x_1, ..., x_n]$.

L'ensemble noté $V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in k^n / f_i(a_1, ..., a_n) = 0, 1 \leqslant i \leqslant s\}$ est appelé *variété affine* définie par $f_1, f_2, ..., f_s$. Donc $V(f_1, ..., f_s) \subset k^n$ et c'est l'ensemble des solutions du système d'équations (S) :

$$\begin{cases} f_1(x_1, ..., x_n) & = 0 \\ f_2(x_1, ..., x_n) & = 0 \\ \vdots & \vdots \\ f_s(x_1, ..., x_n) & = 0 \end{cases}$$

La dimension d'une telle variété affine est égale à $n - r$ où $r = \text{rang } (S)$.

Exemple 2.2.2.

Fixons $k = \mathbb{R}$.

$V(x^2 + y^2 - 1)$ est une variété affine dans $\mathbb{R}^2$ qui n'est autre que le cercle de centre O et de rayon 1.

Lemme 2.2.3.

Si $W, V \subseteq k^n$ des variétés affines. Alors $V \cap W$ et $V \cup W$ sont aussi des variétés affines.

Preuve.

Supposons : $V = V(f_1, ..., f_s)$, $W = V(g_1, ..., g_t)$

$$V \cap W = V(f_1, ..., f_s, g_1, ..., g_t)$$

$$V \cup W = V(f_i g_j; 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t)$$

□

Exemple 2.2.4.

$V[(x-2)(x^2-y); y(x^2-y); (z+1)(x^2-y)] = V(x-2; y; z+1) \cup V(x^2-y)$

2.3 Idéaux

Définition 2.3.1.

Soit I un sous-ensemble de $k[X_1, ..., X_n]$.

I est un idéal de $k[X_1, ..., X_n]$ si et seulement si :

i) $0 \in I$

ii) I est stable par l'addition : $f, g \in I \Rightarrow f + g \in I$

iii) I est stable par la multiplication : $(f \in I, h \in k[X_1, ..., X_n]) \Rightarrow f.h \in I$

Définition 2.3.2.

Soient $f_1, f_2, ..., f_s \in k[X_1, ..., X_n]$.

Alors l'ensemble $I =< f_1, ..., f_s >= \{\sum_{i=1}^{s} h_i f_i, h_1, ..., h_s \in k[X_1, ..., X_n]\}$ est un idéal de $k[X_1, ..., X_n]$ engendré par $f_1, ..., f_s$.

Dans ce cas, I est dit de générateur fini et $\{f_1, ..., f_s\}$ est une base de I.

Proposition 2.3.3.

Si $\{f_1, ..., f_s\}$ et $\{g_1, ..., g_s\}$ sont des bases d'un même idéal I, alors

$$V(f_1, ..., f_s) = V(g_1, ..., g_s)$$

Preuve.

Comme $f_i \in I$ $(1 \leqslant i \leqslant s)$, donc chaque f_i est une combinaison linéaire de $g_1, ..., g_s$ à coéfficient dans $k[X_1, ..., X_n]$. L'autre inclusion s'obtient analogiquement. □

Exemple 2.3.4.

Posons $f(X, Y) = 2X^2 + 3Y^2 - 11$

$g(X, Y) = X^2 - Y^2 - 3$

on a

$$\begin{aligned}\frac{1}{5}f(X,Y)-\frac{2}{5}g(X,Y) &= \frac{1}{5}(2X^2+3Y^2-11)-\frac{2}{5}(X^2-Y^2-3)\\ &= \frac{2}{5}X^2+\frac{3}{5}Y^2-\frac{11}{5}-\frac{2}{5}X^2+\frac{2}{5}Y^2+\frac{6}{5}\\ &= Y^2-1\end{aligned}$$

$$\begin{aligned}\frac{1}{5}f(X,Y)+\frac{3}{5}g(X,Y) &= \frac{1}{5}(2X^2+3Y^2-11)+\frac{3}{5}(X^2-Y^2-3)\\ &= \frac{2}{5}X^2+\frac{3}{5}Y^2-\frac{11}{5}+\frac{3}{5}X^2-\frac{3}{5}Y^2-\frac{9}{5}\\ &= X^2-4\end{aligned}$$

Donc

$$< 2X^2+3Y^2-11; X^2-Y^2-3 >=< X^2-4; Y^2-1 >$$

et

$$V(2X^2+3Y^2-11; X^2-Y^2-3) = V(X^2-4; Y^2-1)$$

Définition 2.3.5.

Soit $V \subset k^n$ une variété affine. On définit l'ensemble :

$$I(V) := \{f \in k[X_1,...,X_n], f(a_1,...,a_n) = 0 \text{ pour tout } (a_1,...,a_n) \in V\}$$

Dans ce cas, $I(V)$ est appelé *idéal de la variété* V.

Exemple 2.3.6.

$\{(0,0)\} \subset k^2$ est une variété affine.

On a : $I(\{(0,0)\}) =< x; y >$

Lemme 2.3.7.

Soient $f_1,..,f_s \in k[X_1,...,X_n]$.

Notons $V = V(f_1,..,f_s)$. *Alors* $< f_1,..,f_s > \subseteq I(V)$

Preuve.

Soit $f \in < f_1, .., f_s >$. Alors, f est une combinaison linéaire de $f_1, .., f_s$ à coéfficient dans $k[X_1, ..., X_n]$.

Or chaque $f_i \quad (1 \leqslant i \leqslant s)$ s'annule sur V, ainsi, il en est de même pour f. Par suite, $f \in I(V)$. □

Pour le contre exemple, on peut considérer l'idéal engendré par $\{X^2; Y^2\}$. En effet, $< X^2; Y^2 > \subsetneq I(V)$, avec $V = V(X^2, Y^2) = \{(0, 0)\}$,

car $X + Y \in I(V)$ mais $X + Y \notin < X^2; Y^2 >$

Proposition 2.3.8.

Soient V et W deux variétés affines de k^n. Alors $V \subseteq W$ si et seulement si $I(V) \supseteq I(W)$.

Preuve.

Soit $f \in I(W)$. Donc f s'annule sur W. Et comme $V \subseteq W$, f s'annule aussi sur V. Par suite, $f \in I(V)$.

Réciproquement, posons $V = V(f_1, ..., f_s)$, $W = V(g_1, ..., g_t)$.

Soit $x \in V$. Comme $I(W) \subseteq I(V)$; donc tous les polynômes de $I(W)$ s'annulent sur V. Ainsi, $g_i(x) = 0$, $1 \leqslant i \leqslant t$. Par suite, $x \in W$. □

Définition 2.3.9.

Soit $I \subset k[X_1, ..., X_n]$ un idéal. On notera par $V(I)$ l'ensemble

$$V(I) := \{(a_1, ..., a_n) \in k^n / f(a_1, ..., a_n) = 0 \text{ pour tout } f \in I\}$$

Proposition 2.3.10.

$V(I)$ est une variété affine. En particulier, si $I =< f_1, ..., f_s >$, alors
$V(I) = V(f_1, ..., f_s)$.

Preuve.

Pour la preuve, admettons que I a un générateur fini (nous ferons la démonstration dans le prochain chapitre).

Alors, supposons maintenant que $I =< f_1, ..., f_s >$

Soit $(a_1, ..., a_n) \in V(I)$. On a $f_i(a_1, ..., a_n) = 0$ car $f_i \in I \quad (1 \leqslant i \leqslant s)$.

Donc

$$(a_1, ..., a_n) \in V(f_1, ..., f_s)$$

Par suite

$$V(I) \subseteq V(f_1, ..., f_s)$$

Prenons maintenant $(a_1, ..., a_n) \in V(f_1, ..., f_s)$. Donc $f_i(a_1, ..., a_n) = 0$ pour tout $1 \leqslant i \leqslant s$. Or, les éléments de I sont des combinaisons à coéfficient dans $k[X_1, ..., X_n]$ des $f_1, ..., f_s$. Ainsi, si $f \in I$, alors $f(a_1, ..., a_n) = 0$.

D'où

$$V(f_1, ..., f_s) \subseteq V(I)$$

□

2.4 Variété torique associée à un cône polyhedral convexe

Soit $\sigma \in N_{\mathbb{R}}$ un cône polyhedral convexe (on dira désormais un cône).

Notons $\mathcal{S}_\sigma = M \cap \sigma^* = \{a \in M / < a, y > \geqslant 0, \forall y \in \sigma\}$, c'est un sous semi-groupe de M qui a la propriété d'être engendré par un nombre fini d'élément de M, c'est-à-dire :

$$\begin{aligned} \mathcal{S}_\sigma &= \mathbb{Z}^+ a_1 + ... + \mathbb{Z}^+ a_s \\ &= \{\alpha_1 a_1 + ... + \alpha_s a_s / \text{pour tout } i, \alpha_i \in \mathbb{Z}, \alpha_i \geqslant 0\} \end{aligned}$$

On associe à $\mathcal{S}_\sigma$ une $\mathbb{C}$ algèbre de type fini, puis une variété algébrique affine de la manière suivante :

Soit $\mathcal{S}_\sigma =< a_1, ..., a_s >$ et $\mathcal{A}_\sigma = \mathbb{C}[u_1, ..., u_s]$ l'algèbre de type fini engendrée par $u_1 = Z^{a_1}, ..., u_s = Z^{a_s}$ où u_i sont les *variables toriques* et Z_i les *coordonnées affines* dans $(\mathbb{C}^*)^n$ avec $Z^{a_i} = Z_1^{a_{i_1}} \times ... \times Z_s^{a_{i_s}}$, $\mathbb{C}^* = \mathbb{C} \backslash \{0\}$ et $Z = (Z_1, ..., Z_s)$.

Comme $\mathcal{S}_\sigma$ est de type fini, $\mathcal{A}_\sigma$ l'est aussi, elle s'écrit donc comme quotient d'un anneau de polynôme $\mathbb{C}[Y_1, ..., Y_s]$ par un idéal.

Comme $\mathbb{C}[Y_1, ..., Y_s]$ est noethérien, tout idéal est engendré par un nombre fini de polynômes $F_1, ..., F_m$ c'est-à-dire :

$$\mathcal{A}_\sigma = \mathbb{C}[Y_1, ..., Y_s]/(F_1, ..., F_m)$$

La variété algébrique affine V_σ associée au cône σ est par définition le sous-ensemble de C^s défini par les équations $F_1 = ... = F_m = 0$.

Définition 2.4.1.

V_σ est appelé la variété torique affine associé à σ et $(F_1, ..., F_m)$ l'idéal torique.

Pour un cône σ, on pose

$$\begin{aligned} U_\sigma = \quad & \{v : \sigma^* \cap M \to \mathbb{C}; v(0) = 1, v(m + m') = v(m)v(m'), \\ & \text{pour tout } m, m' \in \sigma^* \cap M\} \end{aligned}$$

Proposition 2.4.2.

Il existe une bijection Φ de V_σ vers U_σ.

Preuve.

Dans toute la suite, on notera $\varphi_x = \Phi(x)$ pour tout $x \in V_\sigma$.

On peut associer à un point $(y_1, ..., y_s)$ de V_σ un idéal maximal
$(Y_1 - y_1, ..., Y_s - y_s)$ de l'algèbre $\mathcal{A}_\sigma$. Cette correspondance est bijective (d'après le Nullstellensatz). Par ailleurs, à chaque idéal maximal, on peut associer bijectivement un homomorphisme surjectif ψ de $\mathbb{C}$-algèbres de la manière suivante :

$$\begin{aligned} \gamma : \quad V_\sigma \quad &\longrightarrow \quad \mathcal{I} \\ (y_1, ..., y_s) \quad &\longmapsto \quad (Y_1 - y_1, ..., Y_s - y_s) \end{aligned}$$

$$\begin{aligned} \xi : \ \mathcal{I} \quad &\longrightarrow \quad F \\ I \quad &\longmapsto \quad \xi(I) = (\psi : \mathcal{A}_\sigma \to \mathcal{A}_\sigma/I \simeq \mathbb{C}) \end{aligned}$$

où $\mathcal{I}$ est l'ensemble des idéaux maximaux de et $\mathcal{A}_\sigma$, $F = \{\mathcal{A}_\sigma \to \mathcal{A}_\sigma/I; I \in \mathcal{I}\}$

l'application inverse est de la forme

$$(\psi : \mathcal{A}_\sigma \to \mathbb{C}) \longmapsto \ker \psi$$

On a donc associé à chaque point x de V_σ un homomorphisme surjectif de $\mathbb{C}$-algèbre ψ_x.

On peut alors construire un homomorphisme de semi-groupe $\varphi_x \in U_\sigma$ comme composé des applications suivantes :

$$\begin{array}{ccc} \sigma^* \cap M & \longrightarrow & \mathcal{A}_\sigma \\ v & \longmapsto & Z^v \end{array}$$

et de ψ_x, avec $\varphi_x(a_i) = x_i$ pour tout $1 \leqslant i \leqslant s$.

C'est-à-dire

$$\begin{array}{rccc} \Phi : & V_\sigma & \longrightarrow & U_\sigma \\ & x & \longmapsto & \Phi(x) = \varphi_x \end{array}$$

où

$$\begin{array}{rccccc} \varphi_x : & \sigma^* \cap M & \longrightarrow & \mathcal{A}_\sigma & \stackrel{\psi_x}{\to} & \mathbb{C} \\ & u & \longmapsto & Z^u & \longmapsto & \psi_x(Z^u) \end{array}$$

$\varphi_x \in U_\sigma$ car $0 \longmapsto Z^0 = 1 \longmapsto 1$ et

$$(m + m') \longmapsto Z^{m+m'} = \psi_x(Z^{m+m'}) = \psi_x(Z^m \times Z^{m'}) = \psi_x(Z^m)\psi_x(Z^{m'})$$

un point $x \in V_\sigma$ correspond donc à un homomorphisme φ_x de semi-groupe

$$\begin{array}{ccc} \sigma^* \cap M & \longrightarrow & \mathcal{A}_\sigma \longrightarrow (\mathbb{C}, .) \\ u & \longmapsto & Z^u \longmapsto \psi_x(Z^u) \end{array}$$

et cette correspondance est bijective. □

Soit $\{a_1, ..., a_s\}$ une partie génératrice de $\sigma^* \cap M$. Dans ce cas, la variété V_σ est un sous ensemble de $\mathbb{C}^s$. D'après la preuve de la proposition 2.4.2, à un point

$x = (x_1, ..., x_s) \in V_\sigma$, on peut associer un homomorphisme Φ défini par $\Phi(x) = \varphi_x$ de la forme $\varphi_x(a_i) = x_i$, $1 \leqslant i \leqslant s$.

La variété V_σ contient un point distingué que l'on notera x_σ. C'est le point associé à :

$$\begin{array}{rccl} \varphi_{x_\sigma} : & \sigma^* \cap M & \longrightarrow & (\mathbb{C}, .) \\ & \mu & \longmapsto & \begin{cases} 1 & \text{si } \mu \in \sigma^\perp \\ 0 & \text{sinon} \end{cases} \end{array}$$

2.5 Action d'un tore, orbites et diviseurs

Définition 2.5.1.

Le *tore* $T = (C^*)^n$ est un groupe qui agit sur lui-même par la multiplication.

Soit $\{a_1, ..., a_s\}$ un système de générateurs du semi-groupe S_σ, et soit un vecteur $t = (t_1, ..., t_n) \in T$. L'action du tore sur chaque variété torique affine V_σ est donnée par :

$$\begin{array}{rcl} T \times V_\sigma & \longrightarrow & V_\sigma \\ (t, u_1, ..., u_s) & \longmapsto & (t^{a_1} u_1, ..., t^{a_s} u_s) \end{array} \qquad \text{où } t^{a_i} = t_1^{a_{i1}} ... t_n^{a_{in}}$$

Soit τ une face du cône σ et $S_\sigma =< a_1, ..., a_s >$. Notons $I = \{i \in \{1, ..., s\} / a_i \notin \tau^\perp\}$. On appelle *diviseur* associé à τ, l'ensemble noté D_τ et défini par

$$D_\tau = \{u \in V_\sigma / u_i = 0, \text{ pour tout } i \in I\}$$

Exemple 2.5.2.

Dans $\mathbb{R}^2$, considérons le cône σ engendré par les vecteurs $2e_1 - e_2$ et e_2. Le semi-groupe S_σ est engendré par

$$\{a_1 = e_1^*; a_2 = e_1^* + e_2^*; a_3 = e_1^* + 2e_2^*\}$$

On obtient alors la $\mathbb{C}$-algèbre $\mathbb{C}[Z_1, Z_1Z_2, Z_1Z_2^2]$ qui est isomorphe à $\mathbb{C}[u_1, u_2, u_3]/(u_1u_3 - u_2^2)$ où $(u_1u_3 - u_2^2)$ est l'idéal engendré par la relation $u_1u_3 = u_2^2$.

La relation additive $a_1 + a_3 = 2a_2$ donne la relation $u_1u_3 = u_2^2$ entre les coordonnés toriques. La variété torique affine correspondant au cône σ est donc représentée par le cône quadratique suivant :

$$V_\sigma = \{(u_1, u_2, u_3) \in \mathbb{C}^3 / u_1u_3 = u_2^2\}$$

Décrivons à présent les diviseurs et les orbites de cette variété V_σ.

Considérons l'arête (cône de dimension 1) τ_1 engendré par e_2. Alors, $i \in I$ si $< a_i, e_2 > \neq 0$. Donc $I = \{2, 3\}$. L'équation de D_{τ_1} dans l'espace $\mathbb{C}^3$ est donnée par

$$u_2 = 0, u_3 = 0$$

Dans $\mathbb{C}^3$, on a donc $D_{\tau_1} = \mathbb{C} \times \{0\} \times \{0\}$.

Si nous notons τ_2, l'arête engendrée par $2e_1 - e_2$. $i \in I$ si et seulement si $< a_i, 2e_1 - e_2 > \neq 0$ et donc $I = \{1, 2\}$. L'équation de D_{τ_2} dans l'espace $\mathbb{C}^3$ est donnée par

$$u_1 = 0, u_2 = 0$$

Dans $\mathbb{C}^3$, on a donc que $D_{\tau_2} = \{0\} \times \{0\} \times \mathbb{C}$

Enfin, le cône lui-même peut être considéré comme une face et donc, pour cette face particulière, on a $I = \{1, 2, 3\}$. Ainsi, D_σ est donnée par $u_1 = 0, u_2 = 0, u_3 = 0$. Donc $D_\sigma = O_\sigma$ est l'origine $(0, 0, 0) \in \mathbb{C}^3$.

On peut alors lister les orbites suivants :

1. $O_\sigma = \{(0, 0, 0)\}$
2. $O_{\tau_1} = \mathbb{C}^* \times \{0\} \times \{0\}$, orbite du point distingué $x_{\tau_1} = (1, 0, 0)$
3. $O_{\tau_2} = \{0\} \times \{0\} \times \mathbb{C}^*$, orbite du point distingué $x_{\tau_2} = (0, 0, 1)$

Chapitre 3

Base de Gröbner

3.1 Ordres lexicographiques sur $\mathbb{N}^n$

Dans toute la suite, on notera $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ et $\beta = (\beta_1, ..., \beta_n) \in \mathbb{N}^n$.

3.1.1 Ordre lexicographique

On dit que $\alpha \leqslant_{\text{lex}} \beta$ par l'ordre lexicographique si la première composante non nulle à gauche des vecteurs $\beta - \alpha$ est positive.

On dira ainsi : $X^\alpha \leqslant_{\text{lex}} X^\beta$ si $\alpha \leqslant_{\text{lex}} \beta$.

Par exemple dans $\mathbb{N}^3$, $(3; 2; 1) \leqslant_{\text{lex}} (3; 2; 4)$. Et par suite

$$X^3Y^2Z \leqslant_{\text{lex}} X^3Y^2Z^4$$

3.1.2 Ordre lexicographique gradué

On dit que $\alpha \leqslant_{\text{grlex}} \beta$ si $|\alpha| < |\beta|$

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

Dans le cas où $|\alpha| = |\beta|$, on prendra l'ordre lexicographique.

Pour l'exemple, fixons $n = 3$. on a $(1; 2; 0) \leqslant_{\text{grlex}} (3; 2; 0); (1; 1; 5) \leqslant_{\text{grlex}} (1; 2; 4)$

3.1.3 Ordre lexicographique inverse

On dit que $\alpha \leqslant_{\text{invlex}} \beta$ si la première composante non nulle à droite de vecteur $\beta - \alpha$ est positive.

Par exemple $(4;7;1) \leqslant_{\text{invlex}} (4;2;3)$

3.1.4 Ordre lexicographique gradué-inverse

On dit que $\alpha \leqslant_{\text{grevlex}} \beta$ si $|\alpha| < |\beta|$.

Dans le cas où $|\alpha| = |\beta|$, on prendra l'ordre lexicographique inverse.

Pour l'exemple, fixons $n = 3$

$(7;0;1) \leqslant_{\text{grevlex}} (2;3;5)$; $(5;3;2) \leqslant_{\text{grevlex}} (6;0;4)$

3.1.5 Ordre lexicographique renversé

On dit que $\alpha \leqslant_{\text{revlex}} \beta$ si $|\alpha| < |\beta|$.

Dans le cas où $|\alpha| = |\beta|$, $\alpha \leqslant_{\text{revlex}} \beta$ s'il existe $k \in \{1, ..., n\}$ tel que $\alpha_i = \beta_i$ pour tout $k+1 \leqslant i \leqslant n$ et $\beta_k \leqslant \alpha_k$.

3.2 Ordre monômial

Définition 3.2.1.

Un *ordre monomial* de $k[X_1, ..., X_n]$ est une relation d'ordre "$\leqslant$" sur $\mathbb{N}^n$. c'est-à-dire sur l'ensemble $\{X^\alpha, \alpha \in \mathbb{N}^n\}$ vérifiant les conditions suivantes :

i) $\leqslant$ est un ordre total sur $\mathbb{N}^n$

ii) si $\alpha \leqslant \beta$, alors pour tout $\gamma \in \mathbb{N}^n$, on a $\alpha + \gamma \leqslant \beta + \gamma$

iii) $\leqslant$ est un bon ordre sur $\mathbb{N}^n$ c'est-à-dire, tout sous ensemble non vide de $\mathbb{N}^n$ admet un plus petit élément par $\leqslant$.

Définition 3.2.2.

Soient $f = \sum_{\alpha} a_\alpha X^\alpha$ un polynôme non nul de $k[X_1, ..., X_n]$ et "$\leqslant$" un ordre monomial. On appelle :

i) *multidegré* de f, noté $\text{multideg}(f) := \max_{\leqslant}\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$

ii) *coefficient dominant* de f, noté $\text{LC}(f) := a_{\text{multideg}(f)} \in k$

iii) *terme dominant* de f, noté $\text{LT}(f) :=\text{LC}(f)X^{\text{multideg}(f)}$

iv) *monôme dominant* de f, noté $\text{LM}(f) := X^{\text{multideg}(f)}$

Exemple 3.2.3.

Soit $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$

En prenant l'ordre lexicographique $\leqslant_{\text{lex}}$, on a :

- $\text{multideg}(f) = (3; 0; 0)$
- $\text{LC}(f) = -5$
- $\text{LM}(f) = X^3$
- $\text{LT}(f) = -5X^3$

3.2.1 Algorithme de division dans $k[X_1, ..., X_n]$

Fixons un ordre monômial $\leqslant$ sur $\mathbb{N}^n$ et soit $F = (f_1, ..., f_s)$ un s-uplet de polynômes dans $k[X_1, ..., X_n]$. Alors tout polynôme $f \in k[X_1, ..., X_n]$ peut s'écrire comme

$$f = a_1f_1 + a_2f_2 + ... + a_sf_s + r \text{ où } a_i \in k,\ r \in k[X_1, ..., X_n]$$

et soit $r = 0$, soit r est une combinaison linéaire à coefficient dans k des polynômes qui ne divisent aucun des $\text{LT}(f_1)$;... ;$\text{LT}(f_s)$.

r sera appelé le reste de la division de f par F. De plus, si $a_if_i \neq 0$, alors, on a : $\text{multideg}(f) \geqslant \text{multideg}(a_if_i)$

Exemple 3.2.4.

Considérons l'ordre lexicographique

$f = X^2Y + XY^2 + Y^2$; $f_1 = Y^2 - 1$ et $f_2 = XY - 1$

Soit alors $F = (f_1, f_2)$

On a : $f = (Y^2 - 1) + (X + Y)(XY - 1) + X + Y + 1$

$= f_1 + (X + Y)f_2 + X + Y + 1$

3.3 Base de Hilbert

Définition 3.3.1.

Un idéal $I \subset k[X_1, ..., X_n]$ est un *idéal monômiale* s'il existe un sous-ensemble $A \subseteq \mathbb{N}^n$ (éventuellement *infini*) tel que $I =< X^\alpha : \alpha \in A >$.

Lemme 3.3.2.

Soit $I =< X^\alpha : \alpha \in A >$, un idéal monômiale. Alors le monôme $X^\beta \in I$ si et seulement si X^β est divisible par X^α pour un certain $\alpha \in A$.

Preuve.

Si X^β est un multiple de X^α, pour un certain $\alpha \in A$, alors, $X^\beta \in I$ d'après la définition même d'un idéal. Réciproquement, si $X^\beta \in I$, alors, on peut écrire $X^\beta = \sum_{i=1}^{s} h_i X^{\alpha(i)}$ où $h_i \in k[X_1, ..., X_n]$ pour $1 \leqslant i \leqslant s$ et $\alpha(i) \in A$.

Si on développe chaque h_i comme combinaison linéaire des monômes, on voit que les termes à droite de l'équation ci-dessus sont divisibles par un certain $X^{\alpha(i)}$. Alors, il en est de même pour X^β □

Lemme 3.3.3.

Soit I un idéal monômiale, et soit $f \in k[X_1, ..., X_n]$. Alors, les assertions suivantes sont équivalentes :

i) $f \in I$

ii) tous les termes de f appartiennent à I

iii) f est un k-combinaison linéaire des monômes de I

Preuve.

i)⇒ii) Si $f \in I$, alors on a

$$f = a_1 X^{\beta(1)} + ... + a_t X^{\beta(t)} = h_1 X^{\alpha(1)} + h_2 X^{\alpha(2)} + ... + h_s X^{\alpha(s)}$$

D'après la preuve du lemme 3.3.2, le second membre divise un certain $X^{\alpha(i)}$. Donc il en est de même pour f, et particulièrement, pour chaque terme de f. Par suite $X^{\beta(i)} \in I$ $(1 \leqslant i \leqslant t)$, donc $a_i X^{\beta(i)} \in I$ pour tout $i \in \{1, ..., t\}$

ii)⇒iii) C'est claire car $X^{\beta(i)} \in I$ $(1 \leqslant i \leqslant t)$

iii)⇒i) Comme $f = \sum_{i=1}^{t} a_i X^{\beta(i)}$, alors $f \in I$ car un idéal est stable par l'addition.

□

Corollaire 3.3.4.

Deux idéaux monômiaux sont égaux si et seulement s'ils contiennent les mêmes monômes.

Lemme 3.3.5 (lemme de Dikson)**.**

Un idéal monômial $I = < X^\alpha : \alpha \in A > \subset k[X_1, ..., X_n]$ *peut s'écrire comme* $I =< X^{\alpha(1)}, ..., X^{\alpha(s)} >$ *où* $\alpha(i), ..., \alpha(s) \in A$.

Autrement dit, I *a un nombre fini de générateurs.*

Preuve.

Raisonnons par récurrence sur n.

Si $n = 1$, alors, I est engendré par le monôme X_1^α, avec $\alpha \in A \subset \mathbb{N}^n$.

Posons $\beta = \min A$. Alors $\beta \leqslant \alpha$ pour tout $\alpha \in A$. Donc, X_1^β divise tout générateur X_1^α de I. Par suite, $I =< X_1^\beta >$.

Maintenant, supposons que cette affirmation soit vraie jusqu'au rang $n - 1$.

On écrira comme $X_1, X_2, ..., X_{n-1}, Y$ les variables pour qu'on puisse écrire les monômes dans $k[X_1, ..., X_n]$ comme $X^\alpha Y^m$ où $\alpha = (\alpha_1, ..., \alpha_{n-1}) \in \mathbb{N}^{n-1}$, et $m \in \mathbb{N}$. Supposons que $I \subset k[X_1, ..., X_{n-1}, Y]$ soit un idéal monômiale.

Pour donner un générateur à I, considérons un idéal J de $k[X_1, ..., X_{n-1}]$ engendré par les monômes X^α pour chaque $X^\alpha Y^m \in I$. Puisque J est un idéal monômial de $k[X_1, ..., X_{n-1}]$, donc il existe $\alpha(1), ..., \alpha(s)$ tel que $J =< X^{\alpha(1)}, ..., X^{\alpha(s)} >$, d'après l'hypothèse de récurrence.

Pour chaque $i \in \{1, ..., s\}$, la définition de J nous montre que $X^{\alpha(i)}Y^{m_i} \in I$. Soit $m = \max\{m_i, 1 \leqslant i \leqslant s\}$. Alors, pour chaque $0 \leqslant k \leqslant m-1$, on peut considérer l'idéal $J_k \subset k[X_1, ..., X_{n-1}]$ engendré par les monômes X^β tels que $X^\beta Y^k \in I$. D'après l'hypothèse de récurrence, J_k a un générateur fini.
Soit alors, $J_k =< X^{\alpha_k(1)}, ..., X^{\alpha_k(s_k)} >$.

I est engendré par les monômes :
- $X^{\alpha(1)}Y^m, ..., X^{\alpha(s)}Y^m$ d'après J
- $X^{\alpha_0(1)}, ..., X^{\alpha_0(s_0)}$ d'après J_0
- $X^{\alpha_1(1)}Y, ..., X^{\alpha_1(s_1)}Y$ d'après J_1
- $\vdots$
- $X^{\alpha_{m-1}(1)}Y^{m-1}, ..., X^{\alpha_{m-1}(s_{m-1})}Y^{m-1}$ d'après J_{m-1}

En effet, les monômes de I sont divisibles par un dans la liste précédente pour la preuve, soit $X^\alpha Y^\beta \in I$, si $p \leqslant m-1$, alors, $X^\alpha Y^\beta$ est divisible par certain $X^{\alpha_p(i)}Y^p$ d'après la construction de J_p.

Par suite, d'après le lemme 3.3.3, les monômes ci-dessus engendre un idéal qui a des mêmes monômes que I. Donc, d'après le corollaire 3.3.4, cet idéal est égal à I. □

Définitions 3.3.6.

Soit $I \subset k[X_1, ..., X_n]$ un idéal tel que $I \neq \{0\}$.

1. On notera $\mathrm{LT}(I)$ l'ensemble des termes dominants des éléments de (I).
   D'où $\mathrm{LT}(I) = \{CX^\alpha : \exists f \in I \text{ tel que } \mathrm{LT}(f) = CX^\alpha\}$
2. On notera $< \mathrm{LT}(I) >$ l'idéal engendré par les éléments de $\mathrm{LT}(I)$

Proposition 3.3.7.

Soit $I \subset k[X_1, ..., X_n]$ un idéal.

i) $< LT(I) >$ *est un idéal monômiale*

ii) Il existe $g_1, ..., g_s \in I$ *tel que* $< LT(I) >=< LT(g_1), ..., LT(g_s) >$

Preuve.

i) Le monôme dominant $\mathrm{LM}(g)$ des éléments $g \in I\backslash\{0\}$ engendre l'idéal $< \mathrm{LM}(g) : g \in I\backslash\{0\} >$. Comme $\mathrm{LM}(g)$ et $\mathrm{LT}(g)$ se diffèrent à une constante non nulle, cet idéal est égal à $< \mathrm{LT}(g) : g \in I\backslash\{0\} >$. D'où $< \mathrm{LT}(I) >$ est monômiale.

ii) Comme $\mathrm{LT}(I)$ est engendré par les monômes $\mathrm{LM}(g), g \in I\backslash\{0\}$, le lemme de Dikson dans le paragraphe 3.3.5 nous dit qu'il existe $g_1, ..., g_s \in I$ tel que

$$< \mathrm{LT}(I) >=< \mathrm{LM}(g_1), ..., \mathrm{LM}(g_s) >$$

Comme $\mathrm{LM}(g_i)$ et $\mathrm{LT}(g_i)$ se diffèrent à une constante non nulle, on a par suite

$$< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) >$$

□

Théorème 3.3.8 (théorème de la base de Hilbert)**.**
Tout idéal $I \subset k[X_1, ..., X_n]$ *a un générateur fini. Autrement dit, il existe* $g_1, ..., g_s \in I$ *tel que* $I =< g_1, ..., g_s >$.

Preuve.
Si $I = \{0\}$, la preuve est évidente.
Supposons que $I \neq \{0\}$. Alors le générateur $\{g_1, ..., g_s\}$ pour I peut être construit comme suit :

D'après la proposition 3.3.7, il existe $g_1, ..., g_s \in I$ tel que
$< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) >$. Il est claire que $< g_1, ..., g_s > \subseteq I$ car $g_i \in I$, pour tout $i \in \{1, ..., s\}$.

De plus, prenons un polynôme f quelconque qui est élément de I. Si nous appliquons l'algorithme de division du paragraphe 3.2.1, pour faire la division de f par $\{g_1, ..., g_s\}$, on a

$$f = a_s g_1 + ... + a_s g_s + r$$

où aucun terme de r n'est divisible par l'un des $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_s)$. Par suite,

$$r = f - a_1 g_1 - ... - a_s g_s$$

Supposons que $r \neq 0$. Alors

$$\mathrm{LT}(r) \in \mathrm{LT}(I) =< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) >$$

car $r \in I$ d'après l'égalité précédente. Ainsi, d'après le lemme 3.3.2, $\mathrm{LT}(r)$ est divisible par un certain $\mathrm{LT}(g_i) \quad (1 \leqslant i \leqslant s)$ qui contredit la définition d'un reste (cf. paragraphe 3.2.1).
Donc $r = 0$ et $f \in < g_1, ..., g_s >$. D'où $I \subseteq < g_1, ..., g_s >$ et cela complète la preuve.

□

3.4 Base de Gröbner

Définition 3.4.1.

Fixons un ordre monômial. Un sous-ensemble fini $G = \{g_1, ..., g_s\}$ d'un idéal I est dit *base de Gröbner* (ou base standard) si :

$$< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) >=< \mathrm{LT}(I) >$$

Corollaire 3.4.2.

Fixons un ordre monômial.
Alors tout idéal $I \subset k[X_1, ..., X_n]$ tel que $I \neq \{0\}$ a une base de Gröbner. De plus, toute base de Gröbner d'un idéal I est aussi une base pour I.

Preuve.

Prenons un idéal non nul. Alors,l'ensemble $G = \{g_1, ..., g_s\}$ construit dans la preuve du théorème de la base d'Hilbert est une base de Gröbner de I (en appliquant tout simplement la définition).

Pour la seconde partie du corollaire, $G = \{g_1, ..., g_s\}$ est une base de Gröbner de I si $< \mathrm{LT}(I) =< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) >$. Alors, $I =< g_1, ..., g_s >$ d'après les arguments avancés dans la preuve du théorème 3.3.8. □

3.4.1 Propriété de la base de Gröbner

Proposition 3.4.3.

Soit $G = \{g_1, ..., g_s\}$ une base de Gröbner d'un idéal $I \subset k[X_1, ..., X_n]$ et soit $f \in k[X_1, ..., X_n]$. Alors il y a un unique $r \in k[X_1, ..., X_n]$ tel que :

i) Aucun terme de r n'est divisible par un des $LT(g_1), ..., LT(g_s)$

ii) Il existe $g \in I$ tel que $f = g + r$

En particulier, r est le reste de la division de f par G sans tenir compte le rang des éléments de G dans l'application de l'algorithme de division.

Preuve.

L'algorithme de division donne : $f = a_1 g_1 + ... + a_t g_t + r$ où r satisfait i).
Comme $g = a_1 g_1 + ... + a_t g_t$, $g \in I$.

Pour démontrer l'unicité de r, supposons que $f = g + r = g' + r'$ qui vérifient i) et ii). Alors $r - r' = g' - g \in I$ avec $r \neq r'$. Donc

$$\mathrm{LT}(r - r') \in < \mathrm{LT}(I) >=< \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) > .$$

Cela est impossible car r et r' vérifient i). D'où $r - r' = 0$ et $r = r'$. □

Remarques 3.4.4.

– Le reste r est souvent appelé "forme normale" de f.

– La base de Gröbner peut être caractérisée par l'unicité du reste.

Corollaire 3.4.5.

Soit $G = \{g_1, ..., g_s\}$ une base de Gröbner pour un idéal $I \subset k[X_1, ..., X_n]$ et soit $f \in k[X_1, ..., X_n]$.

Alors, $f \in I$ si et seulement si le reste de la division de f par G est zéro.

Preuve.

Si le reste est nul, alors on observe clairement que $f \in I$.

Inversement, soit $f \in I$, alors $f = f+0$ satisfait les deux conditions de la proposition 3.4.3. Par suite, 0 est le reste de la division de f par G. □

Notation.

On notera $\overline{f}^F$ le reste de la division de f par le $s-$uplet $F = \{f_1, ..., f_s\}$.

Exemple 3.4.6.

Si $F = \{X^2Y - Y^2; X^4Y^2 - Y^2\}$ et en considérant $\leqslant_{\text{lex}}$, on a $\overline{X^5Y}^F = XY^3$

Définition 3.4.7.

Soient $f, g \in k[X_1, ..., X_n]$ deux polynômes non nuls.

i) Si multideg$(f) = \alpha$ et multideg$(g) = \beta$, alors posons $\gamma = (\gamma, ..., \gamma_n)$ où $\gamma_i = \max(\alpha_i, \beta_i)$ pour tout $i \in \{1, .., n\}$. Nous notons par X^γ le plus petit commun multiple de LM(f) et LM(g), c'est-à-dire

$$X^\gamma = \text{ppcm}(\text{LM}(f); \text{LM}(g))$$

ii) le *$S-$polynôme* de f et g est la combinaison :

$$S(f; g) = \frac{X^\gamma}{\text{LT}(f)} f - \frac{X^\gamma}{\text{LT}(g)} g$$

Exemple 3.4.8.

Soient $f = X^3Y^2 - X^2Y^3 + X$ et $g = 3X^4Y + Y^2$ dans $\mathbb{R}[X, Y]$.

Considérons l'ordre grlex.

Alors $\gamma = (\gamma_1, \gamma_2)$ avec $\gamma_1 = \max(3;4) = 4$; $\gamma_2 = \max(2;1) = 2$

Par suite $\gamma = (4;2)$

$$\begin{aligned} S(f;g) &= \tfrac{X^4Y^2}{X^3Y^2}f - \tfrac{X^4Y^2}{3X^4Y}g = Xf - \tfrac{1}{3}Yg \\ &= X(X^3Y^2 - X^2Y^3 + X) - \tfrac{1}{3}Y(3X^4Y + Y^2) \\ S(f;g) &= -X^2Y^3 + X^2 - \tfrac{1}{3}Y^3 \end{aligned}$$

Lemme 3.4.9.

Supposons que nous avons la somme $\sum_{i=1}^{s} c_i f_i$, *où* $c_i \in k$ *et multideg*$(f_i) = \delta$ *avec* $\delta \in \mathbb{N}^n$ $(1 \leqslant i \leqslant s)$.

Si multideg$(\sum_{i=1}^{s} c_i f_i) < \delta$, *alors* $\sum_{i=1}^{s} c_i f_i$ *est un combinaison linéaire à coefficient dans* k *des S-polynômes* $S(f_j; f_k)$ *pour* $j, k \in \{1, ..., s\}$.

De plus, pour chaque $S(f_j; f_k)$, *on a multideg*$(S(f_j; f_k)) < \delta$.

Preuve.

Soit $d_i = \mathrm{LC}(f_i)$. On a $c_i d_i = \mathrm{LC}(c_i f_i)$. Comme multideg$(f_i) = \delta$ multideg$(c_i f_i = \delta)$, et comme de plus multideg $\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$,

$\sum_{i=1}^{s} c_i d_i = 0$

Posons $p_i = \frac{f_i}{d_i}$, on a

$$\mathrm{LT}(f_i) = d_i X^\delta \text{ qui implique } \mathrm{ppcm}(\mathrm{LM}(f_i); \mathrm{LM}(f_k)) = X^\delta$$

donc

$$\begin{aligned} S(f;g) &= \tfrac{X^\delta}{\mathrm{LT}(f_j)}f_j - \tfrac{X^\delta}{\mathrm{LT}(f_k)}f_k \\ &= \tfrac{X^\delta}{d_j X^\delta}f_j - \tfrac{X^\delta}{d_k X^\delta}f_k \\ &= \tfrac{1}{d_j}f_j - \tfrac{1}{d_k}f_k \\ S(f_j; f_k) &= p_j - p_k \qquad (1) \end{aligned}$$

En utilisant l'équation $\sum_{i=1}^{s} c_i d_i = 0$, on a :

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i = & \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 p_1 + c_2 d_2 p_2 + c_3 d_3 p_3 + c_4 d_4 p_4 + c_5 d_5 p_5 + ... + c_s d_s p_s \\
= & \ c_1 d_1 p_1 - c_1 d_1 p_2 + c_1 d_1 p_2 + c_2 d_2 p_2 + c_3 d_3 p_3 + c_4 d_4 p_4 + c_5 d_5 p_5 \\
& + ... + c_s d_s p_s \\
= & \ c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + (c_1 d_1 + c_2 d_2 + c_3 d_3) p_3 \\
& + c_4 d_4 p_4 + c_5 d_5 p_5 + ... + c_s d_s p_s \\
= & \ c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + (c_1 d_1 + c_2 d_2 + c_3 d_3)(p_3 - p_4) \\
& + (c_1 d_1 + c_2 d_2 + c_3 d_3) p_4 + ... + c_s d_s p_s \\
= & \sum_{i=1}^{s-1} \left[\sum_{j=1}^{i} c_j d_j \right] [p_i - p_{i+1}] + 0 \\
= & \sum_{i=1}^{s-1} \left[\sum_{j=1}^{i} c_j d_j \right] S(f_i; f_{i+1})
\end{aligned}$$

De plus, comme

- $\text{multideg}(p_i) = \text{multideg}(p_k) = \delta$
- $\text{LC}(p_i) = \text{LC}(p_k) = 1$

$\text{multideg}(p_i - p_k) < \delta$

D'après l'équation (1), on a

$$\text{multideg}(S(f_i; f_k)) < \delta$$

□

Théorème 3.4.10.

Soit I un idéal de $k[X_1, ..., X_n]$.

Alors, une base $G = \{g_1, ..., g_t\}$ de I est une base de Gröbner pour I si et seulement si, pour tout pair $i \neq j$, le reste de la division de $S(g_i; g_j)$ par G est zéro (sans tenir compte l'ordre).

Preuve.

Si G est une base de Gröbner ; alors comme $S(g_i; g_j) \in I$, le reste de la division par G est zéro d'après le corollaire 3.4.5.

Réciproquement, soit $f \in I$, avec $f \neq 0$ et $I =< g_1, ..., g_t >$. Donc il existe $h_1, ..., h_t \in k[X_1, ..., X_n]$ tel que $f = \sum_{i=1}^{t} h_i g_i$ (2)

Alors $\text{multideg}(f) \leqslant \max(\text{multideg}(h_i g_i))$ (3)

Si on a $\text{multideg}(f) < \max(\text{multideg}(h_i g_i))$, alors il aurait quelques annulation au niveau des certains $h_i g_i$. En utilisant le lemme 3.4.9, on peut les écrire comme combinaison linéaire des S-polynômes. D'après notre hypothèse, on peut remplacer les S-polynômes par des expressions en fonction des quelques g_j. En continuant cette procédure, nous pourrons avoir une autre forme de l'expression (2) où on aura une égalité dans l'équation (3).

Cela nous permet de dire que $\text{multideg}(f) = \text{multideg}(h_i g_i)$ pour quelque i. Par suite $\text{LT}(f)$ est divisible par $\text{LT}(g_i)$ et $\text{LT}(f) \in < \text{LT}(g_1), ..., \text{LT}(g_t) >$. □

Exemple 3.4.11.

Dans cet exemple, nous considérons l'ordre $\leqslant_{\text{lex}}$.

Prenons $\mathbb{R}[X, Y]$. Soient

$f_1 = X^3 - 2XY$, donc

$$\text{LT}(f_1) = X^3$$

et $\text{multideg}(f_1) = (3; 0)$

$f_2 = X^2Y - 2Y^2 + X$, donc

$$\text{LT}(f_2) = X^2Y$$

et $\text{multideg}(f_2) = (2; 1)$

Posons $I =< f_1; f_2 >$ et $F = \{f_1; f_2\}$

On a

$$\gamma = \text{ppcm}(\text{multideg}(f_1); \text{multideg}(f_2)) = (3; 1)$$

et

$$S(f_1; f_2) = \frac{X^3Y}{X^3} f_1 - \frac{X^3Y}{X^2Y} f_2 = Y f_1 - X f_2 = -X^2$$

Donc $\overline{S(f_1; f_2)}^F = -X^2$ et F n'est pas une base de Gröbner de I.

Dans ce cas, il faut prendre $f_3 = -X^2$

3.5 Une autre conception de base de Gröbner

Considérons deux polynômes p et q tels que $p, q \in k[X_1, .., X_n]$.
Supposons de plus que q possède un terme αt divisible par $\mathrm{LM}(p)$.

Posons ainsi $t = u\mathrm{LM}(p)$ et $q' = q - \dfrac{\alpha}{\mathrm{LC}(p)}up$

$$= q - \frac{\alpha t}{\mathrm{LT}(p)}p$$

On remarque que q' ne contient plus le monôme t et que $q - q'$ ne contient que des termes strictement inférieurs à t.

Définition 3.5.1.
Le polynôme q' défini ci-dessus est dit polynôme obtenu à partir de q par *réduction modulo* p et on le notera $q \equiv q'[p]$.

Maintenant, s'il existe $q_1, ..., q_k \in P$ tels que $q \equiv q_1[p_1], q_1 \equiv q_2[p_2], ..., q_k \equiv q'[p_k]$ ou directement $q = q'$; on dira que q' est une *réduction de q modulo P* et qu'on notera :

$$q \equiv q'[P]$$

Dans le cas contraire, on dira que q est *irreductible modulo P*.
Enfin, on dira que q' est une *réduite de q modulo P* si $q \equiv q'[P]$ et si de plus, q' est irreductible modulo P. On notera dans ce cas $q \equiv q'[P^*]$.

Lemme 3.5.2.
Soit $P \subset k[X_1, ..., X_n]; p, q, r \in k[X_1, ..., X_n]$ tel qu'il existe $p_i \in P$ vérifiant $(p-q) \equiv r[p_i]$.
Alors, il existe $\tilde{p}$ et $\tilde{q}$ tel que $p \equiv \tilde{p}[p_i]$, $q \equiv \tilde{q}[p_i]$ et $r = \tilde{p} - \tilde{q}$.

Preuve.
Comme $p - q \equiv r[p_i]$, $\quad r = p - q - \dfrac{\alpha t}{\mathrm{LT}(p_i)}p_i$.

Notons par β le coefficient de t dans p et γ celui de t dans q. Par suite, $\beta - \gamma = \alpha$, et comme $\alpha \neq 0$, l'un au moins de ces deux coefficients est non nul. Alors, en suivant

la construction dans l'introduction, posons

$$u = \frac{t}{\mathrm{LM}(p_i)}; \qquad \tilde{p} = p - \frac{\beta}{\mathrm{LC}(p_i)} u p_i; \qquad \tilde{q} = q - \frac{\gamma}{\mathrm{LC}(p_i)} u p_i$$

Ainsi,

$$\begin{aligned} \tilde{p} - \tilde{q} &= p - q - (\beta - \gamma)\frac{up_i}{\mathrm{LC}(p_i)} \\ &= p - q - \frac{\alpha u}{\mathrm{LC}(p_i)} p_i \\ &= r \end{aligned}$$

□

Lemme 3.5.3.

Soit $P \subset k[X_1, ..., X_n]; p, q \in k[X_1, ..., X_n]$ tels que $(p - q) \equiv 0[P]$.
Alors, il existe $r \in k[X_1, ..., X_n]$ tel que $p \equiv r[P]$ et $q \equiv r[P]$.

Preuve.

Raisonnons par récurrence sur le nombre N de réductions qui amènent $p - q$ à 0.

Si $N = 0$, alors $p - q = 0$ et on peut prendre $r = p = q$. Supposons alors que cette hypothèse soit vraie pour $N = k - 1 \quad (k \in \mathbb{N}^*)$. Pour $N = k$, on a :

$$p - q \equiv h_0[p_1]; h_0 \equiv h_1[p_2]; ...; h_{k-2} \equiv 0[p_k]$$

où les $h_i \in P$ $(0 \leqslant 1 \leqslant k)$.

Si nous considérons la première réduction $p - q \equiv h_0[p_1]$, on peut dire d'après le lemme précédent qu'il existe $\tilde{p}$ et $\tilde{q}$:

$$(*) \qquad p \equiv \tilde{p}[P] \text{ et } q \equiv \tilde{q}[P] \text{ et que } h_0 = \tilde{p} - \tilde{q}$$

Or il faut $k - 1$ réductions pour ramener $h_0 = \tilde{p} - \tilde{q}$ à 0 et l'hypothèse de récurrence nous assure que $\tilde{p}$ et $\tilde{q}$ ont une réduction commune. Il en est donc de même de p et q d'après la relation (*). □

Lemme 3.5.4.

Soit $r \in k[X_1, ..., X_n]$. Si $p \equiv p'[r]$, alors pour tout polynôme $q \in k[X_1, ..., X_n]$, les polynômes $p + q$ et $p' + q$ ont une réduction commune.

Preuve.

Comme $p \equiv p'[r]$ alors $p' = p - \dfrac{\alpha u}{\mathrm{LC}(r)}r$ avec $t = u\mathrm{LM}(r)$. Soient de plus, $q \in k[X_1, ..., X_n]$; β le coefficient de t dans q. Ainsi, il est claire que β est le coefficient de t dans $p' + q$.

Par ailleurs, le coefficient de t dans $p + q$ est $\alpha + \beta$.

Posons maintenant :

$$s_1 = p + q - \frac{(\alpha + \beta)u}{\mathrm{LC}(r)}r \text{ et } s_2 = p' + q - \frac{\beta u}{\mathrm{LC}(r)}r$$

Donc

$$(p + q) \equiv s_1[r] \text{ et } (p' + q) \equiv s_2[r]$$

Or $s_1 - s_2 = p + q - \dfrac{(\alpha + \beta)u}{\mathrm{LC}(r)}r - p' - q + \dfrac{\beta u}{\mathrm{LC}(r)}r = (p - p') - \dfrac{\alpha u}{\mathrm{LC}(r)}r = 0$

Donc $s_1 = s_2$ est une réduction commune à $(p + q)$ et $p' + q$. □

Définition 3.5.5.

Soit $G = \{g_1, ..., g_k\} \subset k[X_1, ..., X_n]$ et $I =< g_1, ..., g_k >$. On dit que G est une *base de Gröbner* de I si pour tout $p \in k[X_1, ..., X_n]$, $p \in I$, $p \equiv 0[G^*]$.

3.6 Application

Résolubilité d'un système d'équations

Soit

$$(S)\begin{cases} p_1(X_1, ..., X_n) = 0 \\ \vdots \\ p_r(X_1, ..., X_n) = 0 \end{cases}$$

un système d'équations polynômiales et soit I un idéal de $k[X_1, ..., X_n]$ tel que $I =< p_1, ..., p_r >$.

Soit G une base de Gröbner de I.

Théorème 3.6.1 (Théorème des zéros de Hilbert : Nullstellensatz)**.**
Ce système (S) *a des solutions dans la clôture algébrique de* k *si et seulement si* $1 \notin I$*.*

Preuve.
cf ([Yge01]. p.7). □

Théorème 3.6.2.
Soit I *l'idéal de* $k[X_1, ..., X_n]$ *tel que* $I =< p_1, ..., p_r >$ *et* G *une base de Gröbner de cet idéal. Alors, le système* (S) *a des solutions si et seulement si* $1 \notin G$*.*

Preuve.
Il suffit d'appliquer le théorème 3.6.1 et de remarquer que 1 appartenant à I si et seulement si 0 est la réduite de 1 modulo G ; c'est-à-dire 1 est un élément de G.

Ce théorème est ainsi capital pour connaître si un système admet des solutions ou non, car pour cela, il suffit de construire une base de Gröbner de l'idéal I, et de tester ensuite l'appartenance de 1 à cette base. □

Nombre de solutions d'un système d'équations polynômiales

Théorème 3.6.3.
Soit I *un idéal de* $k[X_1, ..., X_n]$ *et* G *une base de Gröbner de* I*. Notons par* T_0 *l'ensemble des termes qui sont irreductibles modulo* G *et soit* π *la projection canonique de* $k[X_1, ..., X_n]$ *dans* $k[X_1, ..., X_n]/I$*. Alors* $U = \{\pi(t))/t \in T_0\}$ *est une base* $k[X_1, ..., X_n]/I$*.*

Preuve.
Soit $\overline{p} \in k[X_1, ..., X_n]/I$ l'élément représentatif de sa classe. On sait que p est irréductible modulo G, donc combinaison linéaire d'éléments de T_0. Alors, U est une famille génératrice du quotient.

De plus, soit $(\alpha_t)_{t\in T_0} \subset k$ telle que $\sum_{t\in T_0} \alpha_t \pi(t) = 0$, on a

$$\sum_{t\in T_0} \alpha_t t \in I \text{ et donc } \sum_{t\in T_0} \alpha_t t \equiv 0[G^*]$$

Donc, nécessairement $\sum_{t\in T_0} \alpha_t t = 0$ car ce polynôme est irréductible modulo G.
On a donc pour tout $t \in T_0,\ \alpha_t = 0$. Ainsi la famille est également libre. □

Lemme 3.6.4.

Soit

$$(S)\begin{cases} p_1(X_1, ..., X_n) = 0 \\ \vdots \\ p_k(X_1, ..., X_n) = 0 \end{cases}$$

Alors (S) a un nombre fini de solutions si et seulement si T_0 est fini.

Preuve.

Soit I un idéal de $k[X_1, ..., X_n]$ engendré par $p_1, ..., p_k$. Désignons par V l'ensemble des solutions de (S). V est un ensemble fini si et seulement si $k[X_1, ..., X_n]/I$ est de dimension finie. Mais si G est une base de Gröbner de I, on a vu dans le théorème 3.6.3 que $U = \{\pi(t))/t \in T_0\}$ est une base de $k[X_1, ..., X_n]/I$. On en déduit que (S) a un nombre fini de solutions si et seulement si T_0 est fini. □

Théorème 3.6.5.

Soient $I =< p_1, ..., p_k >$, G une base de Gröbner de I.
Alors le système (S) a un nombre fini de solutions si et seulement si pour tout $i \in \{1, .., n.\}$, il existe $m_i \in \mathbb{N}$ tel que $X_i^{m_i} \in LM(G)$.

Preuve.

Supposons que pour tout $i \in \{1, .., n.\}$, il existe $m_i \in \mathbb{N}$ tel que
$X_i^{m_i} \in \mathrm{LM}(G)$. Alors tout monôme irréductible doit être de la forme

$$l = X_1^{k_1} ... X_n^{k_n} \text{ avec } k_i < m_i \text{ pour } i \in \{1, .., n\}$$

Donc, il n'y a qu'un nombre fini de possibilités pour les éléments de T_0.

Inversement, si $X_i^m \notin \mathrm{LM}(G)$ pour tout $m \in \mathbb{N}$, alors tous les monômes X_i^m sont irréductibles, et donc des éléments de T_0 qui sont ainsi en nombre infini. $\square$

Chapitre 4

Base de Gröbner et idéal torique

4.1 Idéal torique

Nous allons considérer une variété torique comme une variété algébrique paramétrée par des monômes.

Considérons l'application :

$$\begin{array}{rccc} \Phi : & k[X] & \longrightarrow & k[T, T^{-1}] \\ & X_i & \longmapsto & T^{a_i} \end{array}$$

où $a_i \in \mathbb{Z}^d (1 \leqslant i \leqslant n)$ et $T^{a_i} = T_1^{a_{i1}} T_2^{a_{i2}} ... T_d^{a_{id}}$.

Notons $I = \ker \Phi$ et $V = V(I)$. I est ainsi l'idéal torique et V la variété torique associée à I ([Stu 96]).

Maintenant, définissons l'ensemble :

$$H := \{v \in \mathbb{Z}^n; \sum_{i=1}^{n} v_i a_i = 0\}$$

associé à l'ensemble $\mathcal{A} = \{a_1, ..., a_n\}$ qui est en relation avec I par :

Proposition 4.1.1.
$X^\alpha - X^\beta \in I$ si et seulement si $\alpha - \beta \in H$.

Preuve.

On a $X^\alpha - X^\beta = X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n} - X_1^{\beta_1} X_2^{\beta_2} ... X_n^{\beta_n}$. Donc $X^\alpha - X^\beta \in I$ si et seulement si $T^{a_1\alpha_1} T^{a_2\alpha_2} ... T^{a_n\alpha_n} - T^{a_1\beta_1} T^{a_2\beta_2} ... T^{a_n\beta_n} = 0$;

ou bien $T^{a_1\alpha_1} T^{a_2\alpha_2} ... T^{a_n\alpha_n} = T^{a_1\beta_1} T^{a_2\beta_2} ... T^{a_n\beta_n}$. C'est-à-dire :

$$T^{a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n} = T^{a_1\beta_1 + a_2\beta_2 + ... + a_n\beta_n}$$

Ou encore

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n = a_1\beta_1 + a_2\beta_2 + ... + a_n\beta_n$$

Autrement dit

$$a_1(\alpha_1 - \beta_1) + a_2(\alpha_2 - \beta_2) + ... + a_n(\alpha_n - \beta_n) = 0$$

en d'autre terme

$$\sum_{i=1}^{n} (\alpha - \beta)_i a_i = 0$$

ce qui équivaut à dire que

$$\alpha - \beta \in H$$

□

Corollaire 4.1.2.

Pour un vecteur $v = (v_1, ..., v_n)$, notons par v^+ le vecteur qui a $v_1^+, ..., v_n^+$ comme composantes où $v_i^+ = 0$ si $v_i \leqslant 0$ et $v_i^+ = v_i$ si $v_i > 0$. Pour cela, notons $v^- = (-v)^+$. Alors on a :

$$X^{(\alpha-\beta)^+} - X^{(\alpha-\beta)^-} \in I \text{ si } X^\alpha - X^\beta \in I$$

Preuve.

Supposons que $X^{(\alpha-\beta)^+} - X^{(\alpha-\beta)^-} \notin I$ c'est-à-dire $(\alpha - \beta)^+ - (\alpha - \beta)^- \notin H$. Donc $(\alpha - \beta) \notin H$ et ainsi, $X^\alpha - X^\beta \notin I$ □

Soit H_+ la partie de H définie par :

$$H_+ = \{v \in H \text{ tel que } X^{v^+} > X^{v^-}\}$$

Par exemple, avec l'ordre lexicographique, ce sont des vecteurs dont les premiers coordonnées non nulles sont positives.

Posons $\mathcal{H}$ la famille des polynômes $\{X^{v^+} - X^{v^-} \text{ tel que } v \in H_+\}$. □

Lemme 4.1.3.

Soit p un polynôme non nul de I. Alors on peut trouver une expression de p telle que $LM(p) = X^{\gamma_j} X^{v_j^+}$ pour un certain j.

Preuve.

Soit p un polynôme non nul de I, I est engendré par $\mathcal{H}$ ([Stu 96] lemme 2.5). Ainsi, p peut s'écrire de la forme suivante :

$$p = \sum_{i=1}^{s} a_i X^{\gamma_i} (X^{v_i^+} - X^{v_i^-}) \text{ où } v_i \in H_+, i \in \{1, ..., s\}$$

Raisonnons par récurrence suivant le nombre de termes de p.

Si $s = 1$, le résultat est évident.

Supposons que cette affirmation soit vraie jusqu'au rang $s-1$.
Soit $q = \sum_{i=1}^{s-1} a_i X^{\gamma_i} (X^{v_i^+} - X^{v_i^-})$. D'après notre hypothèse, on a :

$$\mathrm{LM}(q) = X^{\gamma_j} X^{v_j^+} \text{ pour certain } j < s$$

Donc

- si $\mathrm{LM}(q) < X^{\gamma_s} X^{v_s^+}$, alors $\mathrm{LM}(p) = X^{\gamma_s} X^{v_s^+}$
- si $\mathrm{LM}(q) > X^{\gamma_s} X^{v_s^+}$, alors $\mathrm{LM}(p) = \mathrm{LM}(q) = X^{\gamma_j} X^{v_j^+}$
- si $\mathrm{LM}(q) = X^{\gamma_s} X^{v_s^+}$ et $a_s + a_j \neq 0$, alors $\mathrm{LM}(p) = X^{\gamma_s} X^{v_s^+}$

Sinon, p aurait $s-1$ termes et on a le résultat d'après l'hypothèse de récurrence. □

Proposition 4.1.4.

Tous les monômes de $LM(I)$ sont divisibles par un monôme de $LM(\mathcal{H})$.

Preuve.

D'après le lemme 4.1.3, $\mathrm{LM}(p) = X^{\gamma_j} X^{v_j^+}$. Or, $X^{v_j^+} \in \mathrm{LM}(\mathcal{H})$. D'où les monômes de $\mathrm{LM}(I)$ sont divisibles par un monôme de $\mathrm{LM}(\mathcal{H})$. □

Théorème 4.1.5.

Soit $B \subset H_+$ vérifiant pour tout $v \in H_+$, il existe $w \in B$ tel que $w^+ \leqslant v^+$.

Alors la famille $\mathcal{B} = \{X^{v^+} - X^{v^-} \text{ tel que } v \in B\}$ est une base de Gröbner de I.

Preuve.

Il suffit de remarquer que tous les monômes de $\mathrm{LM}(\mathcal{H})$ sont divisibles par un monôme X^{v^+} où $v \in B$. Donc il en est de même pour les monômes de $LM(I)$, et par suite $LM(I) \subseteq LM(\mathcal{B})$. □

4.2 Minimum successif d'un réseau

Nous démontrerons dans ce paragraphe que les minimums succesifs d'un réseau peuvent donner par le biais de la base de Gröbner d'un idéal torique I.

Définition 4.2.1.

Soient $\mathbb{K}$ un corps, $a, w \in \mathbb{N}^n$ et notons :

$$\deg_w X^a = \sum_{i=1}^{n} a_i w_i =< a; w >$$

où $< -; - >$ soit le produit scalaire standard. Dans ce cas, w est dit le *vecteur poids*. Avec ce vecteur poids, nous pouvons construire un *préordre monômial* défini par :

$$X^a \leqslant_w X^b \Leftrightarrow < a; w > \leqslant < a; w >$$

En effet, cette relation ne satisfait pas la condition d'antisymétrique car il existe toujours deux monômes distincts X^a et X^b tels que $X^a \leqslant_w X^b$ et $X^b \leqslant_w X^a$.

Définition 4.2.2.

Pour une norme dans $\mathbb{R}^n$, les *minimaux successifs* $\lambda_1, ..., \lambda_d$ d'un réseau H de dimension d sont définis par :

λ_k : le rayon de la plus petite boule qui contient k vecteurs linéairement indépendants de H

Considérons maintenant la norme dans $\mathbb{R}^n$ définie par

$$||x||_1 = \sum_{i=1}^{n} |x_i|$$

Notons lad(I) (de l'anglais "the ladder of I") l'ensemble des monômes minimaux de LT(I).

Remarque 4.2.3.

Soit $F = \{X^{a_1} - X^{b_1}, ..., X^{a_q} - X^{b_q}\}$

Alors les vecteurs $a - b, a_1 - b_1, ..., a_q - b_q$ ne sont pas indépendants si $\overline{X^a - X^b}^F = 0$ (cf [Pot 94]. Remarque 4).

Théorème 4.2.4.

Supposons que H est homogène (c'est-à-dire : H est dans l'hyperplan $x_1 + ... + x_n = 0$).

Soient $\lambda_1, ..., \lambda_d$ les minimaux successifs de H par la norme $||.||_1$.

Soit B une base de Gröbner de I pour $\leqslant_{(1,...,1)}$.

Alors il existe des vecteurs indépendants $a_1, ..., a_d$ tels que :

$$||a_k||_1 = \lambda_k \ (1 \leqslant k \leqslant d), \ \textit{et} \ X^{a_k^+} - X^{a_k^-} \in B \quad (1 \leqslant k \leqslant d)$$

Preuve.

Il est à noter tout d'abord que si H est homogène, alors I l'est aussi ([Stu 96]).

Pour le binôme $X^{v^+} - X^{v^-} \in I$, nous avons $\deg_w X^{v^+} = \deg_w X^{v^-} = \dfrac{||v||_1}{2}$ où $w = (1, ..., 1)$. Nous déterminerons $a_1, ..., a_d$ par induction.

Pour $k = 1$:

Soit $a \in H$ tel que $||a||_1 = \lambda_1$. Le binôme $X^{a^+} - X^{a^-}$ est dans I, donc il existe un binôme $X^{a_1^+} - X^{a_1^-} \in B$ tel que $X^{a_1^+} \in \mathrm{lad}(I)$, $X^{a_1^+}$ divise X^{a^+} et

$$\deg_w X^{a_1^+} \leqslant \deg_w X^{a^+}.$$

Ainsi, nous avons $||a_1||_1 = \lambda_1$ d'après la définition 4.2.2. D'où $a = a_1$ et

$$X^{a^+} - X^{a^-} \in B.$$

Pour $k > 1$:

Soient $a_1, ..., a_{k-1}$ les vecteurs de H qui donnent les minimaux succesifs $\lambda_1, ..., \lambda_{k-1}$ respectivements. Alors, il existe $a \in H$ tel que $||a||_1 = \lambda_k$ et a est indépendant des $a_1, ..., a_{k-1}$.

Notons B_k la partie de B formée par les binômes $X^{b^+} - X^{b^-}$ où $a_1, .., a_{k-1}, b$ ne sont pas indépendants.

Si le binôme $X^{a^+} - X^{a^-}$ se réduit à 0 par la division par les binômes de B_k, alors $a_1, ..., a_{k-1}, a$ ne sont pas indépendants. Donc en divisant par les binômes de B_k, $X^{a^+} - X^{a^-}$ se réduit à un binôme $X^{a'^+} - X^{a'^-}$ irréductible par B_k avec $||a'||_1 = ||a||_1 = \lambda_k$ car les binômes de B sont homogènes.

Comme $X^{a'^+} - X^{a'^-} \in I$, il existe un binôme $X^{a_k^+} - X^{a_k^-} \in B \backslash B_k$ tel que $X^{a_k^+} \in \mathrm{lad}(I)$, $X^{a_k^+}$ divise $X^{a'^+}$ et $\deg_w(X^{a_k^+}) \leqslant \deg_w(X^{a'^+})$, $||a_k||_1 \leqslant \lambda_k$. Or, $a_1, ..., a_{k-1}, a_k$ sont indépendants (car sinon $X^{a_k^+} - X^{a_k^-}$ serait dans B_k). D'où $||a_k||_1 = \lambda_k$ d'après la définition de λ_k. □

4.3 Le degré d'une base de Gröbner minimale

Dans toute la suite, nous considérons l'ordre lexicographique renversé. Soit $S \subseteq \mathbb{N}^d$ un semi-groupe engendré par l'ensemble :

$$\mathcal{A} = \{e_1; \ldots; e_d; a_1; \ldots; a_c\} \subseteq M_{\alpha,d} = \{(X_1, \ldots, X_d) \in \mathbb{N}^d / X_1 + \cdots + X_d = \alpha\}$$

où $c \geqslant 1; \alpha \geqslant 2; c, \alpha \in \mathbb{N}$ et $e_i = (0; \ldots; 0; \alpha; 0; \ldots; 0)$, $1 \leqslant i \leqslant d$.

Pour un corps $\mathbb{K}$, considérons l'application définie par :

$$\begin{array}{rccl} \varphi : & \mathbb{K}[X_1; \ldots; X_c; Y_1; \ldots; Y_d] & \longrightarrow & \mathbb{K}[S] \equiv \mathbb{K}[T_1^\alpha; \ldots; T_d^\alpha; T^{a_1}; \ldots; T^{a_c}] \subseteq \mathbb{K}[T] \\ & X_i & \longmapsto & T^{a_i} \\ & Y_j & \longmapsto & T_j^\alpha \quad \text{où } i \in \{1; \ldots; c\}, j \in \{1; \ldots; d\} \end{array}$$

Notons $I_\mathcal{A} = \operatorname{Ker} \varphi$ qui est l'idéal torique défini par $\mathcal{A}$.

Dans toute la suite, on prendra :

$$\deg_w X^n = \deg_{(1,\ldots,1)} X^n$$

Remarquons que $I_\mathcal{A}$ a toujours une base de Gröbner minimale constituée par des binômes. Nous voulons borner le degré maximum de cette base.

Soit $r(S)$ le plus petit entier r tel que

$$(r+1)\mathcal{A} = \{e_1; \ldots; e_d\} + r\mathcal{A}.$$

Théorème 4.3.1.

Le degré maximal d'une base de Gröbner minimale de $I_\mathcal{A}$ est majoré par :

$$\max\{r(S) + 1; 2r(S) - 1\} \leqslant \max\{2; 2(\deg \mathbb{K}[S] - c - 1\}$$

Preuve.

Soit $s = \max\{r(S) + 1; 2r(S) - 1\}$ et

$$G = \{X^m Y^n - X^u Y^v \in I_\mathcal{A} / \deg(X^m Y^n) = \deg(X^u Y^v) \leqslant s\}$$

On a d'après ([HS 03]. Théorème 1.1), $r(S) \leqslant \deg \mathbb{K}[S] - c$.

Donc $2r(S)-1 \leqslant 2(\deg \mathbb{K}[S]-c)-1$; et comme $r(S) > 0$, $r(S) \geqslant 1$, et par suite $r(S)+1 \geqslant 2$. On a alors :

$$\deg(G) \leqslant s \leqslant \max\{2; 2(\deg \mathbb{K}[S] - c) - 1\}$$

Donc il suffit de montrer que G est une base de Gröbner de $I_{\mathcal{A}}$.

Soit $b = X^m Y^n - X^u Y^v \in I_{\mathcal{A}}$ tel que $deg(b) > s$ et $\deg(X^m Y^n)$ soit minimal avec

$$LT(g) \not| X^m Y^n \text{ pour tout } g \in G.$$

Si $\deg(X^m) \geqslant r(S)+1$, alors nous pouvons écrire $X^m = X^{m'} X^{m''}$, où $\deg(X^{m'}) = r(S)+1$. Prenons deux entiers m^*, n^* tels que $\deg(X^{m^*}) = r(S)$ et $g := X^{m'} - X^{m^*} X^{n^*} \in I_{\mathcal{A}}$. Alors $g \in G$ et $LT(g) = X^{m'} | X^m Y^n$ qui contredit l'hypothèse. Donc $\deg(X^m) \leqslant r(S)$.

Si $\deg(X^u) \geqslant r(S)+1$, alors prenons u', u'' tels que $X^u Y^v - X^{u'} Y^{u''+v} \in I_{\mathcal{A}}$ et

$$\deg(X^{u'}) = r(S) < \deg(X^u).$$

Donc $X^m Y^n - X^{u'} Y^{u''+v} = (X^m Y^n - X^u Y^v) + (X^u Y^v - X^{u'} Y^{u''+v}) \in I_{\mathcal{A}}$ et $X^m Y^n > X^u Y^v > X^{u'} Y^{u''+v}$. Ainsi en remplaçant $X^u Y^v$ par $X^{u'} Y^{u''+v}$ nous pourrions supposer dès le début que $\deg(X^u) \leqslant r(S)$.

Maintenant, comme $X^m Y^n - X^u Y^v \in I_{\mathcal{A}}$, nous avons :

$$\left(\sum_{i=1}^{c} m_i a_i\right) + \left(\sum_{i=1}^{d} n_i e_i\right) = \left(\sum_{i=1}^{c} u_i a_i\right) + \left(\sum_{i=1}^{d} v_i e_i\right).$$

(cf Proposition 4.1.1)

Comme $\deg(X^m Y^n)$ est minimal, nous pouvons supposer que $X^m Y^n$ et $X^u Y^v$ n'ont pas de variables communes.

Posons : $C = \{i / m_i \neq 0\}$ et $D = \{j / n_j \neq 0\}$.

Alors, l'égalité ci-dessus peut s'écrire comme :

$$\left(\sum_{i \in C} m_i a_i\right) + \left(\sum_{i \in D} n_i e_i\right) = \left(\sum_{i \notin C} u_i a_i\right) + \left(\sum_{i \notin D} v_i e_i\right).$$

Par suite,

$$\left(\sum_{j\in D}\sum_{i\in C} m_i a_{ij}\right) + \left(\sum_{i\in D} n_i\alpha\right) = \sum_{j\in D}\sum_{i\notin C} u_i a_{ij} = \sum_{i\notin C} u_i \sum_{j\in D} a_{ij} \leqslant \sum_{i\notin C} u_i\alpha$$

On en déduit que,

$$\sum_{i\in D} n_i\alpha \leqslant \sum_{i\notin C} u_i\alpha$$

Ainsi,

$$\sum_{i\in D} n_i \leqslant \sum_{i\notin C} u_i.$$

Cela implique que :

$$\sum_{i=1}^{d} n_i = \sum_{i\in D} n_i \leqslant \sum_{i\notin C} u_i = \deg(X^u) \qquad (1)$$

L'égalité sera acquise si et seulement si $m_i a_{ij} = 0$ pour tout $(i,j) \in C \times D$ et $u_i a_{ij} = 0$ pour tout $(i;j)$ tel que $i \notin C$ et $j \notin D$.
Soit $X^m - Y^v \in I_{\mathcal{A}}$ alors on a $\sum_{i\in C} m_i a_i = \sum_{i\notin D} v_i e_i$. Comme $X^m > Y^v$ et $\deg(X^m) \leqslant r(S)$, alors $g := X^m - Y^v \in G$ car $\sum_{i\in C} m_i = \sum_{i\notin D} v_i$. Mais cela est impossible car $LT(g)|X^m Y^n$. Donc, d'après (1) on a :

$$\sum_{i=1}^{d} n_i < \deg(X^u) \leqslant r(S)$$

Car sinon, on aurait

$$\sum_{i\in C} m_i = \sum_{i\notin D} v_i.$$

On a par suite

$$\deg(b) = \deg(X^m) + \sum_{i=1}^{d} n_i < 2r(S).$$

Alors : $\deg(b) \leqslant 2r(S) - 1 \leqslant s$ qui contredit l'hypothèse. D'où le résultat. □

Théorème 4.3.2.

Le degré minimal d'une base de Gröbner minimale de $I_{\mathcal{A}}$ est majoré par :

$$\max\{c; \alpha; c(\alpha-1)-1\} \leqslant c(\alpha-1)$$

Preuve.

Soit $s = \max\{c; \alpha; c(\alpha-1)-1\}$ et considérons l'ensemble

$G = \{X^mY^n - X^uY^v \in I_{\mathcal{A}} / \deg(X^mY^n) = \deg(X^uY^v) \leqslant s\}$

Comme précédemment, supposons que G n'est pas une base de Gröbner de $I_{\mathcal{A}}$.

Soit $b = X^mY^n - X^uY^v \in I_{\mathcal{A}}$ de degré minimal, avec $\deg(b) > s$; et $LT(g) \not| X^mY^n$ pour tout $g \in G$. Comme $\alpha a_i = a_{i1}e_1 + \cdots + a_{id}e_d$; $X_i^\alpha - Y^{a_i} \in G$ pour tout $i \in \{1; \ldots; c\}$ (notons que $X_i^\alpha > Y^{a_i}$). Comme $LT(X_i^\alpha - Y^{a_i}) \not| X^mY^n$ nous pouvons avoir $m_i \leqslant \alpha - 1$ pour tout $i \leqslant c$; car sinon, si $m_i > \alpha$, alors il existe $\beta \in \mathbb{N}^c$ tel que $m_i = \beta_i + \alpha$. Ainsi :

$$X_1^{m_1} \ldots X_i^{m_i} \ldots X_c^{m_c} Y_1^{n_1} \ldots Y_d^{n_d} = X_1^{m_1} \ldots X_i^{\beta_i} \ldots X_c^{m_c} Y_1^{n_1} \ldots Y_d^{n_d} \times X_i^\alpha$$

Et par suite, $X_i^\alpha | X^mY^n$ qui contredit le fait que $X_i^\alpha - Y^{a_i} \in G$.

Si $u_i \geqslant \alpha$, alors :

$$X^mY^n - \frac{X^u}{X_i^\alpha} Y^{v+a_i} = (X^mY^n - X^uY^v) + (X_i^\alpha - Y^{a_i}) \frac{X^u}{X_i^\alpha} Y^v \in I_{\mathcal{A}}$$

qui contredit l'hypothèse car dans ce cas, on aurait $X_i^\alpha | X^uY^v$. Nous pouvons ainsi supposer que $u_i \leqslant \alpha - 1$ pour tout $i \leqslant c$.

En adoptant la même notation que celle de la preuve du théorème 4.3.1, nous pouvons conclure que :

$$\sum_{i \in D} n_i \leqslant \sum_{i \notin C} u_i \leqslant (c - \sharp C)(\alpha - 1); \qquad (3)$$

et que

$$\sum_{i \in D} n_i = (c - \sharp C)(\alpha - 1) \text{ implique } X^m - Y^v \in I_{\mathcal{A}}.$$

Alors on a

$$\deg(X^mY^n) = \left(\sum_{i \in C} m_i\right) + \left(\sum_{i \in D} n_i\right) \leqslant \sharp C(\alpha - 1) + (c - \sharp C)(\alpha - 1) = c(\alpha - 1).$$

Or $\deg(X^mY^n) = \deg(b) \geqslant c(\alpha - 1)$, ainsi nous pouvons avoir $\deg(X^mY^n) = c(\alpha - 1)$. Donc, $\sum_{i \in D} n_i = (c - \sharp C)(\alpha - 1)$ et $m_i = \alpha - 1$ pour tout $i \in C$. De plus nous avons

d'après (3), $X^m - Y^v \in I_{\mathcal{A}}$. Si $C \neq \{1;\ldots;c\}$, alors $\deg(X^m) \leqslant s$ et, $X^m - Y^v \in G$ qui est impossible car on aurait dans ce cas $X^m | LT(b)$. Par suite, $C = \{1;\ldots;c\}$ qui implique $D = \varnothing$ et

$$b = (X_1 \ldots X_c)^{\alpha-1} - Y^v.$$

Soit un vecteur $\mu := (\mu_1;\ldots;\mu_d)$ tel que $\mu = a_1 + \cdots + a_c$. Nous avons :

$$\sum_{i\in C}(\alpha-1)a_i = \sum_{i\notin D} v_i e_i$$

donc,

$$(\alpha-1)\sum_{i\in C} a_i = \sum_{i\notin D} v_i e_i;$$

ainsi,

$$(\alpha-1)\mu = \sum_{i\notin D} v_i e_i.$$

L'égalité ci-dessus nous permet de dire que $\alpha | (\alpha-1)\mu_i$ pour tout $i \in \{1;\ldots;c\}$. Par suite il existe $v_i' \in \mathbb{N}$ tel que $\mu_i = v_i'\alpha$. Ainsi, $g := X_1 \ldots X_c - Y_1^{v_1'} \ldots Y_d^{v_d'} \in I_{\mathcal{A}}$. En effet,

$$\sum_{i\notin D} v_i' e_i = \sum_{i\notin D} \frac{\mu_i}{\alpha} e_i;$$

donc,

$$\sum_{i\notin D} v_i' e_i = \sum_{i\notin D} \mu_i e_i';$$

où $e_i' = (0;\ldots;0;1;0;\ldots;0)$.

Ainsi,

$$\sum_{i\notin D} v_i' e_i = \mu = \sum_{i\in C} a_i;$$

Comme $\deg(X_1 \ldots X_c) = c \leqslant s$, $g \in G$ et

$$LT(g) = X_1 \ldots X_c | LT(b) = (X_1 \ldots X_c)^{\alpha-1}$$

qui contredit l'hypothèse. D'où le résultat. □

Considérons l'idéal $J_{\mathcal{A}} := (X_1 - T^{a_1}, \ldots, X_c - T^{a_c}, Y_1 - T_1^{\alpha}, \ldots, Y_d - T_d^{\alpha}) \subset \mathbb{K}[T, X, Y]$.
$J_{\mathcal{A}}$ est le noyau de :

$$\begin{array}{ccc} \mathbb{K}[T, X, Y] & \longrightarrow & \mathbb{K}[T] \\ T_j & \longmapsto & T_j \\ X_i & \longmapsto & T^{a_i} \\ Y_j & \longmapsto & T_j^{\alpha} \end{array}$$

Proposition 4.3.3.

Le degré maximal d'une base de Gröbner minimale de $J_{\mathcal{A}}$ est majoré par :

$$d(\alpha - 1) + \min\{2r(S); c(\alpha - 1)\}$$

Preuve.

Comme dans les preuves des deux derniers théorèmes, posons :

$$s = d(\alpha - 1) + \min\{2r(S); c(\alpha - 1)\}$$

$$G = \{T^u X^m Y^n - T^{u'} X^{m'} Y^{n'} \in J_{\mathcal{A}} / \deg(T^u X^m Y^n - T^{u'} X^{m'} Y^{n'}) \leqslant s\}.$$

Supposons que G n'est pas une base de Gröbner de $J_{\mathcal{A}}$. Soit b le binôme de $J_{\mathcal{A}}$ défini par $b := T^u X^m Y^n - T^{u'} X^{m'} Y^{n'}$ de degré minimal $deg(b) > s$ tel que $LT(g) \not| T^u X^m Y^n$ pour tout $g \in G$. Comme dans la preuve du théorème 4.3.2, nous avons $T_i^{\alpha} - Y_i \in G$. Alors, nous pouvons supposer que $u_i' \leqslant \alpha - 1$ pour tout $i \leqslant d$.
En utilisant les arguments du théorème 4.3.1, nous pouvons supposer que $\deg(X^m)$ et $\deg(X^{m'})$ sont inférieurs à $r(S)$.
On a $b \in J_{\mathcal{A}}$ si et seulement si :

$$u + \left(\sum_{i \in C} m_i a_i\right) + \left(\sum_{i \in D} n_i e_i\right) = u' + \left(\sum_{i \notin C} m_i' a_i\right) + \left(\sum_{i \notin D} n_i' e_i\right).$$

Alors

$$u_j + \left(\sum_{i \in C} m_i a_{ij}\right) + n_j \alpha = u_j' + \left(\sum_{i \notin C} m_i' a_{ij}\right) + n_j' \alpha \qquad (4)$$

Pour tout $j \leqslant d$ où C et D sont les ensembles qui sont définis dans la preuve du théorème 4.3.1.

Ainsi, en utilisant le raisonnement dans l'équation (1) du théorème 4.3.1, nous avons :

$$\left(\sum_{j\in D} u_j\right) + \sum_{j=1}^{d} n_j \leqslant \left(\sum_{j\in D} u'_j\right) + \deg(X^{m'}) \leqslant \sharp D(\alpha-1) + r(S).$$

Par suite,

$$\left(\sum_{j\in D} u_j\right) + \sum_{j=1}^{d} n_j \leqslant d(\alpha-1) + r(S).$$

En consequence, $\deg(T^u X^m Y^n) \leqslant d(\alpha-1) + 2r(S)$, et analogiquement,

$$\deg(T^{u'} X^{m'} Y^{n'}) \leqslant d(\alpha-1) + 2r(S)$$

et alors : $\deg(b) \leqslant d(\alpha-1) + 2r(S)$.

Maintenant, en appliquant les arguments de la preuve du théorème 4.3.2 à l'équation (4), nous avons :

$$\deg(b) \leqslant d(\alpha-1) + c(\alpha-1).$$

D'où $\deg(b) \leqslant s$ qui contredit l'hypothèse. □

Conclusion

Dans ce travail, nous avons étudié la base de Gröbner des idéaux toriques. Pour cela, nous avons utilisé les propriétés de la base de Gröbner pour déterminer les éléments d'un idéal et pour vérifier l'existence des solutions d'un système d'équation polynomiale. Pour y arriver, nous avons utilisé entre autres le lemme de Dikson et le Nullstellensatz de Hilbert.

L'idée capitale dans cette étude est la particularité de la base de Gröbner des idéaux toriques car grâce à cette base, on peut déterminer les minimaux successifs de Minkowski d'un réseau et de plus, les caractéristiques de cette base nous ont permis de majorer son degré maximal.

Bibliographie

[Ale 02] D. ALESSANDRINI. *Les singularités des polynômes à l'infini et les compactifications toriques*. Thèse de doctorat. UFR SCIENCES. Université d'Angers,(2002), 16-18.

[BG 07] W. BRUNS and J. GUBELADZE. *Polytopes,rings and K-theory*. Springer (2007), 249-279.

[Dan 78] V.I. DANILOV. *The geometry of toric varieties*. Russian Math. Surveys 33 :2 (1978), 97-110.

[FW 05] K. FUKUDA and Ch. WEIBEL. *Computing All Faces of the Minkowski Sum of V-Polytopes*. Swiss National Science Foundation Project 20021-105202, (2005).

[HHS 09] M. HELLUS, L.T. HOA, J. STÜCKRAD. *Gröbner bases of simplicial toric ideals*. arXiv.0910.0583v1 (2009), 1-9.

[HS 03] L.T. HOA. and J. STÜCKRAD. *Castelnuovo-Mumford regularity of simplicial toric rings*. J. Algebra 259 (2003), 127-133.

[Mai 97] V. MAILLOT. *Géométrie d'Arakelov des varieties toriques et fibrés en droites intégrables*. arXiv : alg-geom/9070600 5v2(1997), 7-14.

[Pot 94] L. POTTIER. *Gröbner bases of toric ideals*. Rapport de recherche. N°2224, INRIA (1994).

[Ram 02] I.P. RAMAHAZOSOA. *Anneaux de monoïde et une théorie de Gröbner pour des modules*. Thèse de doctorat. Département de Mathématiques et Informatique. Université d'Antananarivo. Madagascar.(2002), 9-84.

[Sch 95] U. SCHNELL. *Successive minima, Intrinsic Volumes, and lattice determinants*. Discrete Comput Geom 13 (1995), 233-239.

[Sin 07] A. SINE. *Problème de maximalité pour les variétés toriques*. Thèse de doctorat. UFR SCIENCES. Université d'Angers (2007), 4-6.

[Stu 91] B. STURMFELS. *Gröbner bases of toric varieties*. Tùôhoku Math. J. 43 (1991), 249-253.

[Stu 96] B. STURMFELS. *Equations defining toric varieties*. Alg-geom/9610018. (1996),1-12.

[Yge 01] A. YGER. *La diversité des Mathématiques face à un problème de logique*. Laboratoire de Mathématiques pures. Université Bordeaux 1. 33405 Talence, France. (2001), 1-8.

Candidat : RANDRIAMITANTSOA Manitra Sata Harivony
e-mail : manitrasata@gmail.com

Résumé : Nous avons étudié dans ce mémoire la base de Gröbner des idéaux toriques. Nous mettons en relation ces idéaux avec les sous réseaux de $\mathbb{Z}^d$. Nous avons donné ainsi les propriétés particulières de cette base et quelques applications de ces résultats. Pour cela, nous avons utilisé la base de Gröbner des idéaux toriques pour chercher les minimaux successifs de Minkowski, et outre, nous avons donné quelques majorations du degré de ladite base en utilisant l'ordre lexicographique reversé. Toutefois, la recherche des autres applications concernant cette base est encore ouverte actuellement pour les algébristes et les informaticiens.

Mots clés : Modules, variété torique, idéal torique, base de Gröbner, minimaux successifs.

Abstract : We study here Gröbner bases of toric ideals. We connect these ideals with the sub-lattice of $\mathbb{Z}^d$, then deduce properties on their Gröbner bases, and give application of these results. The main contributions of this memoir are a bound on the maximum degree of a minimal Gröbner basis of simplicial toric ideals with respect to the reverse lexicographic order, the fact that they contain Minkowski successive minima of a lattice. However, the others research concerning these applications are interested many mathematician currently.

Key words : module, toric varieties, toric ideals, Gröbner bases, successive minima.

Encadreur : Irrish Parker RAMAHAZOSOA, Maître de Conferences,
Université d'Antananarivo, Faculté des Sciences,
Département de Mathématiques et Informatique.
e-mail : ramahazos@yahoo.fr
Tél : 033 14 905 17