MA^2 2011-2012
M2 Algèbre formelle

1 Introduction

1.1 Référence

• Ideals, varieties and algorithms, D. Cox, J. Little, D. O'Shea, Undergraduate texts in Mathematics, Springer 1997.
• Using algebraic geometry, D. Cox, J. Little, D. O'Shea, Graduate texts in Mathematics, Springer 2005.
• An introduction to Gröbner bases, W. Adams, P. Loustaunaw, Graduate studies in Mathematics 3 AMS, 1994.

2 Division dans l'anneau des polynômes à plusieurs variables

Dans tout ce cours k désigne un corps.

2.1 Polynômes

Soient $x_1, \ldots, x_n$, n variables.

Définition 2.1.1 *Un* **Monôme** *en $x_1, \ldots, x_n$ est un produit de la forme*

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

où $\alpha_i \in \mathbf{N}$, $1 \leq i \leq n$. On note aussi $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, où $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$. Le **degré total** *de x^α est $|\alpha| = \alpha_1 + \cdots + \alpha_n$.*

Remarque 2.1.2 *Si $\alpha = (0, \dots, 0)$, on note $x^\alpha = 1$.*

Exemples 2.1.3 *Pour programmer, nous utiliserons plutôt la notation $x_1 \cdots x_3 = x^{(1,1,1)}$. Pour calculer, nous utiliserons plutôt la notation xyz.*

Définition 2.1.4 *Un* **polynôme** *f en $x_1, \dots, x_n$ à coefficients dans k est une combinaison linéaire finie de monômes :*

$$f = \sum_\alpha a_\alpha x^\alpha$$

où les $a_\alpha \in k$ sont presque tous nuls, i.e. la somme porte sur un ensemble fini de n-uplets $(\alpha_1, \dots, \alpha_n)$; a_α est dit **coefficient** *du monôme x^α dans f. Si $\alpha \neq 0$, $a_\alpha x^\alpha$ est un terme de f. Le degré total de f est le maximum de $|\alpha|$ pour $a_\alpha \neq 0$.*

Définition 2.1.5 *Un polynôme est dit* **homogène** *si tous les monômes qui apparaissent avec un coefficient non nul ont même degré total.*

Exemples 2.1.6 *Le polynôme $4x^3 + 5x^2y - z^3$ est homogène dans $k[x, y, z]$. Le polynôme $4x^3 + 5x^2y - z^6$ n'est pas homogène dans $k[x, y, z]$.*

Définition 2.1.7 *L'addition et la multiplication munissent l'ensemble des polynômes en $x_1, \dots, x_n$ d'une structure d'anneau commutatif intègre noté $k[x_1, \dots, x_n]$.*
Le corps des fractions de $k[x_1, \dots, x_n]$ est noté $k(x_1, \dots, x_n)$ et est appelé **corps des fractions rationnels à n indéterminés** *:*

$$k(x_1, \dots, x_n) = \{f/g, f, g \in k[x_1, \dots, x_n], g \neq 0\}.$$

2.2 Idéaux

Définition 2.2.1 *Soit $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. On note*

$$< f_1, \dots, f_s >= \{p_1 f_1 + \cdots + p_s f_s, p_i \in k[x_1, \dots, x_n], i = 1, \dots, s\}.$$

Exemples 2.2.2 • $< 0 >= \{0\}$,
• $< 1 >= k[x_1, \dots, x_n]$,
• $< x, y >= k[x, y] - k^*$.

Définition 2.2.3 *Soit $I \subset k[x_1, \ldots, x_n]$ un ensemble non vide.*
L'ensemble I est un **idéal** *de $k[x_1, \ldots, x_n]$ si*
a. $\forall f, g \in I, f + g \in I$,
b. $\forall f \in I$, $\forall p \in k[x_1, \ldots, x_n]$, $pf \in I$.

Exemple 2.2.4 *Dans $k[x, y]$, les ensembles suivants sont des idéaux :* $\{0\}, k[x, y], k[x, y] - k^*$.

Lemme 2.2.5 *L'ensemble $< f_1, \ldots, f_s >$ est le plus petit idéal contenant tous les $f_i, 1 \leq i \leq s$.*

PREUVE : C'est un idéal; $f_i \in I$, $1 \leq i \leq s$. Si J est un idéal contenant $(f_i)_{1 \leq i \leq s}$, alors J contient I. ∎

Corollaire 2.2.6 *Soient $I =< f_1, \ldots, f_s >$ et $J =< g_1, \ldots, g_t >$. Alors $I = J$ si et seulement si $f_i \in J$, $1 \leq i \leq s$ et $g_j \in I$, $1 \leq j \leq t$.*

PREUVE : $\Longrightarrow$ Clair.
$\Longleftarrow$ $f_i \in J$, $1 \leq i \leq s$ implique $I \subset J$. ∎

Exemples 2.2.7 • $< x + y, x - y >=< x, y >$,
• $< 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 >=< x^2 - 4, y^2 - 1 >$ *(on écrit* $y^2 - 1 = 1/5(2x^2 + 3y^2 - 11) - 2/5(x^2 - y^2 - 3)$ *et* $x^2 - 4 = 1/5(2x^2 + 3y^2 - 11) + 3/5(x^2 - y^2 - 3)$*, etc...).*

Définition 2.2.8 *Un idéal est dit* **de type fini** *s'il existe un système de générateurs $(f_i)_{1 \leq i \leq s}$ tel que*

$$I =< f_1, \ldots, f_s > .$$

L'un des objectifs de ce cours est de donner une preuve constructiviste du résultat suivant, dit Théorème de la base de Hilbert :

Théorème 2.2.9 *Tout idéal I de $k[x_1, \ldots, x_n]$ est de type fini.*

La preuve sera constructiviste au sens où nous donnerons un algorithme pour construire un système fini de générateurs de I.
Pour commencer nous traitons le cas des anneaux de polynômes en une seule variable. Dans ce cas, c'est l'algorithme d'Euclide qui résout le problème.

2.3 Polynômes en une seule variable

Dans ce paragraphe, $k[x]$ désigne l'anneau des polynômes en une indéterminée.

Définition 2.3.1 *Soit $f \in k[x]$. Si $f \neq 0$, alors $f = a_0x^m + \cdots a_m$, $a_i \in k$ et $a_0 \neq 0$. Ainsi* $\deg f = m$ *et a_0x^m est dit* **terme dominant** *de f et nous le notons $LT(f) = a_0x^m$.*

Exemple 2.3.2 *Pour $f = 2x^3 - 4x + 3$, $LT(f) = 2x^3$.*

Dans $k[x]$, nous avons l'algorithme de division euclidienne :

Proposition 2.3.3 *Soit $g \in k[x]$, g non nul. Pour tout $f \in k[x]$, il existe un unique couple d'éléments $q, r \in k[x]$ tel que $f = qg + r$, avec $r = 0$ ou* $\deg r < \deg g$.

Preuve : L'algorithme d'Euclide s'écrit en pseudo-code :
Entrée : g, f
Sortie : q, r
$q := 0; r := f$
Tant que $r \neq 0$ et que $LT(g)$ divise $LT(r)$ faire
$q := q + LT(r)/LT(g)$
$r := r - (LT(r)/LT(g))g$

En effet, nous avons toujours

$$f := qg + r = (q + LT(r)/LT(g))g + (r - (LT(r)/LT(g))g).$$

L'algorithme s'arrête quand la proposition ($r \neq 0$ et $LT(g)|LT(r)$) est fausse. Donc en sortie d'algorithme, on a $r = 0$ ou $LT(g) \not| LT(r)$, donc $r = 0$ ou $\deg r < \deg g$.
L'algorithme s'arrête effectivement car à chaque étape le degré de r diminue par substitution à $r - (LT(r)/LT(g))g$.
Il y a unicité de l'écriture. En effet si nous avons deux écritures

$$f = qg + r = q'g + r'$$

satisfaisant les hypothèses de la proposition, alors $\deg(r - r') < \deg g$. Si $r \neq r'$ alors $(q - q')g = r'_r$ donc $q - q' \neq 0$ et $\deg r - r' > \deg g$, absurde ! Donc $r = r'$ et, par suite, $q = q'$. ∎

En corollaire, nous obtenons un résultat plus fort que le théorème de la base de Hilbert pour $k[x]$:

Corollaire 2.3.4 *L'anneau $k[x]$ est principal : pour tout idéal I de $k[x]$, il existe $f \in k[x]$ tel que $I =< f >$. De plus f est unique à multiplication par un scalaire non nul de k.*

PREUVE : Soit I un idéal de $k[x]$.
• Si $I = \{0\}$, $I =< 0 >$.
Sinon, il existe $f \in I - \{0\}$ de degré minimum. Alors $< f > \subset I$. Montrons l'inclusion inverse. Soit $g \in I$, écrivons

$$g = qf + r, \quad \text{avec} \quad r = 0 \quad \text{ou} \quad \deg r < \deg f.$$

Comme I est un idéal, g et $qf \in I$ implique $r = g - qf \in I$. Par minimalité du degré de f, on a $r = 0$ et $g \in < f >$. D'où $I =< f >$.
• Si $< f >=< g >$ alors $f = gh$ avec $h \in k[x]$ d'où $\deg f \geq \deg g$. En inversant les rôles de f et g, nous obtenons l'égalité $\deg f = \deg g$, d'où $h \in k^*$. ∎

2.4 Ordres admissibles

Définition 2.4.1 *Un* **ordre admissible** *sur $k[x_1, \ldots, x_n]$ est une relation $>$ sur l'ensemble des monômes x^α de $k[x_1, \ldots, x_n]$ (ou, de façon équivalente sur les exposants $\alpha \in \mathbf{N}^n$) telle que*
a. La relation $>$ est un ordre total.
b. La relation $>$ est compatible avec la multiplication de $k[x_1, \ldots, x_n]$:

$$\text{Si } x^\alpha > x^\beta, \text{ alors } \forall x^\gamma, x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}.$$

c. La relation $>$ est bien ordonnée : tout ensemble non vide de monômes a un élément minimal pour $>$.

Remarque 2.4.2 *a. signifie que tout polynôme peut s'écrire par une liste de monômes croissants ou décroissants.*

b. montre que cet ordre ne change pas par multiplication par un monôme x^α.
c. montre que l'ensemble des monômes inférieurs à un monôme fixé est fini.
Dans le cas où $n = 1$, ce sont précisément les propriétés du degré qui font marcher l'algorithme d'Euclide. Remarquons enfin que le degré est le seul ordre admissible sur les polynômes à une variable. Mais, comme nous allons le voir, il y a plusieurs ordres admissibles sur $k[x_1, \ldots, x_n]$.

Définition 2.4.3 *L'***ordre lexicograpique** *est l'ordre défini de la façon suivante : soit $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$*

$$x^\alpha >_{lex} x^\beta \iff \text{dans } \alpha - \beta \text{ le premier coefficient non nul est } > 0$$

L'ordre lexicographique correspond à l'ordre du dictionnaire.

Exemple 2.4.4 *Dans $k[x, y, z]$, $x^3y^2z > x^2y^6z^{12}$ car $(3, 2, 1) - (2, 6, 12) = (1, -4, -11)$*

Définition 2.4.5 *L'***ordre lexicographique gradué** *est l'ordre défini de la façon suivante : soit $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$*

$$x^\alpha >_{grlex} x^\beta \iff \begin{cases} \sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i \\ ou \\ \sum \alpha_i = \sum \beta_i \text{ et } x^\alpha >_{lex} x^\beta \end{cases}$$

Exemple 2.4.6 *Dans $k[x, y, z]$, $x^2y^6z^{12} >_{grlex} x^3y^2z$.*

Définition 2.4.7 *L'***ordre lexicographique inverse gradué** *est l'ordre défini de la façon suivante : soit $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$*

$$x^\alpha >_{grevlex} x^\beta \iff \begin{cases} |\alpha| > |\beta| \\ ou \\ |\alpha| = |\beta| \text{ et } \alpha - \beta \in \mathbf{Z}^n \\ \text{et le premier coefficient non nul en partant de la droite est } > 0 \end{cases}$$

Exemple 2.4.8 *Dans $k[x, y, z]$, $x^3y^5z^2 >_{grlex} x^2y^7z$ mais $x^2y^7z >_{grevlex} x^3y^5z^2$.*

Lemme 2.4.9 *Les ordres $lex, grlex, grevlex$ sont des ordres admissibles.*

Nous supposons maintenant que $k[x_1, \ldots, x_n]$ est muni d'un ordre admissible noté $>$. Nous préciserons explicitement lequel lorsque cela sera nécessaire.

Définition 2.4.10 *Le* **terme dominant** *de $f = \sum_\alpha c_\alpha x^\alpha$ non nul est $c_\alpha x^\alpha$ où x^α est le plus grand monôme pour l'ordre $>$. Nous notons $LT(f) = LT_>(f) = c_\alpha x^\alpha$.*
Le **coefficient dominant** *est $LC(f) = c_\alpha$.*
Le **monôme dominant** *est $LM(f) = x^\alpha$.*
Le multi-degré de f est multi-degré$(f) := \max\{\alpha \in \mathbf{N}^n, c_\alpha \neq 0\}$.

Remarque 2.4.11 • *Nous trouverons parfois d'autres notations dans la littérature (voir les travaux dirigés).*
• *Le multi-degré de 0, $LT(0), LM(0)$ et $LC(0)$ ne sont pas définis.*
• *$LT(f)$ dépend de l'ordre choisi (voir exemple).*

Exemple 2.4.12 *Soit $f = 3x^3y^2 + x^2yz^3$ dans $\mathbf{Q}[x, y, z]$. Nous avons*

$$LT_{>_{lex}}(f) = 3x^2y^2, \quad LT_{>_{grevlex}}(f) = x^2yz^3.$$

Nous avons enfin le lemme immédiat suivant :

Lemme 2.4.13 *Soit $f, g \in k[x_1, \ldots, x_n]$. Nous avons $LT(f)LT(g) = LT(fg)$.*

2.5 Algorithme de division dans $k[x_1, \ldots, x_n]$

Soit $>$ un ordre admissible de $k[x_1, \ldots, x_n]$ Nous allons définir une division algorithmique dans $k[x_1, \ldots, x_n]$ analogue à la division euclidienne dans $k[x]$.

Proposition 2.5.1 *Soit $F = (f_1, \ldots, f_s)$ un s-uplet ordonné de polynômes de $k[x_1, \ldots, x_n]$. Alors pour tout $f \in k[x_1, \ldots, x_n]$, on peut écrire*

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

où $a_i, r \in k[x_1, \ldots, x_n]$ et
- pour tout $i \in \{1, \ldots, s\}$, $a_i f_i = 0$ ou $LT_>(f) \geq LT_>(a_i f_i)$,
- $r = 0$ ou r est une combinaison linéaire de monômes dont aucun n'est divisible par $LT_>(f_1), \ldots, LT_>(f_s)$.
Le terme r est alors appelé le **reste** *de la division de f par F et est noté $r = \overline{f}^F$.*

PREUVE : Algorithme de division :
Entrée : $f_1, \ldots, f_s, f$
Sortie $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots, a_s := 0; r := 0$
$p := f$
Tant que $p \neq 0$ faire
$i := 1$
division:=faux
Tant que $i \leq s$ et division=faux faire
Si $LT(f_i)$ divise $LT(p)$ alors (on divise p par f_i et on arrête)
$a_i := a_i + LT(p)/LT(f_i)$
$p := p - (LT(p)/LT(f_i))f_i$
division=vrai
sinon $i := i + 1$ (on essaie la variable suivante)

Si division=faux alors (si aucune variable n'a marché, on regarde le coefficient suivant de p et pour cela, on change r et p) $r := r + LT(p)$
$p := p - LT(p)$
(on recommence tant que $p \neq 0$). Dans cet algorithme, p désigne le polynôme intermédiaire des divisions à chaque étape, $a_1, \ldots, a_s$ sont les quotients et r est le reste.
• Montrons qu'à chaque étape, nous avons

$$f = a_1 f_1 + \ldots + a_s f - s + p + r.$$

C'est vrai au début de l'algorithme. Supposons que c'est vrai à une étape de la division alors
- Si $LT(f_i)|LT(p)$, $a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + p - (LT(p)/LT(f_i))f_i$.
- Sinon $p + r = p - LT(p) + r + LT(p)$.
• Lorsque l'algorithme s'arrête, $p = 0$, donc $f = a_1 f_1 + \cdots + a_s f_s + r$.
• Montrons que l'algorithme s'arrête forcément. Pour cela, nous établissons qu'à chaque étape le multidegré de p diminue :
- Si $LT(f_i)|LT(p)$, $p' = p - (LT(p)/LT(f_i))f_i$. Or $LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$.
Donc p et $\frac{LT(p)}{LT(f_i)} f_i$ ont même terme dominant, d'où, multi-degré(p') < multidegré(p).
- Sinon $p' = p - LT(p)$ et multi-degré(p') < multidegré(p).

Ainsi le multi-degré est une fonction entière positive strictement décroissante et l'algorithme se termine.
• Il reste à montrer que $LT(f) \geq LT(a_i f_i)$ si $a_i f_i \neq 0$. Par construction tous les termes de a_i sont de la forme $\frac{LT(p)}{LT(f_i)}$ où p varie en décroissant son terme dominant. On commence à $p = f$, donc $LT(p) \leq LT(f)$. Ainsi à chaque étape $LT(a_i f_i) \leq LT(f)$. ∎

Remarque 2.5.2 *Le logiciel Maple contient cet algorithme dans le package Groebner (voir travaux dirigés).*

Exemples 2.5.3 *Soit $k[x, y]$ muni de l'ordre lexicographique, $f_1 = xy + 1$, $f_2 = y^2 - 1$ et $f = xy^2 - x$.*
• *Si $F = (f_1, f_2)$, alors $xy^2 - x = y(xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$.*
• *Si $F = (f_2, f_1)$, alors $xy^2 - x = x(y^2 - 1) + 0 \cdot (xy + 1) + 0$.*

L'exemple 2.5.3 montre que $\overline{f}^F$ dépend de l'ordre de la famille ordonnée F. La nullité du reste $r = 0$ est une condition nécessaire mais pas suffisante pour établir l'appartenance

$$f \in < f_1, \ldots, f_s >= I.$$

Les bases de Gröbner fournissent un "bon système" de générateurs de I tels que
- la condition $r = 0$ est équivalente à $f \in I$
- l'ordre de la division n'a pas d'importance.

3 Bases de Grobner

Nous fixons un ordre admissible sur $k[x_1, \ldots, x_n]$.

3.1 Idéaux monomiaux

Il y a une classe d'idéaux de $k[x_1, \ldots, x_n]$ pour laquelle il est très facile de résoudre les problèmes liés à la division. Ce sont les idéaux monomiaux :

Définition 3.1.1 *Un idéal $I \subset k[x_1, \ldots, x_n]$ est dit* **monomial**, *s'il existe un ensemble $A \subset \mathbf{N}^n$ (éventuellement infini) tel que*

$$I =< x^\alpha, \alpha \in A >= \{ \sum_{\alpha \in A} h_\alpha x^\alpha, h_\alpha \in k[x_1, \ldots, x_n] \text{ presque tous nuls}$$

Si I est un idéal monomial, l'inclusion $f \in I$ est facile à déterminer. D'abord pour f un monome :

Lemme 3.1.2 *Soit $I =< x^\alpha, \alpha \in A >$ un idéal monomial. Alors $x^\beta \in I$ si et seulement si il existe $\alpha \in A$ tel que $x^\alpha | x^\beta$.*

PREUVE : $\Longleftarrow$ Clair.
$\Longrightarrow$ On écrit $x^\beta = \sum_{i=0}^{s} h_i x^{\alpha(i)}$ avec $\alpha(i) \in A$. On développe h_i en monômes ; x^β apparaît dans au moins l'un d'entre eux. Donc il existe i, avec $\alpha(i) | \beta$. ∎

Lemme 3.1.3 *Soit I un idéal monomial et $f \in k[x_1, \ldots, x_n]$. Nous avons équivalence entre :*
i. $f \in I$,
ii. tous les termes de f appartiennent à I,
iii. f est une combinaison linéaire de monômes de I.

PREUVE : iii.$\Longrightarrow$ ii. $\Longrightarrow$ i. OK.
i.$\Longrightarrow$iii. récurrence avec le lemme 3.1.2. ∎

Pour les idéaux monomiaux, nous avons un résultat du type "Théorème de la base de Hilbert" : tous les idéaux monomiaux sont maximaux.

Théorème 3.1.4 *(Lemme de Dickson)*
Soit $I =< x^\alpha, \alpha \in A >$ un idéal monomial. Alors on peut écrire $I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$ où $\alpha(1), \ldots, \alpha(s) \in A$. En particulier I a une base finie.

PREUVE : Par réccurrence sur le nombre n de variables. Si $A = \emptyset$, OK.
Si $n = 1$, soit $I =< x_1^\alpha, \alpha \in A >$. Posons $\beta = \min\{\alpha \in A\}$ (ici $A \subset \mathbf{N}$). Pour tout $\alpha \in A$, $\alpha \geq \beta$ donc $x_1^\beta | x_1^\alpha$ et $I =< x_1^\beta >$.
Supposons le théorème vrai pour $n - 1 \geq 1$. Nous écrivons les variables $x_1, \ldots, x_{n-1}, y$ et les monômes de $k[x_1, \ldots, x_{n-1}, y]$ sous la forme

$$x^\alpha y^m, \alpha \in \mathbf{N}^{n-1}, m \in \mathbf{N}.$$

Soit $I \subset k[x_1, \ldots, x_{n-1}, y]$ un idéal monomial. Soit $J =< x^\alpha$ tel que $\exists m$ avec $x^\alpha y^m \in I >$ (la projection de I sur $k[x_1, \ldots, x_{n-1}]$). Par hypothèse $J =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$.
Pour tout $1 \leq i \leq s$, il existe m_i avec $x^{\alpha(i)} y^{m_i} \in I$. Soit $m = \max m_i$ et pour $0 \leq \ell \leq m-1$,

$$J_\ell =< x^\beta \text{ tel que } x^\beta y^\ell \in I >=< x^{\alpha_\ell(1)}, \ldots, x^{\alpha_\ell(s_\ell)} > .$$

Nous allons montrer que

$$I =< x^{\alpha_\ell(i)} y^\ell, 0 \leq \ell \leq m-1, 1 \leq i \leq s_\ell, x^{\alpha(i)} y^m, 1 \leq i \leq s > . \quad (1)$$

Montrons que tout monôme de I est divisible par un monôme de la liste ci-dessus. Soit $x^\alpha y^p \in I$. Si $p \geq m$ alors $\exists i$ avec $x^{\alpha(i)} y^m | x^\alpha y^p$. D'où (1).
Montrons que nous pouvons de plus choisir les $(\alpha_\ell(i), \ell)$ et $(\alpha(i), m) \in A$. En effet

$$I =< x^{\beta(1)}, \ldots x^{\beta(s)} >=< x^\alpha, \alpha \in A >$$

Ainsi chaque $\beta(i)$ est divisible par un $\alpha(j)$. Donc $I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$. ∎

Exemple 3.1.5 *Voyons la base que nous obtenons à partir de l'idéal* $I =< x^4y^2, x^3y^4, x^2y^5 >$. *Ainsi,* $J =< x^4, x^3, x^2 >=< x^2 >$. *Nous avons* $x^2y^5 \in I$ *d'où* $m = 5$.

$$J_0 = J_1 = \{0\},\ J_2 =< x^4 >= J_3,\ J_4 =< x^3 >$$

D'où $I =< x^2y^5, x^4y^2, x^4y^3, x^3y^4 >$.

3.2 Théorème de la base d'Hilbert

Définition 3.2.1 *Soit $I \subset k[x_1, \ldots, x_n]$ un idéal non nul.*
i. Nous définisson l'ensemble des termes dominants de I par

$$LT(I) = \{cx^\alpha \text{ s'il existe } f \in I \text{ tel que } LT(f) = cx^\alpha\}$$

ii. Nous notons $< LT(I) >$ l'idéal engendré par les éléments de $LT(I)$.
Pour $I = \{0\}$, nous noterons $LT(I) = \{0\}$.

Exemple 3.2.2 *Soit $I =< f_1, f_2 >$ avec $f_1 = x^3 - 2xy$, $f_2 = X^2y - 2y^2 + x$. Remarquons que $< LT(I) > \neq < LT(f_1), LT(f_2) >$. En effet*

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

Donc $x^2 \in I$ et $x^2 = LT(x^2) \in < LT(I) >$ mais $x^2 \notin < x^3, x^2y >$.

Proposition 3.2.3 *Soit $I \subset k[x_1, \ldots x_n]$ un idéal. Alors*
i. $< LT(I) >$ est un idéal monomial.
ii. $\exists g_1, \ldots, g_s \in I$ tel que $< LT(I) >=< LT(g_1), \ldots, LT(g_s) >$.

PREUVE : i. $J =< LM(g), g \in I - \{0\} >$ est un idéal monomial. Or $LM(g)$ et $LT(g)$ ne diffère que d'une constante non nulle. D'où $J =< LT(g), g \in I - \{0\} >$.
ii. D'après le lemme de Dickson, nous pouvons écrire

$$< LT(I) >=< LM(g_1), \ldots, LM(g_t) >=< LT(g_1), \ldots, LT(g_t) > .$$

■

Théorème 3.2.4 *(de Hilbert) Tout idéal I de $k[x_1, \ldots, x_n]$ est de type fini.*

PREUVE : Si $I = \{0\}$, le résultat est clair.
Sinon, écrivons $LT(I) =< LT(g_1), \ldots, LT(g_s) >$. Montrons que $I =< g_1, \ldots, g_s >$. L'inclusion $< g_1, \ldots, g_s > \subset I$ est claire. Montrons l'inclusion $I \subset < g_1, \ldots, g_s >$.
Soit $f \in I$, écrivons

$$f = a_1 g_1 + \cdots + a_s g_s + r.$$

Supposons $r \neq 0$. Aucun terme de r n'est divisible par $LT(g_i)$. Or $r = f - a_1 g_1 - \cdots - a_s g_s \in I$. Donc $LT(r) \in < LT(I) >$ donc il existe i avec $LT(g_i)$ divise $LT(r)$. Absurde !
Donc $r = 0$ et $f =< g_1, \ldots, g_s >$. ∎

Corollaire 3.2.5 *L'anneau $k[x_1, \ldots, x_n]$ est noethérien : toute suite croissante d'idéaux de $k[x_1, \ldots, x_n]$ est stationnaire.*

PREUVE : Soit $I_1 \subset I_2 \subset \cdots$ une suite croissante d'idéaux. Soit $I = \cup I_n$. Montrons que I est un idéal de $k[x_1, \ldots, x_n]$.
$0 \in I$ car $\forall j$, $O \in I_j$
Si $f, g \in I$ alors $f \in I_i$, $g \in I_j$. Posons $k = \max(i, j)$. Ainsi $f, g \in I_k$ et $f + g \in I_k \subset I$, $af \in I_i \subset I$, $a \in k[x_1, \ldots, x_n]$.
D'après le théorème de Hilbert, nous pouvons écrire $I =< f_1, \ldots, f_s >$. Chaque $f_i \in I_{j_i}$. Posons $\ell = max\{j_i\}$. Ainsi $I \subset I_\ell$. D'où $< f_1, \ldots f_s >= I_\ell = I_{\ell+1} = \cdots = I$. ∎

3.3 Bases de Gröbner

Définition 3.3.1 *Un sous-ensemble fini $G := \{g_1, \ldots, g_s\}$ d'un idéal $I \subset k[x_1, \ldots, x_n]$ est dit* **base de Gröbner** *si*

$$< LT(g_1), \ldots, LT(g_s) >=< LT(I) >$$

De la preuve du théorème de la base de Hilbert, nous déduisons,

Corollaire 3.3.2 *i. Tout idéal $I \subset k[x_1, \ldots, x_n]$ a une base de Gröbner.*
ii. Toute base de Gröbner de I est une base de I

Proposition 3.3.3 *Soit $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de l'idéal I et $f \in k[x_1, \ldots, x_n]$. Alors il existe un unique $r \in k[x_1, \ldots, x_n]$ tel que*
i. aucun terme de r ne soit divisible par $LT(g_1), \ldots, LT(g_r)$,
ii. il existe $g \in I$ avec $f = g + r$.
En particulier, $r = \overline{f}^G$ est le reste de la division de f par G indépendamment de l'ordre des g_i en utilisant l'algorithme de division.

PREUVE : L'existence de r satisfaisant i. et ii. est assurée l'algorithme de division. Son unicité résulte du calcul suivant : soit $f = g + r = g' + r'$ sont deux écritures satisfaisant les hypothèses i. et ii. Alors $r - r' = g' - g \in I$. Si $r \neq r'$, alors $LT(r - r') \in < LT(I) > = < LT(g_1), \ldots, LT(g_s) >$. Donc il existe i avec $LT(g_i)$ divise $LT(r - r')$ ce qui est exclu ! Donc $r = r'$ et $g = g'$. ∎

Remarque 3.3.4 *En fait les propriétés de la proposition 3.3.3 caractérisent les bases de Gröbner. Voir Becke et Weispfenning (1993).*

Corollaire 3.3.5 *Si G est une base de Gröbner de I. Alors $f \in I$ si et seulement si le reste de f par G est nul.*

3.4 Critère de Buchberger

Il s'agit à présent de reconnaître les bases de Gröbner. Pour cela, commençons par introduire une nouvelle opération sur les polynômes.

Définition 3.4.1 *Soit $f, g \in k[x_1, \ldots, x_n]$ non nuls. Soit $LT(f) = cx^\alpha$ et $LT(g) = dx^\beta$, $c, d \in k$. Notons $\gamma = (\gamma_1, \ldots, \gamma_n)$ avec $\gamma_i = \max(\alpha_i, \beta_i)$, $1 \leq i \leq n$ (autrement dit x^γ est le plus commun multiple de x^α et x^β). Alors le* **S-polynôme** *de f et g est le polynôme*

$$S(f, g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g.$$

Remarque 3.4.2 *Nous avons clairement $S(f, g) \in < F, g >$, $\overline{S(f, g)}^{\{f,g\}} \in < f, g >$. L'opération $S(f, g)$ permet de tuer les coefficients dominants, de définir d'autres éléments de $< f, g >$ et, comme nous le verrons, de construire des éléments des bases de Gröbner.*

Exemples 3.4.3 • *Soit* $f = x^5y + x^2 + 1$, $g = 2x^3y^2 + xy$ *dans* $\mathbf{Q}[x, y]$ *avec* $>_{lex}$. *Ainsi* $x^\gamma = x^5y^2$ *et*

$$S(f, g) = yf - 1/2x^2g = x^2y + y - 1/2x^3y$$

• *Soit* $f = x^3y - 2x^2y^2 + x$, $g = 3x^4 - y$ *dans* $\mathbf{Q}[x, y]$ *avec* $>_{lex}$. *Ainsi* $x^\gamma = x^4y$ *et*

$$S(f, g) = xf - Y/3g = -2x^3y^2 + x^2 + y^2/3$$

$$\overline{S(f, g)}^{\{f,g\}} = -4x^2y^3 + x^2 + 2xy + y^2/3$$

En particulier $LT(\overline{S(f, g)}^{\{f,g\}}) = -4x^2y^3 \in LT(< f, g >)$ *n'est pas divisible par* $LT(f)$, $LT(g)$. *Donc* $LT(\overline{S(f, g)}^{\{f,g\}}) \notin < LT(f), LT(g) >$.

Lemme 3.4.4 *Soit* $f = \sum_{i=1}^{s} c_i f_i$, $c_i \in k$, $LM(f_i) = x^\delta$, $i = 1, \ldots, s$. *Si* $LM(f) < \delta$ *alors* f *est une combinaison linéaire à coefficients dans* k *des S-polynômes* $(S(f_j, f_k))_{1 \leq j < k \leq s}$. *De plus chaque* $LM(S(f_j, f_k)) < \delta$.

PREUVE : Soit $d_i = LC(f_i)$. Comme $LT(f) < \delta$, $\sum_{i=1}^{s} c_i d_i = 0$. Soit $p_i = f_i/d_i$, ainsi $LT(p_i) = 1$ et

$$f = \sum c_i d_i p_i = c_1 d_1(p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_t) + (c_1 d_1 + \cdots + c_s d_s)$$

Or $LT(f_i) = d_i x^\delta$. Donc le plus petit commun multiplde de f_j et f_k est x^δ et

$$S(f_j, f_k) = \frac{x^\delta}{LT(f_j)} f_j - \frac{x^\delta}{LT(f_k)} f_k = p_j - p_k$$

Donc

$$f = c_1 d_1 S(f_1, f_2) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s)$$

et $LM(p_j) = LM(p_k) = x^\delta$ d'où $LC(S(f_j, f_k)) < \delta$. ∎

Proposition 3.4.5 *(Critère de Buchberger)*
Soit $I \subset k[x_1, \ldots, x_n]$ un idéal. Soit $G = \{g_1, \ldots, g_t\}$ une base de I. Alors G est une base de Gröbner si et seulement si pour tout $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$.

PREUVE : $\Longrightarrow$ Si G est une base de Gröbner, comme $S(g_i, g_j) \in I$, nous avons $\overline{S(g_i, g_j)}^G = 0$.
$\Longleftarrow$ Soit $f \in I$. Nous allons montrer que $LT(f) \in < LT(g_1), \ldots, LT(g_t) >$. Écrivons $f = \sum_{i=1}^{t} h_i g_i$, $m(i)$ =multidegré$(h_i g_i)$ et $\delta = \max(m(1), \ldots, m(t))$. Alors multidegré$(f) \leq \delta$. Prenons $f \in I$ tel que δ est minimal.
Si multidegré$(f) = \delta$, alors $LT(f) \in < LT(g_1), \ldots, LT(g_t) >$. En effet il existe i tel que multidegré(f) =multidegré(g_i). Donc $LT(g_i) | LT(f)$.
Si multidegré$(f) < \delta$. Isolons le terme de multidegré δ :

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i$$

Le polynôme f et les deux dernières sommes sont de multidegré strictement inférieur à δ. Donc $\sum_{m(i)=\delta} LT(h_i) g_i$ est de multidegré strictement inférieur à δ. En appliquant le lemme 3.4.4, nous avons

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i = \sum c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k).$$

Or $\overline{S(g_j, g_k)}^G = 0$, donc $S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i$. L'algorithme de division montre que multidegré $(a_{ijk} g_i) <$ multidegré$S(g_j, g_k)$. Écrivons $x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum b_{ijk} x^{\delta - \gamma_{ij}} g_i$. D'après le lemme 3.4.4, multidegré$b_{ijk} g_i \leq$ multidegré$x^{\delta - \gamma_{jk}} S(g_j, g_k) < \delta$.
Donc $\sum_{m(i)=\delta} LT(h_i) g_i = \sum c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum \tilde{h}_i g_i$ avec multidegré$(\tilde{h}_i g_i) < \delta$. Ce qui contredit la minimalité du multidegré de f. Absurde ! D'où multidegré$(f) = \delta$ et la proposition est établie.

∎

Exemple 3.4.6 *Soit* $I =< y-x^2, z-x^3 >$. *Nous allons montrer que* $G = \{y-x^2, z-x^3\}$ *est une base de Grner de* I *pour l'ordre* $>_{lex}$ *avec* $y > z > x$. *Calculons*

$$S(y-x^3, z-x^3) = \frac{yz}{y}(y-x^2) - \frac{yz}{r}(z-x^3) = -zx^2 + yx^3$$

L'algorithme de division donne le reste $r = 0$ *car :*

$$-zx^2 + yx^3 = x^3(y-x^2) + (-x^2)(z-x^3) + 0$$

3.5 Algorithme de Buchberger

Il s'agit à présent de construire une base de Gröbner à partir d'une base de $I = \{f_1, \dots, f_s\}$. C'est l'objet de l'algorithme de Buchberger.

Théorème 3.5.1 *Soit* $I =< f_1, \dots, f_s >$ *un idéal non nul de* $k[x_1, \dots, x_n]$. *Alors nous pouvons déterminer une base de Gröbner pour* I *en un nombre fini d'opérations par l'algorithme suivant :*
Entré : $F = (f_1, \dots, f_s)$
Sortie : une base de Gröbner $G = \{g_1, \dots, g_s\}$ *pour* $I =< F >$ *avec* $F \subset G$.
$G := F$
Fait
$G' := G$
Pour toute paire $p \neq q$ *de* G' *fait* $S := \overline{S(p,q)}^{G'}$, *si* $S \neq 0$ *alors* $G := G \cup \{S\}$
Tant que $G = G'$.

PREUVE : • Montrons qu'à chaque étape $< G >= I$ et $F \subset G$.
D'abord à toutes les étapes $F \subset G$, donc $I \subset< G >$. Montrons que $G \subset I$. C'est vrai à l'initialisation. Ensuite pour $G' \subset G$, nous ajoutons $\overline{S(p,q)}^{G'} \in I$ à G. Donc $G \subset I$.
• L'algorithme s'arrête si $G = G'$. Alors G satisfait le critère de Buchberger. Donc G est une base de Gröbner.
• L'algorithme s'arrête effectivement. En effet à toutes les étapes $G' \subset G$, donc $< LT(G') > \subset< LT(G) >$. Si $G' \neq G$, montrons que $< LT(G') > \subset\neq< LT(G) >$. En effet un S-polynôme rajouté correspond à un polynôme r avec $LT(r) \notin< LT(G') >$. D'où une suite croissante d'idéaux de $k[x_1, \dots, x_n]$ noethérien, donc stationnaire. Ainsi $< LT(G') >=< LT(G) >$ et $G = G'$. ∎

Exemple 3.5.2 *Soit l'idéal* $I =< f_1, f_2 >=< x^3 - 2xy, x^2y - 2y^2 + x >$ *de* $k[x, y]$. *La base* $\{x^3 - 2xy, x^2y - 2y^2 + x\}$ *n'est pas de Gröbner car*

$$LT(S(f_1, f_2)) = -x^2 \notin < LT(f_1), LT(f_2) > .$$

Appliquons l'algorithme de Buchberger :

$$S(f_1, f_2) = f_3 = -x^2,\ S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy$$

Posons $F = \{f_1, \ldots, f_3\}$. *Nous avons* $\overline{S(f_1, f_3)}^F = -2xy \neq 0$. *Posons* $f_4 = -2xy$ *et* $F = \{f_1, \ldots, f_4\}$. *Alors*

$$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0$$

$$S(f_1, f_4) = y(x^3 - 2xy) - (1/2)x^2(-2xy) = -2xy^2 = yf_4, \overline{S(f_1, f_4)}^F = 0$$

$$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$$

Posons $f_5 = -2y^2 + x$ *et* $F = \{f_1, \ldots, f_5\}$. *Nous contrôlons que c'est une base de Gröbner. Remarquons que* ($f_1 = -xf_2 + f_4$ *et* $f_2 = -yf_3 + f_5$) $LT(f_1) = -xLT(f_3)$ *et* $LT(f_2) = -(1/2)xLT(f_4)$. *Donc* $\{f_3, \ldots, f_5\}$ *est encore une base de Gröbner. Il s'agit de systématiser ce calcul.*

Lemme 3.5.3 *Soit* G *une base de Gröbner pour l'idéal* I. *Soit* $p \in G$, *tel que* $LT(p) \in < LT(G - \{p\}) >$. *Alors* $G - \{p\}$ *est encore une base de Gröbner pour* I.

PREUVE : Par définition $< LT(G) >=< LT(I) >$. Comme $LT(p) \in < LT(G - \{p\} >$, $< LT(G - \{p\}) >=< LT(G) >$. Donc $G - \{p\}$ est encore une base de Gröbner. ∎

Définition 3.5.4 *Un base de Gröbner* G *de* I *est dite* **minimale** *si*
i. $LC(p) = 1$, $p \in G$,
ii. pour tout $p \in G$, $LT(p) \notin < LT(G - \{p\}) >$.

Exemples 3.5.5 • *Dans l'exemple 3.5.2, la base* $\{x^2, xy, y^2 - (1/2)x\}$ *est minimale. Mais il n'y a pas unicité de la base minimal car pour tout* $a \in k$, $\{x^2 + axy, xy, y^2 - (1/2)x\}$ *est aussi minimale.* • *Si* G *et* G' *sont deux bases minimales de* I *alors* $LT(G) = LT(G')$.

Définition 3.5.6 *Un base de Gröbner G de I est dite* **réduite** *si*
i. $LC(p) = 1$, $p \in G$,
ii. pour tout $p \in G$, *aucun monôme de* p *n'appartient à* $< LT(G - \{p\}) >$.

Proposition 3.5.7 *Soit I un idéal non nul de polynômes. Alors pour tout ordre admissible, I admet une unique base de Gröbner réduite.*

PREUVE : Soit G une base de Gröbner minimale de I. Nous dirons que $g \in G$ est réduit pour G si aucun monômes de g n'appartient à $< LT(G - \{g\} >$. Nous allons modifier G jusquà obtenir une base réduite.
Remarquons d'abord que si g est réduit pour G alors g est réduit pour toute base de Gröbner minimale de I qui contient g et qui a le même ensemble de termes dominants (la définition de base réduite ne concerne que les termes dominants).
$g \in G$, $g' = \overline{g}^{G-\{g\}}$ et posons $G' = (G - \{g\}) \cup \{g'\}$. Montrons que G' est encore une base minimale de I. En effet, quand on divise g par $G - \{g\}$, $LT(g)$ n'est divisible par aucun élément de $LT(G - \{g\})$, donc $LT(g) = LT(g')$. Donc $< LT(G) >=< LT(G') >$. Comme $G' \subset I$, G' est une base de Gröbner de I, qui est minimale. De plus g' est réduit pour G'. Nous appliquons ce procédé sur tous les éléments de G et nous obtenons ainsi une base réduite.
Montrons par l'absurde l'unicité. Soit G et G' deux bases réduites de I. Alors $LT(G) = LT(G')$ (à montrer pour deux bases minimales).
Soit $g \in G$. Il existe $g' \in G'$ avec $LT(g) = LT(g')$. Or $g - g' \in I$, donc $\overline{g - g'}^{G} = 0$. or $LT(g) = LT(g')$ et aucun terme du reste n'est divisible par un élément de $LT(G) = LT(G')$ (réduite). D'où $g - g' = 0$ et $G = G'$. ∎

3.6 Premières applications des bases de Gröbner

• Nous avons vu que si $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner de I et $f \in k[x_1, \ldots, x_n]$ alors

$$f \in I \text{ si et seulement si } \overline{f}^{G} = 0$$

Exemple 3.6.1 *Soit* $I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 > \in \mathbf{C}[x, y, z]$ *muni de l'ordre* $>_{grlex}$. *Soit* $f = xy - 5z^2 + x$. *Nous voulons déterminer si* $f \in I$. *Nous déterminons une base de Gröbner de* I : $G = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}$ *et nous constatons que* $LT(f) \notin < LT(G) >$. *Donc* $f \notin I$.

• Considérons le systême d'équations dans $\mathbf{C}^3$

$$\begin{cases} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{cases}$$

Considérons l'idéal $I =< x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z >$. Déterminons une base de Gröbner de I : $G := \{g_1 = x - z, g_2 = -y + 2z^2, g_3 = z^4 + (1/2)z^2 - 1/4\}$. Le système est équivalent au systême $g_1 = g_2 = g_3 = 0$. Or $g_3 = 0$ est équivalent à

$$z = \pm 1/2\sqrt{\pm\sqrt{5} - 1}$$

Ce qui permet de résoudre le système recherché.

• Soit la courbe de $\mathbf{C}^4$ d'équation :

$$\begin{cases} x = t^4 \\ y = t^3 \\ z = t^2 \end{cases}$$

Calculons une base de Gröbner de $I =< t^4 - x, t^3 - y, t^2 - z >$ pour l'ordre $>_{lex}$ dans $\mathbf{C}[t, x, y, z]$. Nous trouvons

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

Par conséquent la courbe est incluse dans l'intersection des surfaces $x - z^2 = 0, y^2 - z^3$. Nous ignorons si cette intersection est plus grosse que la courbe initiale. Cette question sera notamment l'objet du chapitre suivant.

4 Variétés affines et systèmes d'équations polynômiales

4.1 Rappels sur les résultants

Soit $f \in k[x_1, \ldots, x_n]$. Le polynôme f est irréductible sur k s'il n'est pas constant et s'il n'est pas produit de deux polynômes non constants dans $k[x_1, \ldots, x_n]$. Rappelons que pour k un corps, $k[x_1, \ldots, x_n]$ est factoriel. Ainsi tout polynôme non constant $f \in k[x_1, \ldots, x_n]$ est produit de polynômes irréductibles et la décomposition est unique à l'ordre près des facteurs irréductibles associés. De plus dans $k[x_1, \ldots, x_n]$, le lemme de Gauss est satisfait : si f est irréductible et si f divise $gh \in k[x_1, \ldots, x_n]$ alors f divise g ou h. Par conséquent :

Corollaire 4.1.1 *Soit $f, g \in k[x_1, \ldots, x_n]$ ayant des degrés en x_1 strictement positifs. Alors f et g ont un facteur commun dans $k[x_1, \ldots, x_n]$ de degré strictement positif en x_1 si et seulement si ils ont un facteur commun dans $k(x_2, \ldots, x_n)[x_1]$.*

PREUVE : $\Longrightarrow$ Clair.
$\Longleftarrow$ $f = \tilde{h}\tilde{f}_1$, $g = \tilde{h}\tilde{g}_1$ avec $\tilde{h}, \tilde{f}_1, \tilde{g}_1 \in k(x_2, \ldots, x_n)[x_1]$. Soit $d \in k[x_2, \ldots, x_n]$ le dénoinateur commun de $\tilde{h}, \tilde{f}_1, \tilde{g}_1$. Alors $d^2 f = h f_1$ et $d^2 f = h g_1$ dans $k[x_1, \ldots, x_n]$ ($f_1 = d\tilde{f}_1$...). Soit h_1 un facteur irréductible de h de degré strictement positif en x_1 (comme $\tilde{h} = h/d$ a un degré strictement positif en x_1, h_1 existe). Alors h_1 divise $d^2 f$. Mais $d^2 \in k[x_2, \ldots, x_n]$ donc h_1 divise f. De même h divise g. ∎

Lemme 4.1.2 *Soit $f, g \in k[x]$ des polynômes de degré $\ell > 0$ et $m > 0$. Alors f et g ont un facteur commun si et seulement si il existe des polynômes $A, B \in k[x]$ tels que :*
i. A et B ne sont pas tous les deux nuls
ii. A est de degré au plus $m - 1$ et B est de degré au plus $\ell - 1$,
iii. $Af + Bg = 0$.

PREUVE : Si f, g ont un facteur commun $f = h f_1$ et $g = h g_1$ alors $A = g_1$ et $B = -f_1$ conviennent.

Réciproquement si f, g n'ont pas de facteur commun $fu + gv = 1$. S'il existe A, B avec $Bg = -Af$, alors

$$B = (uf + vG)B = uBf + vBg = (uB - vA)f$$

et $\deg B > \ell$ absurde. ∎

Définition 4.1.3 *Soient $f, g \in k[x]$ de degrés strictement positifs avec*

$$f = a_0 x^\ell + \cdots a_\ell, \;\; g = b_0 x^m + \cdots + b_m.$$

La matrice de Sylvester de f, g est la matrice $(\ell + m) \times (\ell + m)$

$$Syl(f, g, x) = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & a_0 & & b_1 & b_0 & \\ a_2 & a_1 & \dots & b_2 & b_1 & \dots \\ \dots & & a_\ell & & & b_m \end{pmatrix}$$

Le résultant est le déterminant de la matrice de Sylvester $Res(f, g, x) = \det Syl(f, g, x)$.

Proposition 4.1.4 *Soit $f, g \in k[x]$ de degré strictement positif. Alors $Res(f, g, x)$ est un polynôme à coefficient entiers en les coefficients de f et g. Les polynômes f, g ont un facteur commun dans $k[x]$ si et seulement si $Res(f, g, x) = 0$.*
De plus, il existe des polynômes $A, B \in k[x]$ entiers en les coefficients de f et g avec $Af + Bg = Res(f, g, x)$.

Preuve : Il s'agit de résoudre le système $fu + gv = 1$ en utilisant la formule de Cramer qui fait intervenir $Res(f, g, x)$ en dénominateur. ∎

Il s'agit s'agit d'adapter les résultats sur les résultants au cas des anneaux de polynômes à plusieurs variables. Pour $f, g \in k[x_1, \ldots, x_n]$ de degré strictement positif en x_1, nous pouvons écrire :

$$f = a_0 x^\ell + \cdots a_\ell, \;\; g = b_0 x^m + \cdots + b_m$$

avec $a_i, b_j \in k[x_2, \ldots, x_n]$. On peut donc définir comme avant le résultant $Res(f, g, x_1) \in k[x_2, \ldots, x_n]$. Nous avons les résultats suivants :

Proposition 4.1.5 *Soit $f, g \in k[x_1, \ldots, x_n]$ de degré strictement positif en x_1. Alors*
i. $Res(f, g, x_1)$ est le premier idéal d'élimination $< f, g >_1 =< f, g > \cap k[x_2, \ldots, x_n]$.
ii. $Res(f, g, x_1) = 0$ si et seulement si f et g ont un facteur commun dans $k[x_1, \ldots, x_n]$ de degré strictement positif en x_1.

PREUVE : i. D'après la proposition 4.1.4, le résultant est un polynôme entier en les a_i, b_j. Donc $Res(f, g, x_1) \in k[x_2, \ldots, x_n]$ et il existe A, B des polynômes en x_1 entiers en les a_i, b_j tels que $Af + Bg = Res(f, g, x_1)$. Donc $A, B \in k[x_2, \ldots, x_n][x_1]$, donc $Res(f, g, x_1) \in < f, g >$.
ii. On applique la proposition 4.1.4 à $f, g \in k(x_2, \ldots, x_n)[x_1]$. Donc $Res(f, g, x_1) = 0$ ssi f, g ont un facteur commun dans $k(x_2, \ldots, x_n)[x_1]$, donc dans $k[x_1, \ldots, x_n]$. ∎

On montre ensuite comment le résultant est utile pour étendre les solutions partielles :

Proposition 4.1.6 *Soit $f, g \in k[x_1, \ldots, x_n]$ de degré strictement positif en x_1, avec*

$$f = a_0 x^\ell + \cdots a_\ell, \;\; g = b_0 x^m + \cdots + b_m$$

où $a_i, b_j \in k[x_2, \ldots, x_n]$.
Si $Res(f, g, x_1) \in \mathbf{C}[x_2, \ldots, x_n]$ s'annule en $(c_2, \ldots, c_n) \in \mathbf{C}^{n-1}$ alors
ou bien a_0 ou b_0 s'annulent en $(c_2, \ldots, c_n)$ ou bien il existe $c_1 \in \mathbf{C}$ tels que f et g s'annulent en $(c_1, \ldots, c_n) \in \mathbf{C}^n$.

PREUVE : Notons $c = (c_2, \ldots, c_n)$. Il s'agit de montrer que $f(x_1, c)$ et $g(x_1, c)$ ont une racine commune lorsque $a_0(c)$ et $b_0(c)$ ne sont pas tous les deux nuls. On suppose $a_0(c) \neq 0$ et $b_0(c) \neq 0$. Par hypothèses $h(c) = Res(f, g, x_1)(c) = 0$. Remarquons que $0 = h(c) = Res(f(x_1, c), g(x_1, c), x_1)$. Donc $f(x_1, c)$ et $g(x_1, c)$ ont une racine commune. ∎

4.2 Variétés affines

Définition 4.2.1 *Soit $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. L'ensemble des solutions du système d'équations polynômiales :*

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

est dit **variété affine définie par** $f_1, \ldots, f_s$ *et est notée* $V(f_1, \ldots, f_s)$.
Un ensemble $V \subset k^n$ est dit **variété affine** *s'il existe une famille de polynômes $f_1, \ldots, f_s$ telle que $V = V(f_1, \ldots, f_s)$.*

Exemples 4.2.2 • $V(x^2 + z^2 - 1)$ *(cylindre)*
• $V(x^2 + y^2 + (z-1)^2 - 4)$ *(sphère)*
• $V((x^2 + z^2 - 1)(x^2 + y^2 + (z-1)^2 - 4))$ *(réunion)*
• $V(x^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 4)$ *(intersection)*
• $\mathbf{R} - \{0, 1, 2\}$ *n'est pas une variété affine.*

Lemme 4.2.3 *i. Si V, W sont des variétés affines, alors $V \cap W$ et $W \cup V$ sont des variétés affines.*
ii. Un ensemble fini de points de k^n est une variété affine.

Preuve : i. Supposons que $V = V(f_1, \ldots, f_s)$ et $W = V(g_1, \ldots, g_r)$. Montrons que

$$V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_r), \;\; V \cup W = V(f_i g_j, 1 \leq i \leq s, 1 \leq j \leq r)$$

La première égalité est claire. Pour la deuxième, on a $V, W \subset V(f_i g_j)$. Si $(a_1, \ldots a_n) \in V(f_i g_j) - V$, alors il existe i_0 avec $f_{i_0}(a_1, \ldots, a_n) \neq 0$. Or $f_{i_0} g_j(a_1, \ldots, a_n) = 0$, $1 \leq j \leq r$ donc $(a_1, \ldots, a_n) \in W$. ii. Il suffit de prendre le polynôme dont les racines sont les points de l'ensemble fini. ∎

Il alors naturel de se poser les questions suivantes :
• $V(f_1, \ldots, f_s) \neq \emptyset$? i.e, le système a-t-il des solutions ?
• Si $V(f_1, \ldots, f_s)$ est fini, peut-on trouver les solutions explicitement ?
• Peut-on définir est déterminer la dimension de $V(f_1, \ldots, f_s)$?
Nous allons voir que les réponses à ces questions sont en lien avec les bases de Gröbner.

4.3 Des variétés affines aux idéaux

Commençons par le lemme élémentaire suivant :

Lemme 4.3.1 *Si* $< f_1, \ldots, f_s >=< g_1, \ldots, g_r >$ *alors* $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_r)$.

D'après le lemme 4.3.1, on peut donc penser à V comme défini par un idéal I de $k[x_1, \ldots, x_n]$ et écrire $V(I)$. Réciproquement, étant donné V, on peut définit $I(V)$ tel $V = I(V)$.

Définition 4.3.2 *Soit* $V \subset k^n$ *une variété affine, nous définissons*

$$I(V) = \{f \in k[x_1, \ldots, x_n], f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in V\}.$$

Lemme 4.3.3 $I(V)$ *est un idéal.*

PREUVE : $O \in I(V)$, $f, g \in I(V) \Longrightarrow f - g \in I(V)$, $hf \in I(V)$. ∎

Remarque 4.3.4 *Soit* $V = V(f_1, \ldots, f_s)$. *En général,* $< f_1 \ldots, f_s > \neq I(V(f_1, \ldots, f_s))$.

Exemple 4.3.5 *Soit* $I = (x^2)$ *et* $V = V(I) = V(x^2)$ *dans* $\mathbf{R}^2$. *Ainsi* $V = \{(0, b), b \in \mathbf{R}\}$. *Donc* $x \in I(V)$ *et* $I \neq I(V)$.

Lemme 4.3.6 *i.*$< f_1, \ldots, f_s > \subset I(V(f_1, \ldots, f_s))$
ii. Soit V *une variété affine,* $V(I(V)) = V$.

PREUVE : i. Clair.
ii. $I \subset I(V) \Longleftrightarrow V(I) \subset V(I(V))$. Réciproquement si $(a_1, \ldots, a_n) \in V(I)$ alors $(a_1, \ldots, a_n) \in V(I(V))$ donc $V(I) \subset V(I(V))$. ∎

Le lien entre $< f_1, \ldots, f_s >$ et $I(V(f_1, \ldots, f_s))$ est assez subtile et dépend du corps considéré:

Exemples 4.3.7 • *Dans* $\mathbf{R}$, $V(x^2+1) = \emptyset$ *ainsi* $I(V(x^2+1)) = \mathbf{R}[X]$.
• *Dans* $\mathbf{C}$, $V(x^2+1) = \{\pm i\}$ *et* $I(V(x^2+1)) =< x^2+1 >$.

Même si, en général, $I(V(f_1, \ldots, f_s))$ est différent de $< f_1, \ldots, f_s >$, l'idéal de la variété détermine la variété de façon unique :

Lemme 4.3.8 *Soit* V, W *deux variétés affines dans* k^n.
i. $V \subset W$ *ssi* $I(W) \subset I(V)$.
ii. $V = W$ *ssi* $I(V) = I(W)$.

Preuve : i. Clair
ii. Si $W = (g_1, \ldots, g_s)$ alors $g_i \in I(V)$ et les g_i s'annulent sur V donc $V \subset W$ ∎

Ainsi, nous devinons la richesse du lien entre variété affine et idéaux. Nous allons pouvoir déduire des résultats obtenus sur les idéaux des informations sur les variétés affines et donc sur la résolution des systèmes d'équations de polynômes.

5 Résolution des systèmes d'équations polynômiales

5.1 Théorème d'élimination

Nous allons décrire des méthodes systèmatiques pour éliminer des variables dans un systèmes d'équations polynômiales. Commençons par rappeler la stratégie pour un systême d'équations linéaires $AX = B$:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \qquad\qquad \cdot \\ \qquad\qquad \cdot \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}$$

Par opérations successives sur les lignes de ce système, on se ramène à un système triangulaire $TX = C$ qu'il est facile à résoudre. Nous voyons, qu'il y a donc deux étapes :

• une étape **d'élimination** qui consiste à trianguliariser le système.
• une étape **d'extension** qui consiste à reporter dans chaque équation les solutions de l'équation précédente en partant du bas.
Nous cherchons à faire la même chose pour les systèmes d'équations polynômiales.

Exemple 5.1.1 *Soit le systême*

$$\begin{cases} x^2+y+z=1 \\ x+y^2+z=1 \\ x+y+z^2=1 \end{cases}$$

On considère l'idéal $I =< x^2+y+z=1, x+y^2+z=1, x+y+z^2=1 >$. *Une base de Gröbner pour* I *(ordre* $>_{lex}$*) est*

$$\begin{aligned} g_1 &= x+y+z^2-1 \\ g_2 &= y^2-y-z^2+z \\ g_3 &= 2yz^2+z^4-z^2 \\ g_4 &= z^6-4z^4+4z^3-z^2 \end{aligned}$$

Or $g_4 = z^2(z-1)^2(z^2+2z-1)$. *Donc* $z \in \{0, 1, -1 \pm \sqrt{2}\}$. *On remplace dans* g_2 *et* g_3, *on détermine les* y *possibles et on remplace le tout dans* g_1. *D'où les solutions du systêmes*

$$(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Nous constatons que nous sommes passés par les mêmes deux étapes pour les systèmes polynomiaux que pour les systêmes linéaires. Dans l'étape d'élimination, nous avons obtenu $g_4 \in I \cap k[z]$, $g_2, g_3 \in I \cap k[y,z]$. *Ce qui a permis de faire fonctionner l'étape d'extension. Nous allons généraliser ces idées.*

Définition 5.1.2 *Soit* $I =< f_1, \ldots, f_s > \subset k[x_1, \ldots, x_n]$. *Le* ℓ**-ième idéal d'élimination** I_ℓ *est l'idéal de* $k[x_{\ell+1}, \ldots, x_n]$ *défini par*

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n]$$

Remarque 5.1.3 *(voir TD)* • I_ℓ *est un idéal de* $k[x_{\ell+1}, \ldots, x_n]$
• $I_0 = I$
• *le* ℓ*-ème idéal d'élimination dépend de l'ordre choisi sur les variables.*

Il s'agit de trouver un moyen systématique pour trouver les éléments de I_ℓ.

Théorème 5.1.4 *(d'élimination)*
Soit $I \subset k[x_1, \ldots, x_n]$, G une base de Grobner de I pour l'ordre lexicographique où $x_1 > x_2 > \cdots > x_n$. Alors pour tout $0 \leq \ell \leq n$,

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

est une base de Gröbner du ℓ-ème idéal d'élimination I_ℓ.

PREUVE : Soit $0 \leq \ell \leq n$, $G_\ell \subset I_\ell$ et il suffit de montrer que $< LT(I_\ell) > \subset < LT(G_\ell) >$ (l'autre inclusion est claire).
Il suffit de montrer que

$$\forall f \in I_\ell, \exists g \in G_\ell \text{ avec } LT(g) | LT(f)$$

Comme $f \in I$, $\exists g \in G$ tel que $LT(g)|LT(f)$.
Comme $f \in I_\ell$, $LT(g) \in k[x_{\ell+1}, \ldots, x_n]$.
Comme on utilise l'ordre lexicographique $x_1 > \ldots > x_n$, tout monôme contenant $x_1, \ldots, x_\ell$ est plus grand que tout monôme de $k[x_{\ell+1}, \ldots, x_n]$. D'où $LT(g) \in k[x_{\ell+1}, \ldots, x_n]$, $g \in k[x_{\ell+1}, \ldots, x_n]$ et $g \in G_\ell$. ∎

Remarque 5.1.5 *(voir TD) D'après le théorème d'élimination, une base de Gröbner pour l'ordre lexicographique permet d'éliminer la première variable, les deux premières, les trois premières... Si on veut éliminer seulement certaines variables, il faudra choisir un ordre mieux adapter.*

Voyons à présent, l'énoncé de l'étape d'extension.

5.2 Théorème d'extension

Et maintenant l'étape d'extension :

Théorème 5.2.1 *(d'extension)*
Soit $I =< f_1, \ldots, f_s > \subset \mathbf{C}[x_1, \ldots, x_n]$ *et soit* I_1 *le premier idéal d'élimination de* I. $\forall 1 \leq i \leq s$, *écrivons,*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{termes où } x_1 \text{ a un degré } < N_i$$

Supposons avoir une solution partielle $(a_2, \ldots, a_n) \in V(I_1)$. *Si* $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$ *alors* $\exists a_1 \in \mathbf{C}$ *tel que* $(a_1, \ldots, a_n) \in V(I)$.

Avant de démontrer ce théorème, nous allons expliquer son énoncé et donner quelques applications.

Remarque 5.2.2 • *Ici l'hypothèse sur le corps* $\mathbf{C}$ *est essentielle. Le théorème d'extension est faux, par exemple sur* $\mathbf{R}$ *:*

$$\begin{cases} x^2 = y \\ x^2 = z \end{cases}$$

En éliminant la variable x, *on trouve* $y = z$. *Mais la solution* (a, a) *pour* $a \in \mathbf{R}$ *ne s'étend pas en une solution sur* $\mathbf{R}^3$ *pour* $a < 0$.
• *Dans le théorème, les* $g_i x_1^{N_i}$ *sont les termes dominants des* f_i. *L'hypothèse* $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$, *signifie donc que les termes dominants ne s'annulent pas simultanément. Cette hypothèse est nécessaire comme le montre l'exemple suivant*

$$\begin{cases} xy = 1 \\ xz = 1 \end{cases}$$

$I_1 =< y - z >$. *La solution partielle* $(0, 0)$ *ne s'étend pas.*
• *Même si le théorème est énoncé pour une seule variable, il peut servir à relever plusieurs variables en l'appliquant plusieurs fois. Par exemple, soit le système :*

$$\begin{cases} x^2 + y^2 + z^2 = 1 \\ xyz = 1 \end{cases}$$

Une base de Gröbner pour I *pour* $>_{lex}$ *est* $G = \{g_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1, g_2 = x + y^3z + yz^3 - yz\}$. *Le théorème d'élimination donne*

$$I_1 =< g_1 >, I_2 = \{0\}$$

Donc $V(I_2) = \mathbf{C}$ *et tout* $c \in \mathbf{C}$ *est solution partielle. Il s'agit maintenant de savoir si toute solution partielle* $c \in \mathbf{C}$ *se relève en une solution* $(a, b, c) \in V(I)$.
D'abord on cherche à relever c *en une solution partielle* $(b, c) \in V(I_1)$. *Le coefficient de* y^4 *de* g_1 *est* z^2. *Donc tout* $c \in C^*$ *sétend en une solution de* $V(I_1)$ *(remarquons que pour* $c = 0$, g_1 *n'a pas de solution. Pour* $V(I)$, *on remplace* (b, c) *dans le système et on trouve qu'il a une solution* a *en* x. *Le théorème donne aussi le résultat car les coefficient dominant sont 1 et* yz *qui ne s'annulent pas pour* $c \neq 0$. *Donc toute solution partielle* $c \neq 0$ *se relève en une solution du système.*

Il y a un cas particulier du théorème qui est particulièrement facile à utiliser : c'est le cas où le coefficient dominant est constant :

Corollaire 5.2.3 *Soit* $I =< f_1, \ldots, f_s > \subset \mathbf{C}[x_1, \ldots, x_n]$ *et supposons qu'il existe* i *tel que*

$$f_i = cx_1^N + \text{ termes où } x_1 \text{ a un degré} < N$$

où $c \in \mathbf{C}^*$ *et* $N > 0$. *Alors si* $(a_2, \ldots, a_n) \in V(I_1)$ *alors il existe* $a_1 \in \mathbf{C}$ *tel que* $(a_1, \ldots, a_n) \in V(I)$.

Démontrons d'abord le théorème d'extension lorsque l'idéal est engendré par deux polynômes puis le cas général.

Proposition 5.2.4 *Soit* $I =< f, g >$ *idéal de* $k[x_1, \ldots, x_n]$ *et* I_1 *le premier idéal d'élimination de* I. *Supposons avoir une solution partielle* $(c_2, \ldots, c_n) \in V(I_1)$. *Si* $(c_2, \ldots, c_n) \notin V(a_0, b_0)$ *alors il existe* $c_1 \in \mathbf{C}$ *tel que* $(c_1, \ldots, c_n) \in V(I)$.

PREUVE : Si $a_0(c)$ et $b_0(c)$ ne s'annulent pas, appliquer la proposition 4.1.6. Il faut maintenant montrer qu'il suffit que l'un des deux s'annulent. Supposons $a_0(c) \neq 0$ et $b_0(c) = 0$. Pour tout $N > 0$, $< f, g >=< f, g + x^N f >$. Choisissons N assez grand de telle façon que $x_1^N f$ est de degré en x_1 plus grand que le degré en x_1 de g. Ainsi le coefficient dominant de $g + x_1^N f(c) \neq 0$. D'où $existsc_1 \in C$ tel que $(c_1, c) \in V(f, g)$. ∎

Définition 5.2.5 *Soient $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ et $u_2, \dots, u_s$ des variables. Le résultant généralisé de $f_1, \dots, f_s$ est*

$$Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \dots, x_n) u^\alpha \in k[x_2, \dots, x_n, u_2, \dots, u_s]$$

où $h_\alpha \in k[x_2, \dots, x_n]$ et $u^\alpha = u_2^{\alpha_2} \cdots u_s^{\alpha_s}$.

Maintenant, nous allons démontrer le théorème d'extension avec un nombre arbitraire de générateurs de I :

Théorème 5.2.6 *Soit $I =< f_1, \dots, f_s > \subset \mathbf{C}[x_1, \dots, x_n]$ et I_1 le premier idéal d'élimination de I. Pour tout $1 \leq i \leq s$, écrivons f_i sous la forme*

$$f_i = g_i(x_2, \dots, x_n) x_1^{N_i} + \text{ termes de degré en } x_1 < N_i$$

où $N_i \geq 0$ et $g_i \in \mathbf{C}[x_2, \dots, x_n]$ non nul. Supposons avoir une solution partielle $(c_2, \dots, x_n) \in V(I_1)$. Si $(c_2, \dots, c_n) \notin V(g_1, \dots, g_s)$ alors il existe $c_1 \in \mathbf{C}$ tel que $(c_1, c_2, \dots, c_n) \in V(I)$.

PREUVE : On note $c = (c_2, \dots, c_n)$. Il suffit de démontrer le théorème pour $s \geq 3$. Comme $c \notin V(g_1, \dots, g_s)$ on peut supposer $g_1(c) \neq 0$. Considérons le résultant généralisé :

$$Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha u^\alpha = h$$

• Montrons que les h_α appartiennent à I_1.
Il existe $A, B \in \mathbf{C}[u_2, \dots, u_s, x_1, \dots, x_n]$ avec

$$Af_1 + B(u_2 f_2 + \cdots + u_s f_s) = Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha u^\alpha$$

Écrivons $A = \sum_\alpha A_\alpha u^\alpha$ et $B = \sum_\alpha B_\alpha u^\alpha$ avec $A_\alpha, B_\alpha \in k[x_1, \dots, x_2]$. Il suffit de démontrer que $h_\alpha \in I$ car comme $h_\alpha \in k[x_2, \dots, x_n]$ on aura $h_\alpha \in I_1$.
Posons $e_i = (0, \dots, 0, 1, 0 \dots, 0)$ (à la place i). Nous avons

$$\sum_\alpha h_\alpha u^\alpha = \Big(\sum_\alpha A_\alpha u^\alpha \Big) f_1 + \Big(\sum_\beta B_\beta u^\beta \Big) \Big(\sum_{i \geq 2} u^i f_i \Big)$$

$$= \sum_{\alpha} \Big(A_\alpha f_1 + \sum_{i\geq 2, \beta, \beta+e_i=\alpha} B_\beta f_i \Big) u^\alpha.$$

D'où $h_\alpha = A_\alpha f_1 + \sum_{i\geq 2,\beta,\beta+e_i=\alpha} B_\beta f_i$. Donc $h_\alpha \in I$ donc $h_\alpha \in I_1$ pour tout α.

Comme $c \in I_1$, $h_\alpha(c) = 0$ pour tout α, donc $h(c, u_2, \dots, u_s) = 0$.

• Supposons que $f_2(c) \neq 0$ et que le degré en x_1 de f_2 est plus grand que les degrés en x_1 de $f_3, \dots, f_s$. Nous allons démontrer le théorème dans ce cas.
Pour cela commençons par montrer que

$$h(c, u_2, \dots, u_s) = Res(f_1(x_1, c), u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c), x_1).$$

Rappelons que $h = Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1)$, donc si on l'évalue en c on trouve le résultant pourvu que les coefficients dominants de f_1 et $u_2 f_2 + \cdots + u_s f_s$ ne s'annulent pas. Ce qui est le cas par hypothèse.
Ainsi $h(c, u_2, \dots, u_s) = 0 = Res(f_1(x_1, c), u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c), x_1)$. Donc il existe un polynôme F de degré strictement positif en x_1 avec F divise $f_1(x_1, c)$ (donc $F \in \mathbf{C}[x_1]$) et F divise $u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c)$. Il existe $A \in \mathbf{C}[x_1, u_2, \dots, u_s]$ tel que

$$F(x_1) A(x_1, u_2, \dots, u_s) = u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c).$$

En comparant les coefficients de $u_2, \dots, u_s$ nous trouvons F divise $f_2(x_1, c), \dots, f_s(x_1, c)$. Donc F est un facteur commun aux f_i, $1 \leq i \leq s$. Donc ils ont une racine $c_1 \in \mathbf{C}$ commune. D'où le théorème d'extension.
• Montrons comment ramener le cas général au cas précédent. Pour cela, il suffit de remplacer f_2 par $f_2 + x_1^N f_1$ pour N assez grand. ∎

5.3 Rappels sur les idéaux

Définition 5.3.1 *Soit I un idéal d'un anneau A. Le radical de I est l'idéal*

$$rac(I) = \{x \in A, \exists r \in \mathbf{N}, x^r \in I\}.$$

Exemple 5.3.2 *Soit $f \in k[x_1, \ldots, x_n]$ et $I =< f >$. Si $f = f_1^{\alpha_1} \cdots f_s^{\alpha_s}$ est la décomposition de f en irréductible alors $rac(I) =< f_1 \cdots f_s >$. (exercice).*

Définition 5.3.3 *Soit $I \subset k[x_1, \ldots, x_n]$. L'idéal I est dit* **premier** *si pour tout $f, g \in k[x_1, \ldots, x_n]$, $fg \in I$ implique que f ou g appartient à I.*

Remarque 5.3.4 *Si I est premier, $k[x_1, \ldots, x_n]/I$ est intègre.*

Définition 5.3.5 *Un idéal I de A est dit* **maximal** *si $I \neq A$ et si tout idéal J contenant I est égal à A ou à I.*

Proposition 5.3.6 *Un idéal I de A est maximal si et seulement si A/I est un corps.*

PREUVE : Si I est maximal et $\bar{x}$ est non nul dans A/I, alors $x \notin I$ donc l'idéal $I + xA$ contient strictement I ; par minimalité de I, on a $A = I + xA$ et 1 sécrit $1 = i + xa$ avec $i \in I$ et $a \in A$ ce qui se traduit par $\bar{1} = \bar{x}\bar{a}$, d'où $\bar{x}$ inversible dans A/I. Comme $I \neq A$, l'anneau A/I n'est pas nul et ses éléments non nuls sont inversibles, i.e A/I est un corps. En sens inverse si A/I est un corps, alors $I \neq A$ et tout idéal J de A contenant strcitement I contient un élément $x \notin I$. Alors $\bar{x}$ est inversible dans A/I, soit $\bar{1} = \bar{x}\bar{a}$ avec $a \in A$, ou encore $1 = xa + i$ avec $i_i nI \subset J$ et $x \in J$. Ainsi $1 \in J$ et $J = A$. ∎

Théorème 5.3.7 *(Krull) Dans un anneau commutatif A, tout idéal $I \neq A$ est inclus dans un idéal maximal.*

PREUVE : L'ensemble des idéaux de A contenant I et disctincts de A est inductif car si $(I_i)_{i \in I}$ est une famille totalement ordonnée d'idéaux distincts de A, la réunion est encore un idéal (parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1). On applique alors le lemme de Zorn. ∎

Définition 5.3.8 *Une partie S d'un anneau commutatif intègre A est dite* **multiplicative**, *si $1 \in S$, $0 \notin S$ et si $\forall s, s' \in S$, $ss' \in S$.*

Exemples 5.3.9 • *$S = A - \{0\}$ est une partie multiplicative de A.*
• *Soit $f \in A - \{0\}$, $S = \{f^n, n \in \mathbf{N}\}$ est une partie multiplicative de A.*
• *Si $\mathbf{p}$ est un idéal premier alors $S = A - \{\mathbf{p}\}$ est une partie multiplicative de A ($0 \in \mathbf{p}$, $1 \notin \mathbf{p}$, $x, y \in S, \Longrightarrow, xy \in S$).*

Nous pouvons établir le résultat suivant (en copiant la construction du corps $\mathbf{Q}$ à partir de l'anneau $\mathbf{Z}$:

Proposition 5.3.10 *Sur le produit $S \times A$, considérons la relation suivante $(s, a)\tilde{}(s', a')$ si $s'a = a's$. Alors $\tilde{}$ est une relation d'équivalence compatible avec les opérations suivantes :*

$$[(s_1, a_1), (s_2, a_2)] \mapsto (s_1 s_2, s_1 a_2 + s_2 a_1)), \quad [(s_1, a_1), (s_2, a_2)] \mapsto (s_1 s_2, a_1 a_2)$$

Muni de ces deux opérations l'ensemble quotient $S^{-1}A = S \times \tilde{}$ est un anneau.
L'application $i : A \to S^{-1}A$, $a \mapsto (1, a)$ est un morphisme d'anneaux injectif et les images des éléments $(1, s)$ sont inversibles d'inverses $(s, 1)$.

Corollaire 5.3.11 *Si $S = A - \{0\}$, l'anneau $S^{-1}A$ est un corps appelé le* **corps des fractions de** *A.*

Par construction Frac A est le plus petit corps contenant A.

Exemples 5.3.12 • *Pour $f \in A$ et $S = \{f^n, n \in \mathbf{N}\}$. On note $S^{-1}A = A_f$ et on a $A_f \simeq A[T]/(fT - 1)$.*
• *Pour $\mathbf{p}$ un idéal premier et $S = A - \mathbf{p}$, on note $S^{-1}A = A_{gp}$.*

5.4 Rappel sur le Nullstellensatz

Référence : Introduction à la géométrie algébrique, D. Perrin.

Lemme 5.4.1 *Soit k un corps algébriquement clos non dénombrable et K une extension de k de dimension au plus dénombrable. Alors $K = k$.*

PREUVE : Il suffit de démontrer que K est algébrique sur k. Sinon il contiendrait un élément transcendant donc un sous-corps isomorphe au corps des fractions rationnelles $k(T)$. Mais ce corps contient la famille non dénombrables des $1/(T-a)$ avec $a \in$ et cette famille est libre : si on a une relation

$$\sum_{i=1}^{n} \frac{\lambda_i}{T-a_i} = 0$$

en multipliant par $T - a_i$ et en faisant $T = a_i$, ontrouve bien $\lambda_i = 0$. ∎

Théorème 5.4.2 *(nullstellensatz faible)*
Soit I un idéal de $\mathbf{C}[x_1, \ldots, x_n]$ distincts de $\mathbf{C}[x_1, \ldots, x_n]$. Alors $V(I)$ est non vide.

PREUVE : Quitte à plonger I dans un idéal maximal, nous pouvons supposer I maximal. Notons $K = \mathbf{C}[x_1, \ldots, x_n]/I$ le corps résiduel. Or $\mathbf{C}[x_1, \ldots, x_n]$ est un $\mathbf{C}$-espace vectoriel de dimension au plus dénombrable sur $\mathbf{C}$, donc K aussi. D'après le lemme 5.4.1, $K = \mathbf{C}$. Notons a_i les images de X_i dans K. Si $P(X_1, \ldots, X_n) \in I$ alors $P(a_1, \ldots, a_n) = 0$ donc $(a_1, \ldots, a_n) \in V(I)$, non vide. ∎

Théorème 5.4.3 *(Nullstellensatz)*
Soit I un idéal de $k[x_1, \ldots, x_n]$. On a $I(V(I)) = rac(I)$.

PREUVE : Posons $R = k[x_1, \ldots, x_n]$ et $I =< f_1, \ldots, f_s >$ et $V = V(I)$. Il est clair que $rac(I) \subset I(V(I))$.
Réciproquement soit $f \in I(V)$, montrons que $f^m \in I$ pour m assez grand.
Soit $R_{(f)}$ l'anneau localisé en f. Il suffit de montrer que l'idéal $IR_{(f)}$ engendré par I dans $R_{(f)}$ est égal à $(1) = R_{(f)}$ car alors

$$1 = \sum_i \frac{f_i P_i}{f^m}$$

donc en chassant le dénominateur, on trouve bien $f^m \in I$.
Mais l'anneau $R_{(f)}$ est isormorphe à $k[x_1, \ldots, x_n, T]/(1 - Tf)$, donc la condition $IR_{(f)} =$

(1) signifie que $1 = \sum_i f_i P_i + A(1 - Tf)$ avec $A, P_i \in k[x_1, \ldots, x_n, T]$. Soit $J = (f_1, \ldots, f_s, 1_T f)$ l'idéal de $k[x_1, \ldots, x_n, T]$. On a $V(J) = \emptyset$ dans k^{n+1} car si $(c_1, \ldots, c_n, t) \in V(J)$, le point $(c_1, \ldots, c_n)$ annulerait les f_i et serait dans V donc annulerait f et ne pourrait pas annuler $1 - Tf$. Il résulte du nullstellensatz faible que $J = (1)$. ∎

Exemple 5.4.4 • *Pour $I = (x, y^2)$, nous avons $I(V(I)) = (x, y)$.* • *Il est clair que $I(V)$ est égal à sa racine. Il est radical. Ainsi $I(V(I)) = I$ si et seulement si I est radical.*

Corollaire 5.4.5 *Sur un corps algébriquement clos,*
I: variétés affines $\to$ idéaux radicaux
V: idéaux radicaux $\to$ variétés affines
sont des bijections inverses l'une de l'autre.

5.5 Théorème de fermeture

Nous allons voir ici le lien entre les variétés affines engendrées par les idéaux d'élimination et les projections de la variété sur des sous-espaces affines. Dans tout ce paragraphe, nous travaillons avec le corps $k = \mathbf{C}$.

Soit $V = V(f_1, \ldots, f_s) \subset \mathbf{C}^n$ une variété affine. Soit $1 \leq \ell \leq n$ et soit la projection

$$\pi_\ell : \mathbf{C}^n \to \mathbf{C}^{n-\ell}, (a_1, \ldots, a_n) \mapsto (a_{\ell+1}, \ldots, a_n).$$

Ainsi $\pi_\ell(V) \subset \mathbf{C}^{n-\ell}$. Nous allons relier $\pi_\ell(V)$ avec le ℓ-ième idéal d'élimination.

Lemme 5.5.1 *Soit $I =< f_1, \ldots, f_s > \in \mathbf{C}[x_1, \ldots, x_n]$. Dans $\mathbf{C}^{n-\ell}$, nous avons $\pi_\ell(V) \subset V(I_\ell)$.*

PREUVE : Soit $f \in I_\ell$. Si $(a_1, \ldots, a_n) \in V$, alors f s'annule en $(a_1, \ldots, a_n)$ car $f \in < f_1, \ldots, f_s >$. Or $f \in \mathbf{C}[x_{\ell+1}, \ldots, x_n]$, donc $f(a_{\ell+1}, \ldots, a_n) = f(\pi_\ell(a_1, \ldots, a_n)) = 0$. Donc f s'annule en tout point de $\pi_\ell(V)$. ∎

D'après la preuve du lemme, nous avons

$$\pi_\ell(V) = \{(a_{\ell+1}, \ldots, a_n) \in V(I_\ell), \text{ tel que } \exists a_1, \ldots, a_\ell \in \mathbf{C} \text{ avec } (a_1, \ldots, a_\ell, a_{\ell+1}, \ldots a_n) \in V\}.$$

Ainsi π_ℓ est l'ensemble des solutions partielles qui s'étendent en des solutions de V. Remarquons que $\pi_\ell(V)$ n'est pas une variété affine en général. Pour le système

$$\begin{cases} xy = 1 \\ xz = 1 \end{cases}$$

$V(I_1) = \{x = z\}$ mais $\pi_1(V) = \{(a, a) \in \mathbf{C}^2, a \neq 0\}$.
Le lien entre $\pi_\ell(V)$ et $V(I_\ell)$ est précisé par le théorème suivant :

Théorème 5.5.2 *(de fermeture) Soit $V = V(f_1, \ldots, f_s) \subset \mathbf{C}^n$ et soit I_ℓ le ℓ-ème idéal d'élimination de $< f_1, \ldots, f_s >$. Alors*
i. $V(I_\ell)$ est la plus petite variété affine contenant $\pi_\ell(V) \subset \mathbf{C}^{n-\ell}$.
ii. Si $V \neq 0$, alors il existe une variété affine $W \subset\neq V(I_\ell)$ tel que $V(I_\ell) - W \subset \pi_\ell(V)$.

Remarque 5.5.3 *D'après le théorème de fermeture, $V(I_\ell)$ est la plus petite variété telle que $\pi_\ell(V) \subset V(I_\ell)$. De plus si Z est une autre variété de $\mathbf{C}^{n-\ell}$ contenant $\pi_\ell(V)$ alors $V(I_\ell) \subset Z$. Autrement dit, $V(I_\ell)$ est la fermeture de Zariski de $\pi_\ell(V)$.*

Nous allons maintenant démontrer le théorème de fermeture. Pour cela, il nous faut introduire la notion de fermeture de Zariski.

Définition 5.5.4 *La fermeture de Zariski d'un sous-ensemble d'un espace affine est la plus petite variété affine contenant cet ensemble.*

Proposition 5.5.5 *Soit $S \subset k^n$. La variété affine $V(I(S))$ est la fermeture de Zariski S.*

PREUVE : Si $S \subset W$ alors $I(W) \subset I(S)$ et $V(I(S)) \subset V(I(W))$. Comme W est une variété affine $W = V(I(W))$. ∎

Théorème 5.5.6 *(de fermeture)*
Soit k un corps algébriquement clos. Soit $V = V(f_1, \dots, f_s) \in k^n$ et $\pi_\ell : k^n \to k^{n-\ell}$ la projection sur les $n - \ell$ dernières variables. Si I_ℓ est le ℓ-ème idéal d'élimination $I_\ell =< f_1, \dots, f_s > \cap k[x_{\ell+1}, \dots, x_n]$ alors $V(I_\ell)$ est la fermeture de Zariski de $\pi_\ell(V)$.

PREUVE : Il s'agit de montrer que $V(I_\ell) = V(I(\pi_\ell(V)))$. Nous avons déjà $\pi_\ell(V) \subset V(I_\ell)$. Comme $V(I(\pi_\ell(V)))$ est la plus petite variété contenant $\pi_\ell(V)$, nous avons $V(I(\pi_\ell(V))) \subset V(I_\ell)$.
Réciproquement si $f \in I(\pi_\ell(V))$, i.e $f(a_{\ell+1}, \dots, a_n) = 0$ pour tout $(a_{\ell+1}, \dots, a_n) \in \pi_\ell(V)$. Alors considéré comme un élément de $k[x_1, \dots, x_n]$, $f(a_1, \dots, a_n) = 0$ pour tout $(a_1, \dots, a_n) \in V$. D'après le théorème des zéros de Hilbert, $f^N \in < f_1, \dots, f_s >$. Comme f ne dépend pas de $x_1, \dots, x_\ell$, f^N non plus et $f^N \in < f_1, \dots, f_s > \cap k[x_{\ell+1}, \dots, x_n] = I_\ell$. Donc $f \in rac(I_\ell)$. Donc $I(\pi_\ell(V)) \subset rac(I_\ell)$. Donc $V(I_\ell) = V(rac(I_\ell)) \subset V(I(\pi_\ell(V)))$. ∎

6 Variétés irréductibles

6.1 Définitions, motivations

Définition 6.1.1 *Une variété affine V est dite* **irréductible** *si V ne peut pas s'écrire $V = V_1 \cup V_2$ où V_1, V_2 sont des variétés affines distinctes de V.*

Exemple 6.1.2 *$V(xz, xy)$ n'est pas une variété irréductible.*

Proposition 6.1.3 *Soit $V \subset k^n$ une variété affine. Alors V est irréductible si et seulement si $I(V)$ est un idéal premier.*

PREUVE : Supposons V irréductible et soit $fg \in I(V)$. Soit $V_1 = V \cap V(f)$ et $V_2 = V \cap V(g)$. Comme $fg \in I(V)$, on a $V = V_1 \cup V_2$ donc $V = V_1 = V \cap V(f)$ et f s'annule sur V et $f \in I(V)$.
Réciproquement si $I(V)$ est premier. Soit $V = V_1 \cup V_2$. Si $V \neq V_1$, montrons que $I(V) = I(V_2)$. Comme $V_2 \subset V$, on a $I(V) \subset I(V_2)$. Par ailleurs $I(V) \not\subset I(V_1)$. Soit $f \in I(V_1) - I(V)$ et $g \in V(I_2)$. On a $fg \in I(V)$. Donc f ou $g \in I(V)$. Donc $g \in I(V)$. D'où $I(V) = I(V_2)$ et $V = V_2$. ∎

Corollaire 6.1.4 *Si k est algébriquement clos I et V sont des correspondances 1-1 entre les variétés affines irréductibles et les idéaux premiers.*

Remarque 6.1.5 *Un idéal premier est radical.*

Nous avons vu comment resoudre les systèmes d'équations polynômiales grâce aux théorèmes d'élimination et d'extension.

Exemple 6.1.6 • *Soit le système*

$$\begin{cases} x+y+z=1 \\ x+2y-z=3 \end{cases}$$

Le théorème d'élimination permet de le mettre sous la forme

$$\begin{cases} x+3z=-1 \\ y-2z=2 \end{cases}$$

et donc d'obtenir les solutions paramétrées par z.
• *Le cercle $x^2+y^2=1$ est paramétré par $x=\frac{1-t^2}{1+t^2}$, $y=\frac{2t}{1+t^2}$. Il manque le point $(-1,0)$ dans cette paramétrisation.*

Réciproquement, nous nous interessons à présent aux systèmes paramétrés :

$$\begin{cases} x_1 = f_1(t_1,\dots,t_m) \\ x_2 = f_2(t_1,\dots,t_m) \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x_n = f_n(t_1,\dots,t_m) \end{cases}$$

Deux questions naturelles se posent à présent :
- Quelle est la variété algébrique minimale qui contient les solutions de ce système ? Autrement dit, comment rendre les équations implicites ?
- Quelle est le sous-ensemble de cette variété qui n'est pas atteint par la paramétrisation ?
C'est encore les bases de Gröbner et les théorèmes d'extension, de fermeture et d'élimination qui vont nous permettre de répondre à ses questions.

6.2 Résolution d'équations implicites

Soit

$$\begin{cases} x_1 = f_1(t_1, \dots, t_m) \\ x_2 = f_2(t_1, \dots, t_m) \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x_n = f_n(t_1, \dots, t_m) \end{cases}$$

un système paramétré, où $f_i \in k[t_1, \dots, t_m]$. Notons

$$F : k^m \to k^n, \;\; F(t_1, \dots, t_m) = (f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)).$$

Le système définit une variété algébrique de k^{n+m} via

$$V = V(x_1 - f_1, \dots, x_n - f_n)$$

Les points de V correspondent au graphe de la fonction F : $(t_1, \dots, t_m, f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m$
Nous avons la projection

$$\pi_m : k^{m+n} \to k^n, \; (t_1, \dots, t_m, x_1, \dots, x_m) \mapsto (x_1, \dots, x_n).$$

et nous nous interessons donc à l'image $F(k^n) = \pi_m(V)$. Les théorèmes d'élimination et de fermeture permettent donc de déterminer la plus petite variété contenant $F(k^n)$.

Théorème 6.2.1 *Soit $k \subset \mathbf{C}$ un corps, soit $F : k^m \to k^n$ la fonction définie par le système $(*)$. Soit I l'idéal $I =< x_1 - f_1, \dots, x_n - f_n > \subset k[t_1, \dots, t_m, x_1, \dots, x_n]$ et soit $I_m = I \cap k[x_1, \dots, x_n]$ le m-ème idéal d'élimination. Alors $V(I_m)$ est la plus petite variété de k^n contenant $F(k^m)$.*

Preuve : Si $k = \mathbf{C}$, $F(\mathbf{C}^m) = \pi_m(V)$ et d'après le théorème de fermeture, $V(I_m)$ est la plus petite variété contenant $\pi_m(V)$.
Soit k un sous-corps de $\mathbf{C}$. Ainsi $\mathbf{Z} \subset k$ et k est infini. On note V_k et $V_{\mathbf{C}}$ les variétés dans k et dans $\mathbf{C}$. Par définition, nous avons toujours $F(k^m) = \pi_m(V_k) \subset V_k(I_m)$. Soit $Z_k = V_k(g_1, \dots, g_s) \subset k^n$ une variété de k^n telle que $F(k^m) \subset Z_k$. Nous devons montrer

que $V_k(I_m) \subset Z_k$.
Remarquons d'abord que $g_i = 0$ sur Z_k, donc $g_i = 0$ sur $F(k^m)$. Donc $g_i \circ F$ s'annule sur k^m. Or $g_i \subset k[x_1, \ldots, x_n]$ et $F = (f_1, \ldots, f_n)$ avec $f_i \in k[t_1, \ldots, t_m]$. Donc $g_i \circ F \in k[t_1, \ldots, t_m]$. Comme k est infini, nous avons $g_i \circ F = 0$. Donc $g_i \circ F$ s'annule sur $\mathbf{C}^m$ donc les g_i s'annulent sur $F(\mathbf{C}^m)$. Donc $Z_{\mathbf{C}} = V_{\mathbf{C}}(g_1, \ldots, g_s)$ est une variété de $\mathbf{C}^n$ contenant $F(\mathbf{C}^m)$. Donc $V_{\mathbf{C}}(I_m) \subset Z_{\mathbf{C}}$. Si nous ne regardons que les solutions à valeurs dans k^n, nous obtenons $V_k(I_m) \subset Z_k$. ∎

Remarque 6.2.2 *Ce théorème donne un algorithme pour rendre implicite le système* $(*)$. *En effet, nous calculons une base de Gröbner pour un ordre lexicographique tel que tous les* t_i *soient supérieurs aux* x_j. *Par le théorème d'élimination, nous obtenons une base de Grobner de* I_m *ne faisant pas intervenir* $t_1, \ldots, t_m$. *Enfin d'après le théorème précédent* $V(I_m)$ *est la plus petite variété contenant la paramétrisation.*

Le théorème précédent se généralise sans difficulté aux paramétrisations rationnelles et plus seulement polynômiales :

$$(**) \begin{cases} x_1 = \frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)} \\ x_2 = \frac{f_2(t_1,\ldots,t_m)}{g_2(t_1,\ldots,t_m)} \\ \quad\cdot \\ \quad\cdot \\ \quad\cdot \\ x_n = \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \end{cases}$$

avec $f_i, g_j \in k[t_1, \ldots, t_m]$. Notons

$$F : k^m - W \to k^n, \;\; F(t_1, \ldots, t_m) = \Big(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}\Big)$$

où $W = V(g_1 \ldots g_n)$ est l'ensemble des zéros de $g_1 \cdots g_n$. Il s'agit seulement de considérer l'idéal $I =< g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - g_1 \cdots g_n y >\in k[y, t_1, \ldots, t_m, x_1, \ldots, t_n]$. La variable y est introduite pour interdire l'annulation des dénominateurs. Le résultat obtenu s'énonce alors :

Théorème 6.2.3 *Soit $k \subset \mathbf{C}$ un corps, soit $F : k^m - W \to k^n$ la fonction définie par le système $(**)$. Soit J l'idéal $< g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - g_1 \cdots g_n y > \subset k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ et soit $J_{m+1} = J \cap k[x_1, \ldots, x_n]$ le $m+1$-ème idéal d'élimination. Alors $V(J_{m+1})$ est la plus petite variété de k^n contenant $F(k^m - W)$.*

6.3 Critère d'irréductiblité

Nous allons voir que les variétés définies par une paramétrisation sont irréductibles.

Proposition 6.3.1 *Soit $k \subset \mathbf{C}$ et $V \subset k^n$ une variété définie par une paramétrisation*

$$\begin{cases} x_1 = f_1(t_1, \ldots, t_m) \\ x_2 = f_2(t_1, \ldots, t_m) \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x_n = f_n(t_1, \ldots, t_m) \end{cases}$$

où $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$. Alors V est irréductible.

Preuve : Par définition V est la fermeture de Zariski de $F(k^m)$. En particulier, $I(V) = I(F(k^m)$.
Pour $g \in k[x_1, \ldots, x_n]$, $g \circ F \in k[t_1, \ldots, t_m]$:

$$g \circ F = g(f_1(t_1, \ldots, t_m), \ldots, (t_1, \ldots, t_m)).$$

Comme k est infini, $I(V) = I(F(k^m))$ est l'ensemble des polynômes de $k[x_1, \ldots, x_n]$ donc la composition par F donne le polynôme nul de $k[t_1, \ldots, t_m]$:

$$I(V) = \{g \in k[x_1, \ldots, x_n], g \circ F = 0\}.$$

Montrons à présent que $I(V)$ est premier. Soit $gh \in I(V)$. Ainsi $gh \circ F = (g \circ F)(h \circ F) = 0$. Or $k[t_1, \ldots, t_m]$ est intègre, donc $g \circ F$ ou $h \circ F$ est nul. Donc g ou h appartient à $I(V)$. Donc $I(V)$ est premier et V est irréductible. ∎

Le résultat précédent s'étend aux variétés définies par des paramétrisations rationnelles :

Proposition 6.3.2 *Soit $k \subset \mathbf{C}$ et V la variété définie par*

$$\begin{cases} x_1 = \frac{f_1(t_1,\dots,t_m)}{g_1(t_1,\dots,t_m)} \\ x_2 = \frac{f_2(t_1,\dots,t_m)}{g_2(t_1,\dots,t_m)} \\ \quad\vdots \\ x_n = \frac{f_n(t_1,\dots,t_m)}{g_n(t_1,\dots,t_m)} \end{cases}$$

avec $f_i, g_j \in k[t_1, \dots, t_m]$. Alors V est irréductible.

PREUVE : Soit $W = V(g_1 \cdots g_n)$ et

$$F : k^m - W \to k^n, \ \ (t_1, \dots, t_m) \mapsto \left(\frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \dots, \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)}\right)$$

La variété V est la fermeture de Zariski de $F(k^m - W)$. Ainsi $I(V)$ est l'ensemble des $h \in k[x_1, \dots, x_n]$ tels que $h \circ F$ est nul sur tous les $(t_1, \dots, t_m) \in k^m - W$. La difficulté ici, provient du fait que $h \circ F$ n'est plus un polynôme, nous ne pouvons pas conclure directement comme dans la proposition précécente.
Donnons un nouveau critère pour déterminer si $h \in I(V)$. Rappelons que

$$g_1(t_1, \dots, t_m) \cdots g_n(t_1, \dots, t_m) \neq 0$$

pour tout $(t_1, \dots, t_m) \in k^m - W$. La condition $(g_1 \cdots g_n)^N (h \circ F) = 0$ est donc équivalente à $h \circ F = 0$ sur $k^m - W$. Or si N est le degré total de $h \in k[x_1, \dots, x_n]$, $(g_1 \cdots g_n) h \circ F$ est un polynôme de $k[t_1, \dots, t_m]$ et ce polynôme est nul sur $k^m - W$ si et seulement si il est nul sur k^m (fg est nul sur k^m donc nul et k^m est intègre donc $f = 0$). Ainsi

$$h \in I(V) \Longleftrightarrow (g_1 \cdots g_n)(h \circ F) = 0 \in k[t_1, \dots, t_m].$$

Montrons à présent que $I(V)$ est premier. Soit $pq \in I(V)$, et N, M les degrés totaux de $p, q \in k[x_1, \dots, x_n]$. Nous avons

$$(g_1 \cdots g_n)^{N+M} (p \circ F)(q \circ F) = 0 \in k[t_1, \dots t_m]$$

Donc p ou $q \in I(V)$.

■

6.4 Décomposition d'une variété en sous-variétés irréductibles

Lemme 6.4.1 *Toute suite décroissante de variétés de k^n est stationnaire.*

PREUVE : Soit $\cdots \subset V_2 \subset V_1$ une suite croissante de variétés de k^n. Soit $I(V_1) \subset I(V_2) \subset \cdots$ la suite croissante des idéaux associés. Comme $k[x_1, \ldots, x_n]$ est noetherien, cette suite est stationnaire. ∎

Théorème 6.4.2 *Soit $V \subset k^n$ une variété affine. Alors V est réunion finie $V = V_1 \cup \cdots \cup V_m$ de variétés affines V_i irréductibles.*

PREUVE : Raisonnons par l'absurde. Supposons que V ne puisse pas s'écrire comme réunion finie de variétés irréductibles. Alors V n'est pas irréductible et $V = V_1 \cup V_1'$ où $V \neq V_1$ et $V \neq V_1'$ et V_1 ou V_1' n'est pas réunion finie de variétés irréductibles. Nous construisons ainsi par récurrence une suite infinie strictement décroissante de variétés qui ne sont pas réunion finie de variétés irréductibles. Ce qui est absurde car tout suite décroissante de variétés est stationnaire. ∎

Exemple 6.4.3 • *$V(xz, yz)$ est union de l'axe des z ($V(x, y)$) et le plan xy ($V(z)$) qui sont deux variétés irréductibles.*

Nous allons montrer qu'en général la décomposition en variétés irréductibles est unique à l'ordre près pourvu qu'on interdise à une variété irréductible d'apparaître deux fois ou d'être incluse dans une autre.

Définition 6.4.4 *Soit $V \subset k^n$ une variété affine. La décomposition en variétés irréductibles*

$$V = V_1 \cup \cdots \cup V_m,$$

est dite **minimale** *si $V_i \not\subset V_j$ pour $i \neq j$*

Théorème 6.4.5 *Soit $V \subset k^n$ une variété affine. Alors V a une décomposition minimale*

$$V = V_1 \cup \cdots \cup V_m$$

où tous les V_i sont irréductibles et $V_i \not\subset V_j$ si $i \neq j$. De pls cette décomposition est unique à l'ordre des facteurs près.

PREUVE : La variété V s'écrit comme réunion finie de variétés irréductibles : $V = \cup V_i$.
Si $V_i \subset V_j$ on peut supprimer V_i et ainsi se ramener à une décomposition minimale.
Soit $V = V_1' \cup \cdots \cup V_r'$ une autre décomposition minimale. Pour tout i

$$V_i = V_i \cap V = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_r').$$

Comme V_i est irréductible, il existe j avec $V_i = V_i \cap V_j' \subset V_j'$. Le même argument appliqué à v_j' montre l'existence de k avec $V_j' \subset V_k$ et par minimalité des décompositions, $V_j' = V_i$. Donc tous les V_i apparaissent dans le décomposition $V = V_1' \cup \cdots \cup V_r'$. D'où $m \leq r$. Le même raisonnement sur les V_j' montre l'uncité de la décomposition à l'ordre près. ∎

7 Dimension d'une variété affine

7.1 Cas monomial

Nous commençons par définir la notion de dimension pour les variétés définies par les idéaux monomiaux.

Exemples 7.1.1 • *Soit $I =< x^2y, x^3 >$ un idéal monomial dans $k[x, y]$. La variété $V(I) = V(x^2y) \cap V(x^3) = H_{x=0}$ est composée de l'axe des y. C'est un k-espace vectoriel de dimension 1. La variété est dite de dimension 1.*
• *Soit $I =< y^2z^3, x^5z^4, x^2yz^2 >$, $V(I) = H_{z=0} \cup H_{xy=0}$, réunion de la droite $\{x = y = 0\}$ et du plan $\{z = 0\}$. La dimension de cette variété est 2.*
Dans ces exemples, la variété était réunion de sous-espaces vectoriels coordonnées (correspondant à l'annulation de certaines coordonnées) de k^n et sa dimension correspondait à la dimension du plus grand sous-espace vectoriel. Nous allons généraliser ces remarques.

Proposition 7.1.2 *Soit I un idéal monomial de $k[x_1, \ldots, x_n]$. Alors $V(I)$ est une réunion finie de sous-espaces vectoriels coordonnées de k^n.*

PREUVE : Soit le monôme $x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r} \in k[x_1, \ldots, x_n]$ avec $\alpha_i > 0$. Alors

$$V(x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r}) = H_{x_{i_1}} \cup \cdots \cup H_{x_{i_r}}$$

où $H_{x_{i_j}} = V(x_{i_j})$. Donc une variété définie par un monôme est réunion finie d'hyperplans de k^n.
Une variété définie par un ordre monomial est donc intersection finie de réunion finie d'hyperplans de k^n, donc (par distributivité de l'intersection par rapport à la réunion) réunion finie d'intersections d'hyperplans. Enfin une intersection d'hyperplans donne un sous-espace vectoriel coordonnée de k^n. ∎

Remarque 7.1.3 *La décomposition minimale en sous-espaces vectoriels coordonnées est unique à l'ordre des facteurs près.*

Définition 7.1.4 *Soit V une variété réunion de sous-espaces linéaires de k^n. Alors la* **dimension** *de V, notée dim$V$ est la plus grande des dimensions des sous-espaces.*

Nous avons un algorithme pour déterminer la dimension d'une variété définie par un ordre monomial :

Proposition 7.1.5 *Soit $I =< m_1, \ldots, m_r >$ un idéal monomial. Soit*

$M_j = \left\{k \in \{1, \ldots, n\}, x_k | m_j\right\}$, $1 \leq j \leq r$ *et* $N = \left\{J \subset \{1, \ldots, k\}, J \cap M_j \neq \emptyset, \forall 1 \leq j \leq r\right\}$.

Alors dim$V(I) = n - \min(|J|, J \in N)$.

PREUVE : Soit $J = \{i_1, \ldots, i_r\} \in N$ avec $|J| = r$ minimal. Alors tout monôme m_j contient une puissance d'un x_{i_k}. Donc le sous-espace coordonnée $W = V(x_{i_1}, \ldots, x_{i_r}) \subset V$. Donc dim$V \geq n - |J|$.
Si dim$V > n - |J|$ alors V contient un sous-espace coordonnée $W' = V(x_{j_1}, \ldots, x_{j_s})$ avec $r > s$. Chaque monôme m_j s'annule sur W', donc un x_{j_k} divise m_j donc $J' = \{x_{j_1}, \ldots, x_{j_s}\} \in N$ ce qui exclut la minimalité de r. ∎

Pour définir la dimension d'une variété affine en gén éral, nous avons besoin d'un travail préliminaire sur les idéaux monomiaux. Il s'agit de déterminer les monômes de degré total majoré qui n'appartiennent pas à un idéal monomial donné.

Exemple 7.1.6 *Soit I un idéal monomial propre de $k[x,y]$ (distinct de $k[x,y]$). Alors*
• *$V(I) = \{(0,0)\}$. Dans ce cas $\exists a, b$ avec $x^a \in I$ et $y^b \in I$. On peut supposer a, b minimaux. Le nombre de monômes qui ne sont pas dans I sont donc en nombre fini $\leq ab$ (dessin sous escalier inclus dans le rectangle ab).*
• *$V(I) = H_x$ ou $V(I) = H_y$ l'axe des y ou l'axe des x. Alors si axe des x $y^b \in I$ mais aucune puissance de x n'appartient à I (dessin escalier borne en b et ouvert en x). Infinité de monômes n'appartenant pas à I.*
• *$V(I)$ est la réunion des axes des x et des y. (dessin escalier ouvert en x et y). Infinité de monômes n'appartenant pas à I.*

Pour discuter le cas général, nous avons besoin de notations. Soit I un idéal monomial de $k[x_1, \ldots, x_n]$, notons

$$C(I) = \{\alpha \in \mathbf{N}^n : x^\alpha \notin I\}$$

et $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ le n-uplet où tous les éléments sont nuls sauf le i-ème qui vaut 1. Ainsi les éléments de $\mathbf{N}^n$ s'écrivent sous la forme $\alpha = \sum_{i=1}^n \alpha_i e_i$. Pour $i_1 < \cdots < i_r$, notons le sous-espace coordonnée de dimension r.

$$[e_{i_1}, \ldots, e_{i_r}] = \{\alpha_1 e_{i_1} + \cdots + \alpha_r e_{i_r} \in \mathbf{N}^n\},$$

et son translaté par $\alpha \in \mathbf{N}^n$:

$$\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta \in [e_{i_1}, \ldots, e_{i_r}]\}.$$

Proposition 7.1.7 *Soit $I \subset k[x_1, \ldots, x_n]$ un idéal monomial propre.*
i. Le sous-espace coordonnée $V(x_i, i \notin \{i_1, \ldots, i_r\})$ est contenu dans $V(I)$ si et seulement si $[e_{i_1}, \ldots, e_{i_r}] \subset C(I)$.
ii. La dimension de $V(I)$ est la dimension du plus grand sous-espace coordonnée dans $C(I)$.

PREUVE : i. $W = V(x_i, i \notin \{i_1, \ldots, i_r\})$ contient le point p ayant pour coordonnée 1 pour $1 \leq j \leq r$ et O sinon. Pour tout $\alpha \in [e_{i_1}, \ldots, e_{i_r}]$, le monôme $x^\alpha = x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r}$ qui vaut 1 en p donc $x_n^\alpha ot \in I$. Donc $\alpha \in C(I)$.
Réciproquement si $[e_{i_1}, \ldots, e_{i_r}] \subset C(I)$, comme I est propre, chaque monôme de I contient au moins une autre variable que $x_{i_1}, \ldots, x_{i_r}$. Donc tous les monômes de I s'annulent aux points $(a_1, \ldots, a_n)$ qui ont une coordonnée $a_i = 0$ avec $i \notin \{i_1, \ldots, i_r\}$. Ainsi tous les monômes de I s'annulent sur $V(x_i, i \notin \{i_1, \ldots, i_r\})$ qui est donc inclus dans $V(I)$.
ii. L'espace $V(x_i, i \notin \{i_1, \ldots, i_r\})$ est de dimension r. D'après i., les dimensions des sous-espaces coordonnées de k^n inclus dans $V(I)$ et les dimensions des sous-espaces coordonnées dans $\mathbf{N}^n$ sont les mêmes. Comme $\dim V(I)$ est le maximum de ces dimensions, $\dim V(I)$ est le maximum des dimension des sous-espaces coordonnés dans $C(I)$. ∎

Nous pouvons à présent décrire le complémentaire d'un idéal monomial.

Théorème 7.1.8 *Soit $I \subset k[x_1, \ldots, x_n]$ un idéal monomial propre. L'ensemble $C(I) \subset \mathbf{N}^n$ des exposants des monômes qui n'appartiennent pas à I est réunion finie de sous-espaces coordonnées de N^n.*

PREUVE : Si $I = (0)$ c'est clair. Supposons $I \neq (0)$. La preuve s'effectue par réccurence sur le nombre de variables n. Si $n = 1$ alors $I(x^k)$ et $C(I) = \{0, 1, \ldots, k-1\}$ est réunion finie de points.
Supposons le résultat établi pour $n-1$ variables. Pour tout $j \geq 0$, soit $I_j =< m | m x_n^j \in I$. Ainsi $C(I_j)$ correspond aux $\alpha \in N^{n-1}$ tels que $x^\alpha x_n^j \notin I$. Donc $C(I_j)$ est l'intersection de $C(I)$ avec l'hyperplan $(0, \ldots, 0, j) + [e_1, \ldots, e_{n-1}]$.
Nous construisons ainsi une suite croissante d'idéaux I_j donc stationnaire à I_{j_0}. Montrons que

$$C(I) = (C(I_{j_0} \times N) \cup \cup_{j=0}^{j_0 - 1} (C(I_j) \times \{j\}).$$

L'inclusion dans $C(I)$ est claire.
Pour $\subset$, soit $\alpha = (\alpha_1, \ldots, \alpha_n) \in C(I)$. Ainsi $\alpha \in C(I_{\alpha_n}) \times \{\alpha_n\}$ et nous concluons. Ensuite la récurrence conclut. ∎

Il s'agit à présent de déterminer le nombre de monômes de degré total $\leq s$ de $C(I)$.

Lemme 7.1.9 *Le nombre de points de* $\alpha+[e_{i_1},\dots,e_{i_n}]$ *degré total* $\leq s > |\alpha|$ *est* $\binom{n+s-|\alpha|}{s-|\alpha|}$. *C'est une fonction polynôme en* s *de degré* m *et de coefficient dominant* $1/m!$.

PREUVE : Il s'agit de compter le nombre de monômes de la forme $\alpha+\gamma$ avec $\gamma \in [e_{i_1},\dots,e_{i_n}]$ et $|\gamma| \leq s-|\alpha|$. ∎

Théorème 7.1.10 *Si* $I \subset k[x_1,\dots,x_n]$ *est un idéal monomial avec* $\dim V(I) = d$, *alors pour* s *assez grand, le nombre de monômes de degré total* $\leq s$ *qui ne sont pas dans* I *est un polynôme de degré* d *en* s. *de plus le coefficient de* s^d *est positif.*

PREUVE : On sait que l'ensemble $C(I) \subset \mathbf{N}^n$ est réunion finie de sous-espaces coordonnées de N^n :

$$C(I) = T_1 \cup T_2 \cup \cdots \cup T_t,\ mboxavecT_i \neq T_j, i \neq j.$$

La dimension d'un T_i est la dimension du sous-espace coordonnée associé. Donc $\dim T_i \leq d$ avec égalité pour au moins un i. Notons $C(I)^s$ (resp. T_j^s) le sous-ensemble de $C(I)$ (resp. T_j) des éléments de degré total $\leq s$. Ainsi, par le principe d'inclusion-exclusion,

$$|C(I)|^s = |T_1^s \cup \cdots \cup T_t^s| = \sum_{1\leq r\leq t} \sum_{1\leq i_1<\cdots<i_r\leq t} (-1)^{r+1} |T_{i_1}^s \cap \cdots \cap T_{i_r}^s|$$

Or l'intersection de deux sous-espaces coordonnés distincts de dimension respective d_1, d_2 est un sous-espace coordonnée vide ou de dimension strictement inférieur à $\max(d_1,d_2)$. Ainsi le nombres de points des $|T_{i_1}^s \cap \cdots \cap T_{i_r}^s|$ est un polynôme en s de degré $< d$ si $r > 1$. Ainsi $|C(I)^s|$ est un polynôme en s de degré d et de coefficient dominant $r'/d!$ où r' est le nombre de T_i de dimension d. ∎

7.2 Dimension d'une variété affine. Fonction de Hilbert

Définition 7.2.1 *Soit I un idéal de $k[x_1, \ldots, x_n]$. Pour $s \in \mathbf{N}$, on note $I_{\leq s} = I \cap k[x_1, \ldots, x_n]_{\leq s}$. La fonction de Hilbert affine de I est la fonction de $s \in \mathbf{N}$ définie par*

$$^aHF_I(s) = \dim_k k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} = \dim_k k[x_1, \ldots, x_n]_{\leq s} - \dim_k I_{\leq s}.$$

Proposition 7.2.2 *Soit I un idéal monomial propre de $k[x_1, \ldots, x_n]$.*
i. Pour tout $s \geq 0$, $^aHF_I(s)$ est le nombre de monômes de degré total $\leq s$ qui n'appartiennent pas à I.
ii. Pour s assez grand, la fonction affine de Hilbert de I est donné par un polynôme de la forme

$$^aHF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

où $b_i \in \mathbf{Z}$ et $b_0 \in \mathbf{N}^*$.
iii. Le degré de $^aHF_I(s)$ pour s assez grand est le maximum des dimensions des sous-espaces coordonnées contenus dans $V(I)$.

Pour définir la dimension d'une variété affine définie par un idéal quelconque, on se ramène au cas monômial grâce à la proposition suivante :

Proposition 7.2.3 *Soit I un idéal de $k[x_1, \ldots, x_n]$ muni d'un ordre admissible gradué, i.e. tel que $x^\alpha \geq x^\beta$ si $|\alpha| > |\beta|$. Alors les idéaux I et $< \mathrm{LT}(I) >$ ont les mêmes fonctions affines de Hilbert.*

Preuve : L'ensemble des monômes dominants de I_s est fini, on l'ordonne par $\mathrm{LM}(f_1) > \cdots > \mathrm{LM}(F_m$ pour des $f_i \in I_S$. Montrons que les f_i pour $1 \leq i \leq m$ forment une base du k-espace vectoriel $I_{\leq s}$. C'est en effet une famille libre car si $a_1 f_1 + \cdots + a_m f_m = 0$ avec i_0 minimum tel que $a_{i_0} \neq 0$. Alors $\mathrm{LT}(a_1 f_1 + \cdots + a_m f_m) = \mathrm{LT}(a_{i_0} f_{i_0}) \neq 0$, absurde ! La famille est génératrice : Soit W le sous-k-espace vectoriel de $I_{\leq s}$ engendré par les f_i pour $1 \leq i \leq m$. Si $W \neq I_{\leq s}$, prnons un $f \in I_{\leq s} - W$ avec $\mathrm{LM}(f)$ minimal . Comme $\mathrm{LM}(f) = \mathrm{LM}(f_i)$, il existe $\lambda \in k^*$ tel que $f - \lambda f_i \in I_{\leq s}$ ce qui contredit la minimalité de $\mathrm{LM}(f)$.

Par ailleurs $LM(f_i) \in < LT(I) >_{\leq s}$. Montrons que les $\mathrm{LM}(f_i)$ forment une base de $< LT(I) >$. Ils sont linéairement indépendants (même preuve qu'avant) et

$$\{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\} = \{\mathrm{LM}(f), f \in I_{\leq s}\}$$

car $>$ est un ordre gradué donc $\mathrm{LM}(f)$ a le même degré que f.
Ainsi $I_{\leq s}$ et $> LT(I) >_{\leq s}$ ont la même dimension et

$${}^aHF_I(s) = \dim_k k[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} = \dim_k k[x_1, \ldots, x_n]_{\leq s}/ < \mathrm{LT}(I) >_{\leq s} = {}^a HF_{<\mathrm{LT}(I)>}(s).$$

∎

Nous montrerons en TD :

Lemme 7.2.4 *Si $I_1 \subset I_2$, $\deg^a HP_{I_1} \geq \deg^a HP_{I_2}$.*

Définition 7.2.5 *Le polynôme qui s'identifie à ${}^aHF_I(s)$ pour s assez grand est dit polynôme de Hilbert de I et est noté ${}^aHP_I(s)$.*
La dimension de la variété affine $V \subset k^n$ est le degré du polynôme de Hilbert de l'idéal $I(V)$.

Cette définition a une signification géométrique car

Proposition 7.2.6 *Soit $I \subset k[x_1, \ldots, x_n]$ un idéal. Alors les polynômes de Hilbert de I et $\sqrt{I}$ ont même degré*

Preuve : Pour un idéal monomial, on sait que le degrd́u polynôme affine de Hilbert est la dimension du plus grand sous-espace coordonnée de k^n contenu dans $V(I)$. Comme $V(I) = V(\sqrt{I})$ les polynômes ${}^aHP_I$ et ${}^aHP_{\sqrt{I}}$ ont même degré.
Soit $I \subset k[x_1, \ldots, x_n]$ un id{eal quelconque et $>$ un ordre gradué. Montrons que

$$< \mathrm{LT}(I) > \subset < \mathrm{LT}(\sqrt{I}) > \subset \sqrt{< \mathrm{LT}(I) >}$$

La première inclusion provient de $I \subset \sqrt{I}$. Pour montrer la seconde, soit $x^\alpha \in < \mathrm{LT}(\sqrt{I}) >$. Ainsi il existe $f \in \sqrt{I}$ avec $\mathrm{LT}(f) = x^\alpha$. Donc il existe $r \geq 1$ tel que $f^r \in I$ et $x^{r\alpha} \in <$

$\mathrm{LT}(I)>$. Donc $x^\alpha \in \sqrt{<\mathrm{LT}(I)>}$.
Ainsi

$$\deg^a HP_{\sqrt{<\mathrm{LT}(I)>}} \leq \deg^a HP_{<\mathrm{LT}(\sqrt{I})>} \leq \deg^a HP_{<\mathrm{LT}(I)>}.$$

Comme $\deg^a HP_{\sqrt{<\mathrm{LT}(I)>}} = \deg^a HP_{<\mathrm{LT}(I)>}$, $\deg^a HP_{<\mathrm{LT}(\sqrt{I})>} = \deg^a HP_{<\mathrm{LT}(I)>}$ et $\deg^a HP_I = \deg^a HP_{\sqrt{I}}$. ∎

Théorème 7.2.7 *Soit $V = V(I)$ une variété affine pour I un idéal de $k[x_1, \ldots, x_n]$. Si k est algébriquement clos, alors*

$$\dim V = \deg^a HP_I.$$

Si de plus $>$ est un ordre gradué sur $k[x_1, \ldots, x_n]$, alors

$$\dim V = \deg^a HP_{<\mathrm{LT}(I)>}$$

$\dim V =$ *dimension maximale des sous-espaces coordonnés inclus dans* $V(<\mathrm{LT}(I)>)$

Les deux dernières égalités sont vrais pour n'importe quel corps k pour $I = I(V)$.

PREUVE : Si k est algébriquement clos $I(V) = I(V(I)) = \sqrt{I}$. ∎

Et à présent le lien avec la définition donnée dans le cours sur les courbes algébriques. On rappelle que des éléments $y_1, \ldots, y_r \in k[V] = k[x_1, \ldots, x_n]/I$ sont dits algébriquement indépendants s'il n'existe aucun polynôme non nul en r variables à coefficients dans k tel que $p(y_1, \ldots, y_r) = 0 \in k[V]$.

Théorème 7.2.8 *Soit $V \subset k^n$ une varété affine. La dimension de V est éagle au nombre maximum d'éléments de $k[V] = k[x_1, \ldots, x_n]/I(V)$ qui sont algébriquement indépendants.*

PREUVE : Soit $d = \dim V$. Montrons qu'il existe d éléments de $k[V]$ algébriquement indépendants. Posons $I = I(V)$. Pour un ordre gradué fixé, d est donc la dimension maximale des sous-espaces coordonnées inclus dans $V(< \mathrm{LT}(I) >)$. Ainsi il existe $W = V(x_j, j \notin \{i_1, \ldots, i_d\}) \subset V(\mathrm{LT}(I))$. • Montrons que $\overline{x_{i_1}}, \ldots, \overline{x_{i_d}}$ sont algébriquement indépendants dans $k[V]$. Soit $p = (p_1, \ldots, p_n) \in k^n$ avec $p_i = 0$ si $i \neq \{i_1, \ldots, i_d\}$ et $p_i = 1$ si $i \in \{i_1, \ldots, i_d\}$. Comme $p \in W \subset V(< \mathrm{LT}(I) >)$, les monômes de $< \mathrm{LT}(I) >$ font tous intervenir au moins un x_i pour $i \notin \{i_1, \ldots, i_d\}$. Ainsi $< \mathrm{LT}(I) > \cap k[x_{i_1}, \ldots, x_{i_d}] = \{0\}$ et $I \cap k[x_{i_1}, \ldots, x_{i_d}] = \{0\}$.
Supposons qu'il existe un polynôme $P \in k[y_1, \ldots, y_d]$ tel que $P(\overline{x_{i_1}}, \ldots, \overline{x_{i_d}}] = 0 \in k[V]$. Alors $p(x_{i_1}, \ldots, x_{i_d}) \in I \cap k[x_{i_1}, \ldots, x_{i_d}]$. Donc $p = 0$ et $x_{i_1}, \ldots, x_{i_d}$ sont algébriquement indépendants.
• Soit $\overline{f_1}, \ldots, \overline{f_r}$ r éléments algébriquement indépendants dans $k[V]$. Soit N le plus grand degré total des f_i. Si le degré total de $P \in k[y_1, \ldots, y_r]$ est $\leq s$, alors le degré total de $P(f_1, \ldots, f_r)$ est inférieur à Ns. On a donc une application k-linéaire

$$\alpha : k[y_1, \ldots, y_r]_{\leq s} \to k[x_1, \ldots, x_r]_{\leq Ns}/I_{\leq Ns},\ P(y_1, \ldots, y_r) \mapsto \overline{P(f_1, \ldots, f_r)}.$$

L'application α est injective car

$$\overline{P(f_1, \ldots, f_r)} = P(\overline{f_1}, \ldots, \overline{f_r}) \in k[V]$$

et $\overline{f_1}, \ldots, \overline{f_r}$ sont algébriquement indépendants donc $\overline{P(f_1, \ldots, f_r)} = 0$ implique $P = 0$. Donc

$${}^aHF_I(Ns) = \dim_k k[x_1, \ldots, x_n]_{\leq NS}/I_{\leq Ns} \geq \dim_k k[y_1 \ldots, y_r]_{\leq s} = \binom{r+s}{s}.$$

Donc ${}^aHP_I(Ns)$ est plus grand qu'un polynôme de degré r en s pour tout s assez grand. donc $\deg^a HP_I(NS) \geq r$ et $r \leq \dim V$. ∎

Théorème 7.2.9 *Soit $V \subset k^n$ une variété affine irréductible. Alors la dimension de V est égale au degré de transcendance de $k(V)$ sur k.*

PREUVE : Notons $d = \dim V$. Comme $k[V] \subset k(V)$, il existe d éléments de $k(V)$ qui sont algébriquement indépendants sur k. Soit $\phi_1, \ldots, \phi_r \in k(V)$ r éléments algébriquement indépendants. On les réduit au même dénominateur, ainsi il existe $\overline{f}, \overline{f_1}, \ldots, \overline{f_r} \in k[V]$, tel que $\phi_i = \overline{f_i}/\overline{f}$, $1 \leq i \leq r$. On définit l'application k-linéaire

$$\beta : k[y_1, \ldots, y_r] \to k[x_1, \ldots, x_r]_{\leq Ns}/I_{\leq Ns},\ P(y_1, \ldots, y_r) \mapsto \overline{f^s P(f_1/f, \ldots, f_r/f)}.$$

Montrons que β est injective. Dans le corps $k(V)$

$$\overline{f}^s P(\overline{f_1}/\overline{f}, \ldots, \overline{f_r}/\overline{f}) = \overline{f}^s P(\phi_1, \ldots, \phi_r)$$

comme $\overline{f}$ est inversible et les ϕ_i sont algébriquement indépendants, β est injective et $\dim V \geq r$. ∎

8 Caractéristique mixte

8.1 Bases de Gröbner sur un anneau

Dans ce paragraphe, R désigne un anneau noethérien et $A = R[x_1, \ldots, x_n]$.

Définition 8.1.1 *On dit que les équations linéaires sont résolubles dans R si les deux propriétés suivantes sont satisfaites :*
i. Etant donnés $a, a_1, \ldots, a_m \in R$, il existe un algorithme qui détermine si $a \in < a_1, \ldots, a_m >$ et si tel est le cas qui calcule $b_1, \ldots, b_m \in R$ tels que $a = b_1 a_1 + \cdots + a_m b_m$.
ii. Etant donnés $a_1, \ldots, a_m \in R$, il existe un algorithme qui détermine un ensemble de générateurs du module

$$\mathrm{Syg}_R(a_1, \ldots, a_m) = \{(b_1, \ldots, b_m) \in R^m | a_1 b_1 + \cdots + a_m b_m = 0\}.$$

Définition 8.1.2 *Soit $f, h, f_1, \ldots, f_s$ des polynômes de A avec $f_1, \ldots, f_s \neq 0$. Notons $F = \{f_1, \ldots, f_m\}$. On dit que f se réduit en h modulo F et on note $f \to^F h$, s'il existe des polynômes $h_1, \ldots, h_{t-1} \in A$ tels que*

$$f \to^F h_1 \to^F h_2 \to^F \cdots \to^F h_{t-1} \to^F h,$$

où $g \to^F g'$ si $\exists c_1, \ldots, c_s \in R$ et $\exists X_1 \ldots, X_s$ des produits de puissances de x_i tels que $g = g' - (c_1 X_1 f_1 + \cdots + c_s X_s f_s)$ avec $\mathrm{LM}(g) = X_i \mathrm{LM}(f_i)$ pour les i avec $c_i \neq 0$.

Définition 8.1.3 *Un polynôme r est dit minimal pour $F = \{f_1, \dots, f_s\}$ si r ne se réduit pas modulo F.*

Lemme 8.1.4 *Un polynôme $r \in A$ non nul est minimal pour $F = \{f_1, \dots, f_s\} \neq \{0\}$ si et seulement si $\mathrm{LT}(r) \notin < \mathrm{LT}(F) >$.*

PREUVE : Si r n'est pas minimal, alors on peut le réduire avec

$$\mathrm{LT}(r) = c_1 X_1 \,\mathrm{LT}(f_1) + \cdots + c_s X_s \,\mathrm{LT}(f_s), \text{ pour } c_i \in R.$$

Ainsi $\mathrm{LT}(r) \in LT(F)$.
Réciproquement si $\mathrm{LT}(r) \in \mathrm{LT}(F)$, alors il existe des polynômes $h_i \in A$ avec

$$\mathrm{LT}(r) = h_1 \,\mathrm{LT}(f_1) + \cdots + h_s \,\mathrm{LT}(f_s)$$

En regardant les monômes de cette équation, on observe que le seul produit de puissances qui peut intervenir avec un coefficient non nul est $\mathrm{LT}(r)$, donc chaque $h_i = c_i X_i$. Ainsi $r - (c_1 X_1 f_1 + \cdots + c_s X_s f_s)$ est une réduction de r. ∎

Théorème 8.1.5 *Soit $F = \{f_1, \dots, f_s\}$ une famille de polynômes non nuls de A et $f \in A$ non nul. Alors il existe un polynôme minimal pour F, $r \in A$, tel que $f \to^F r$. De plus il existe $h_1, \dots, h_s \in A$ satisfaisant*

$$f = h_1 f_1 + \cdots + h_s f_s + r$$

avec $\mathrm{LP}(f) = \max\Big(\max_{1 \leq i \leq s}(\mathrm{LP}(h_i)\,\mathrm{LP}(f_i)\Big), \mathrm{LP}(r))$. *Si les équations linéaires sont résolubles dans R, alors $h_1, \dots, h_s, r$ sont calculables.*

PREUVE : Par récurrence si f n'est pas minimal pour F, on construit une suite de r_i ($f \to^F r_1 \to^F r_2 \cdots$) avec $\mathrm{LP}(f) > \mathrm{LP}(r_1) > \mathrm{LP}(r_2) > \cdots$ Ainsi on obtient un r et des réductions $f - r_1 = c_{11} X_{11} + \cdots + c_{1s} X_{1s} f_s$ avec $c_{11}, \dots, c_{1s} \in R$ et $X_{11}, \dots, X_{1s}$ des puissances avec $\mathrm{LT}(f) = c_{11} X_{11} \,\mathrm{LT}(f_1) + \cdots + c_{1s} X_{1s}\ LT(f_s)$ et $\mathrm{LP}(f) = X_{1i} \,\mathrm{LP}(f_i)$ pour tout i avec $c_{1i} \neq 0$. De même pour $r_1 - r_2$ avec $\mathrm{LT}(r_1) = c_{21} X_{21} \,\mathrm{LT}(f_1) + \cdots c_{2s} X_{2s} \,\mathrm{LT}(f_s)$ et $\mathrm{LT}(r_1) = X_{2i} \,\mathrm{LP}(f_i)$, pour tout i avec $c_{2i} \neq 0$. Ainsi

$$f - r_2 = (c_{11} X_{11} + c_{21} X_{21}) f_1 + \cdots + (c_{1s} X_{1s} + c_{2s} X_{2s}) f_s.$$

Par récurrence, on conclut. ∎

Théorème 8.1.6 *Soit I un idéal de A et $G = \{g_1, \dots, g_t\}$ un ensemble de polynômes non nuls de I. Les propositions suivantes sont équivalentes :*
i. $\mathrm{LT}(G) = \mathrm{LT}(I)$,
ii. Pour tout polynôme $f \in A$,

$$f \in I \text{ ssi } f \to^G 0$$

iii. Pour tout $f \in I$, il existe une {ecriture de f sous la forme $f = h_1 g_1 + \cdots + h_t g_t$, avec $h_1, \dots, h_t \in A$ tels que $\mathrm{LP}(f) = \max_{1 \leq i \leq t} \Big(\mathrm{LP}(h_i)\,\mathrm{LP}(g_i)) \Big)$.

PREUVE : i.⇒ ii. Si $f \to^G 0$ alors $f \in I$. Réciproquement si $f \in I$, alors il existe r minimal avec $f \to^G r$. Si $r \neq 0$ alors $\mathrm{LT}(r) \notin \mathrm{LT}(G)$. Or $f, f - r \in I$ donc $r \in I$ donc $\mathrm{LT}(r) \in \mathrm{LT}(I) = \mathrm{LT}(G)$. Absurde !
ii.⇒ iii. C'est le cas particulier $r = 0$ dans le théorème 8.1.5.
iii.⇔ i. Soit $f \in I$, nous allons montrer que $\mathrm{LT}(f) \in \mathrm{LT}(G)$. Or $f = h_1 g_1 + \cdots + h_t g_t$ avec $\mathrm{LP}(f) = \max_{1 \leq i \leq t}(\mathrm{LP}(h_i)\,\mathrm{LP}(g_i))$. Ainsi $\mathrm{LT}(f) = \sum \mathrm{LT}(h_i)\,\mathrm{LT}(f_i)$ où la somme prote sur les i avec $\mathrm{LP}(f) = \mathrm{LP}(h_i)\,\mathrm{LP}(g_i)$. Donc $\mathrm{LT}(f) \in \mathrm{LT}(G)$. ∎

Définition 8.1.7 *Un ensemble de polynômes non nuls G inclus dans un idéal I est dit base de Gröbner pour I si G satisfait l'une des conditions du théorème 8.1.6.*

Exemple 8.1.8 *Soit $R = \mathbf{Z}$ et $A = \mathbf{Z}[x, y]$ muni de l'ordre deglex avec $x < y$. Soit $f_1 = 4x + 1$, $f_2 = 6y + 1$ et $I =< f_1, f_2 >$. Alors $3yf_1 - 2xf_2 = 3y - 2x \in I$ et $\mathrm{LT}(3y - 2x) = 3y \notin < \mathrm{LT}(f_1), \mathrm{LT}(f_2) >=< 4x, 6y >$. Donc $\{f_1, f_2\}$ n'est pas une base de Gröbner pour I.*
Soit $g_1 = 2x + 1$, $g_2 = 3y + 1$ et $I' =< f_1, f_2 >$. Alors $\mathrm{LT}(I') =< 2x, 3y, xy >=< 2x, 3y >=< \mathrm{LT}(g_1), \mathrm{LT}(g_2) >$. Donc $\{g_1, g_2\}$ est une base de Gröbner pour I'.

Remarque 8.1.9 *On peut déduire de cette définition, les propriétés analogues au cas $R = k$ un corps. On peut définir un analogue au critère de Buchberger.*

8.2 Rappel sur les limites projectives

Soit $(A_i)_i \in I$ un système projectif d'anneaux : pour tous $i, j, k \in I$ avec $i \leq j \leq k$, on a des morphismes d'anneaux $\varphi_{i,j} : A_j \to A_i$, tels que $\varphi_{i,i} = Id$, $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$. La limite projective de $(A_i)_i \in I$ est l'anneau A

$$A = \{(g_i) \in \Pi A_i, \forall i \leq j, g_i = \varphi_{i,j}(g_j)\}.$$

Il peut être défini par la propriété universelle suivante : si Y anneau avec morphismes compatibles dans les A_i, alors il existe un morphisme de $Y \to A$ qui induit tout.

Soit p un nombre premier pour $i \leq j$, la réduction mod p^i définit un morphisme d'anneaux $\mathbf{Z}/p^j\mathbf{Z} \to \mathbf{Z}/p^i\mathbf{Z}$ et fait de $(\mathbf{Z}/p^n\mathbf{Z})_{n\in\mathbf{N}^*}$ un système projectif.

Définition 8.2.1 *Soit p un nombre premier. L'anneau des entiers p-adiques $\mathbf{Z}_p$ est la limite projective des $\mathbf{Z}/p^n\mathbf{Z}$, $n \in \mathbf{N}^*$.*

8.3 Nombres p-adiques

Soit p un nombre premier. Pour tout rationnel $a \in \mathbf{Q}^*$, $a = p^r m/n$ avec $m, n \in \mathbf{Z}$ non divisibles par p. On définit $|a|_p = 1/p^r$ et $|0|_p = 0$. Alors

Lemme 8.3.1 *Soit $a \in \mathbf{Q}$.*
i. $|a|_p = 0$ *ssi* $a = 0$,
ii. $|ab|_p = |a|_p|b|_p$,
iii. $|a + b|_p \leq \max(|a|_p, |b|_p)$.
Ainsi $d_p(a, b) = |a - b|_p$ définit une métrique sur $\mathbf{Q}$.

Définition 8.3.2 *Le corps des nombres p-adiques $\mathbf{Q}_p$ est le complété de $\mathbf{Q}$ pour la métrique d_p.*
Les éléments de $\mathbf{Q}_p$ s'écrivent sous la forme

$$a_{-n}p^{-n} + \cdots + a_0 + a_1 p + \cdots + a_m p^m + \cdots, \quad 0 \leq a_i \leq p - 1.$$

L'anneau des entiers p-adiques est l'ensemble des éléments $\alpha \in \mathbf{Q}_p$ avec $|\alpha|_p \leq 1$, i.e. l'ensemble des éléments de $\mathbf{Q}_p$ qui s'écrivent sous la forme

$$a_0 + a_1 p + \cdots + a_m p^m + \cdots, \ 0 \leq a_i \leq p - 1.$$

8.4 Anneau des vecteurs de Witt

Soit A un anneau commutatif. On note $W(A)$ l'ensemble $A^{\mathbf{N}}$ des suites infinies à valeurs dans A. Les éléments de $W(A)$ sont dits vecteurs de Witt à coefficients dans A. A chaque morphisme d'anneaux $f : A \to B$, on associe l'application d'ensembles $W(f) : W(A) \to W(B)$, $(a_k)_k \mapsto (f(a_k))_k$. Ainsi W définit un foncteur de la catégorie des anneaux commutatifs dans la catégorie des ensembles.
A chaque vecteur $x = (x_k)_k$ de $W(A)$, on associe la suite $x^{(*)} = (x^{(k)})_k$ de $A^{\mathbf{N}}$ définie par :

$$\forall k \geq 0, x^{(k)} = x_0^{p^k} + px_1^{p^{k-1}} + \cdots + p^k x_k.$$

Les coefficients $x^{(k)}, k \geq 0$ de la suite $x^{(*)}$ sont dits composantes fantômes de x. On définit l'application

$$g_A : W(A) \to A^{\mathbf{N}}, \ \ (x_k)_k \mapsto (x^{(k)})_k$$

Proposition 8.4.1 *Si l'anneau A contient le corps $\mathbf{Q}$ des nombres rationnels, l'application g_A est bijective.*

Preuve : On a $x_0 = x^{(0)}$ et $x_1 = (x^{(1)} - x^{(0)^p})/p$. En suite pour $k \geq 1$, nous avons :

$$x_k = \frac{1}{p^k}(x^{(k)} - \sum_{0 \leq d \leq k-1} p^d x_d^{p^{n-d}}).$$

Ainsi chaque composante x_k s'écrit comme combinaison linéaire des $x^{(d)}$ avec $0 \leq d \leq k$ à coefficients rationnels. Donc g_A est bijective. ∎

Si A contient $\mathbf{Q}$, l'application g_A est bijective et nous posons

$$a \hat{+} b = g_A^{-1}(a^* + b^*) \text{ et } a \hat{\times} b = g_A^{-1}(a^* \times b^*).$$

Plus précisément, la somme et le produit sont définis comme les vecteurs de Witt dont les composantes fantômes sont donnés par :

$$\forall k \geq 0, (a \hat{+} b)^{(k)} = a^{(k)} + b^{(k)}, \ \ (a \hat{\times} b)^{(k)} = a^{(k)} \cdot b^{(k)}.$$

C'est en particulier le cas pour $R_{\mathbf{Q}} = \mathbf{Q}[X_0, X_1, \dots, Y_0, Y_1, \dots]$. On observe alors que l'addition et la multiplication définies sur $W(R_{\mathbf{Q}})$ n'utilisent que des coefficients entiers : notons

$$(X\hat{+}Y)_k = S_k(X_0, \dots, x_k, Y_0, \dots, Y_k), \text{ et } (X\hat{\times}Y)_k = P_k(X_0, \dots, X_k, Y_0, \dots, Y_k)$$

Proposition 8.4.2 *Pour tout $k \geq 0$, $S_k, P_k \in \mathbf{Z}[X_0, \dots, X_k, Y_0, \dots, Y_k]$.*

On va définir une addition et une multiplication sur $a, b \in W(A)$ pour A anneau commutatif. Pour cela, on introduit l'unique homomorphisme d'anneaux

$$\phi_{ab} : R_{\mathbf{Z}} \to A, X_k \mapsto a_k, Y_k \mapsto b_k, \forall k \in \mathbf{N}.$$

Définition 8.4.3 *Soit A un anneau commutatif. Pour tout $a, b \in W(A)$, on définit*

$$a\hat{+}b = W(\phi_{ab})(X\hat{+}Y),\ a\hat{\times}b = W(\phi_{ab})(X\hat{\times}Y)$$

Exemple 8.4.4

$$(a+b) = (a_0 + b, a_1 + b_1 - \sum_{k=1}^{p-1} 1/p \binom{p}{k} a_0^k b_0^{p-k}, \cdots)$$

$$(ab) = (a_0 b_0, a_1 b_0^p + a_0 b_1 + p a_1 b_1, \dots)$$

Nous avons la propriété fonctorielle (admis)

Proposition 8.4.5 *Soit A un anneau commutatif. Tous vecteurs de Witt a, b dans $W(A)$ satisfont les relations suivantes :*

$$g_A(a\hat{+}b) = g_A(a) + g_A(b),\ g_A(a\hat{\times}b) = g_A(a)g_A(b)$$

Proposition 8.4.6 *Soit A, B deux anneaux commutatifs. Si $f : A \to B$ est un morphisme d'anneaux, alors l'application induite :*

$$W(f) : W(A) \to W(B)$$

est additive et multiplicative pour les lois $\hat{+}$ et $\hat{\times}$.

Preuve :

$$W(f)(a\hat{+}b) = W(f \circ \phi_{ab})(X\hat{+}Y) = W(\phi_{W(f)(a),W(f)(b)})(X\hat{+}Y)$$

$$= W(\phi_{W(f)(a),W(f)(b)})(X)\hat{+}W(\phi_{W(f)(a),W(f)(b)})(Y) = W(f)(a) + W(f)(b)$$

de même pour le produit. ∎

Théorème 8.4.7 *Soit A un anneau commutatif. Notons 0,1 ses éléments neutre pour l'addition et la multiplication. Alors l'ensemble $W(A)$ muni de $\hat{+}$ et $\hat{*}$ est un anneau d'éléments neutre $(0,0,\dots)$ et $(1,0,\dots)$.*

PREUVE : Si A contient $\mathbf{Q}$, l'application g_A est bijective, additive, multiplicative donc transfert la structure d'anneau commutatif de $(A^N,+,*)$ à $(W(A),\hat{+},\hat{\times})$.
Si A est un sous-anneau d'un anneau contenant $\mathbf{Q}$, $W(A)$ est encore un anneau. C'est en particulier le cas pour $A_{\mathbf{Z}} = \mathbf{Z}[X_0,X_1,\dots,Y_0,Y_1,\dots,Z_0,Z_1,\dots]$ dans lequel nous notons X,Y et Z les vecteurs de Witt $(X_0,X_1,\dots)$, $(Y_0,Y_1,\dots)$ et $(Z_0,Z_1,\dots)$.
Sinon, soit $a,b,c \in W(A)$. Notons $\phi_{abc} : A_{\mathbf{Z}} \to W(A)$ l'homomorphisme d'anneaux qui envoie les composantes X_k (resp. Y_k, Z_k) sur a_k (resp. b_k, c_k) pour tout entier $k \geq 0$. L'application ϕ_{abc} est additive, multiplicative, elle transporte donc les relations d'associativité, distributivit et commutativité de l'anneau $W(A_{\mathbf{Z}})$ dans l'ensemble $W(A)$ pour les lois $\hat{+}$, $\hat{*}$. Ainsi $W(A)$ est muni d'une structure d'anneau commutatif.
Les éléments neutres : c'est trivial quand $\mathbf{Q} \subset A$ et une preuve analogue à la précédente conlcut. ∎

On en déduit alors :

Corollaire 8.4.8 *Soient A,B deux anneaux commutatifs. Pour tout morphisme d'anneaux $f : A \to B$, l'application induite $W(f) : W(A) \to W(B)$ est un morphisme d'anneaux.*

Définition 8.4.9 *Pour tout entier $n \geq 1$, nous notons $W_n(A)$ l'ensemble des vecteurs de Witt de $W(A)$ tronqués $(x_0,x_1,\dots,x_{n-1})$ de longueur n*

Ainsi $W_n(A),\hat{+},\hat{\times}$ est un anneau commutatif, quotient de $W(A)$. Pour $n \geq m \geq 1$, nous notons le morphisme de troncation

$$t_{nm} : W_n(A) \to W_n(A), (x_0,\dots,x_{n-1}) \mapsto (x_0,\dots,x_{m-1}).$$

Théorème 8.4.10 *(admis) Soit A un anneau commutatif. L'anneau de Witt $W(A)$ est isomorphe à la limite projective du système $(W_n),t_{nm})_n$:*

$$W(A) = \lim_{\leftarrow} W_n(A)$$

ce qui munit $W(A)$ d'une topologie.

Définition 8.4.11 *On appelle Verschiebung l'application* $V : W(A) \to W(A)$, $V(x_0, x_1, \dots) = (0, x_0, x_1, \dots)$.

8.5 Vecteurs de Witt sur $\mathbf{F}_p$

L'objet de ce paragraphe est de décrire explicitement l'anneau des vecteurs de Witt $W(\mathbf{F}_p)$. Pour tout $n \geq 1$, nous rappellons l'existence d'un isomorphisme canonique d'anneaux :

$$F_n : W_n(\mathbf{F}_p) \to \mathbf{Z}/p^n\mathbf{Z},\ (x_0, x_1, \dots) \mapsto \bar{x}_0 + p\bar{x}_1 + \cdots + \bar{x}_{n-1}p^{n-1} \mod p$$

où chaque $\bar{x}_i \in \mathbf{Z}$ désigne l'unique représentant modulo p de x_k dans $\{0, \dots, p-1\}$. Cet isomorphisme transforme le Verschiebung V en la mulitplication par p :

$$\begin{array}{ccc} W_n(\mathbf{F}_p) & \longrightarrow^{F_n} & \mathbf{Z}/p^n\mathbf{Z} \\ \downarrow V & & \downarrow p \\ W_{n+1}(\mathbf{F}_p) & \to^{F_{n+1}} & \mathbf{Z}/p^{n+1}\mathbf{Z} \end{array}$$

De plus pour tout $n \geq 1$, nous avons un autre diagramme commutatif :

$$\begin{array}{ccc} W_{n+1}(\mathbf{F}_p) & \longrightarrow^{F_{n+1}} & \mathbf{Z}/p^{n+1}\mathbf{Z} \\ \downarrow t_n & & \downarrow red_n \\ W_n(\mathbf{F}_p) & \to^{F_n} & \mathbf{Z}/p^n\mathbf{Z} \end{array}$$

où t_n est le morphisme de troncation et red_n est la réduction modulo p^n. Ainsi en munissant les anneaux finis de la topologie discrète, on a un isomorphisme de systèmes projectifs d'anneaux :

$$\lim_{\leftarrow} W_n(\mathbf{F}_p) \to \lim_{\leftarrow} \mathbf{Z}/p^n\mathbf{Z}$$

D'où un isomorphisme d'anneaux topologiques $W(\mathbf{F}_p) \to \mathbf{Z}_p$.

Théorème 8.5.1 *Les vecteurs de Witt à coefficients dans* $\mathbf{F}_p$ *satisfont :*

$$W(\mathbf{F}_p) = \mathbf{Z}_p$$

et pour tout $n \geq 1$ *:*

$$W_n(\mathbf{F}_p) = \mathbf{Z}/p^n\mathbf{Z}$$

9 Caractéristique $p > 0$

Dans ce chapitre p désigne un nombre premier, $q = p^r$ et $\mathbf{F}_q$ est le corps à q éléments.

9.1 Codes linéaires, distance de Hamming

Définition 9.1.1 *Un codage est une application injective $E : \mathbf{F}_q^k \to \mathbf{F}_q^n$. L'image $C = E(\mathbf{F}_q^k) \subset F_q^n$ est dit code. Un décodage est une fonction $D : \mathbf{F}_q^n \to \mathbf{F}_q^k$ tellle que $D \circ E$ est l'identité de $\mathbf{F}_q^k$.*

Nous ne nous interessons ici qu'aux codes linéaires, i.e. pour lesquels E est une application linéaire. Ainsi C est un sous-espace vectoriel de $\mathbf{F}_q^n$. La matrice G de E dans les bases canoniques est dite matrice génératrice correspondant à E.

Exemples 9.1.2 *Soit C le code linéaire défini par $E : \mathbf{F}_2^4 \to \mathbf{F}_2^2$ avec*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Alors $C = \{(0,0,0,0), (1,0,1,0), (1,1,1,1), (0,1,0,1)\}$.

Définition 9.1.3 *Un code linéaire, étant un sous-espace vectoriel de dimension r de $\mathbf{F}_q^n$ peut également être défini comme le noyau d'un système linéaire, donc par une matrice H de taille $(n-r) \times n$, dite matrice de vérification. Ainsi $xH = 0$, pour tout $x \in C$.*

Exemples 9.1.4 *Le code défini dans l'exemple 9.1.2 admet la matrice de vérification suivante :*

$$H = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

On définit une distance sur les codes, la distance de Hamming :

$$\forall x, y \in \mathbf{F}_q^n, d(x,y) = |\{i, 1 \leq i \leq n, x_i \neq y_i\}|$$

(voir TD). Cette distance permet de déterminer combien d'erreurs sont admissibles dans la transmission d'un code au sens suivant :

Proposition 9.1.5 *Soit C un code de distance minimum $d = \min\{d(x,y), x \neq y \in C\}$. Alors toute erreur de $d-1$ termes peut être détectée. De plus si $d \geq 2t+2$ toute erreur de $t \geq 1$ termes peut être corrigée par la fonction de décodage du plus proche voisin.*

PREUVE : Si tour tout $x \neq y \in C$, $d(x,y) \geq d$, une erreur de transmission sur au plus $d-1$ termes pourra être détectée.
De plus si $d \geq 2t+1 \geq 3$ alors $d(x,z) + d(z,y) \geq d(x,y) \geq 2t+1$. Ainsi $d(x,z) > t$ ou $d(y,z) > t$. Or $\{y \in C, d(y,x) \leq t\} = \{x\}$, donc $D(x) = E^{-1}(c)$ où $c \in C$ minimise $d(x,c)$. ∎

9.2 Codes cycliques

Définition 9.2.1 *Un code cyclique est un code linéaire $C \subset \mathbf{F}_q^n$ tel que C est stable par permutations des composantes dans $\mathbf{F}_q^n$.*

Cette définition est motivée par l'isomorphisme

$$\mathbf{F}_q^n \to R = \mathbf{F}_q[x]/(x^n - 1), \quad (a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$$

Un code cyclique définie donc un sous ensemble de poynômes de degré $n-1$ stable par multiplication par x dans R.

Proposition 9.2.2 *Soit $R = \mathbf{F}_q[x]/ < x^n - 1 >$. Un sous-espace $C \subset R$ est un code cyclique si et seulement si C est un idéal de R.*

PREUVE : Un sous-espace vectoriel de R stable par multiplication par x est stable par mulplication par tout $h(x) \in R$. ∎

Proposition 9.2.3 *Les idéaux de R sont principaux engendrés par un diviseur g de $x^n - 1$.*

PREUVE : Les idéaux de R sont en bijection avec les idéaux de $\mathbf{F}_q[x]$ contenant $x^n - 1$. ∎

Définition 9.2.4 *Soit $J \subset k[x_1, \ldots, x_n]$ un idéal. Les monômes standards sont les monômes non inclus dans* $< \mathrm{LT}(J) >$.

L'isomorphisme

$$R = \mathbf{F}_q[x_1, \ldots, x_m]/ < x_1^{n_1}, \ldots, x_m^{n_m} - 1 > \cong \mathbf{F}_q^{n_1 \cdot n_2 \cdots n_m}$$

permet de définir les codes cycliques de dimension m via un système de générateurs $\{\overline{f_1}, \ldots, \overline{f_s}\}$ d'un idéal I de R. L'idéal correspondant J dans $\mathbf{F}_q[x_1, \ldots, x_m]$ est

$$J = < f_1, \ldots, f_s > + < x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1 >$$

Théorème 9.2.5 *Soit $I \subset R = \mathbf{F}_q[x_1, \ldots, x_m]/ < x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1 >$ un code cyclique de dimension m et G une base de Gröbner pour l'idéal associé $J \subset \mathbf{F}_q[x_1, \ldots, x_m]$ pour un ordre monomial fixé. On a le codage E suivant de I :*
Input : Base de Gröbner G pour J
w une combinaison linéaire de monômes non standards
Output : $E(w) \in C$
$\overline{w} := \overline{w}^G$
$E(w) := w - \overline{w}$

PREUVE : Soit w une combinaison linéaire de monômes non standards. Ainsi $\overline{w}^G$ est une combinaison linéaire de monômes non standards dont les symboles de w ne sont pas changés dans le calcul de $E(w) = w - \overline{w}$. Montrons que $E(w) \in I$. On a $I = J/ < x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1 >$ et

$$R/I \cong \mathbf{F}_q[x_1, \ldots, x_m]/J.$$

donc $h(x_1, \ldots, x_m) \in F_q[x_1, \ldots, x_m]$ représente un élément de I dans R ssi $\overline{h}^G = 0$. ∎