POLYNÔMES MULTIVARIÉS

Soit K un corps. On considère l'anneau $R = K[X_1, \ldots, X_n]$.

Rappel. *Un idéal I de R est un sous-groupe de $(R, +)$ tel que pour tout $a \in I$ et $f \in R$, l'élément af appartient à I. On rappelle aussi que si $\mathcal{P}$ est une partie de R, alors l'idéal engendré par $\mathcal{P}$ est le plus petit idéal de R contenant $\mathcal{P}$. C'est l'ensemble*

$$< \mathcal{P} >= \left\{ \sum_{p \in J} q_p p \ : \ J \subset \mathcal{P} \text{ est finie et } q_p \in R \ \forall p \in J \right\}.$$

Soient $f_1, \ldots, f_r$ des éléments de R. On va s'intéresser à l'idéal I engendré par $f_1, \ldots, f_s$, c'est-à-dire

$$I =< f_1, \ldots, f_s >= \left\{ \sum_{i=1}^{s} q_i f_i \ : \ (q_1, \ldots, q_s) \in R^s \right\}.$$

Comment travailler avec un tel idéal ? Plus précisément, on peut se poser les questions suivantes.

- Soit f un élément de R. Comment savoir si f appartient ou non à I ?
- Soit J un autre idéal de R. Comment savoir si J est inclus dans I ?
- Soit
$$\begin{aligned} V(I) &= \{x = (x_1, \ldots, x_n) \in K^n \ f(x) = 0 \ \forall f \in I\} \\ &= \{x = (x_1, \ldots, x_n) \in K^n \ f_i(x) = 0 \ \forall i \in [[1, s]]\}. \end{aligned}$$
Comment savoir si $V(I)$ est vide ? Comment savoir s'il est fini ? Et dans ce cas, comment calculer ses éléments ?

Si $n = 1$, nous savons répondre facilement à ces questions. Dans ce cas, tout idéal I est principal. Donc I s'écrit $I = gR$ où $g \in R$ (c'est le pgcd des f_i). Pour savoir si f appartient à I, on effectue la division euclidienne $f = gq + r$. Alors $f \in I$ si et seulement si $r = 0$. Enfin, $V(I)$ est l'ensemble des racines de g dans K.

Pour répondre à ces question dans le cas où $n \geq 2$, nous allons définir une *division multivariée dans R*. Cela nous mènera à définir certains systèmes de générateurs de I pour lesquels cette division possèdera la propriété d'unicité du reste. Ces systèmes sont appelés *bases de Gröbner*.

1. Division multivariée avec reste

Un monôme est un élément de R de la forme

$$X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n} \text{ où } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n.$$

Pour définir la division, nous aurons besoin d'une relation d'ordre total sur les monômes (donc sur $\mathbb{N}^n$), qui vérifieront certaines propriétés supplémentaires. Rappelons d'abord ce qu'est une relation d'ordre.

Définition 1.1. *Soit A un ensemble. Une relation $\preceq$ de A est une relation d'ordre si les conditions suivantes sont réalisées.*

(1) *Pour tout x dans A, $x \preceq x$ ($\preceq$ est réflexive).*

(2) *Si $x \preceq y$ et $y \preceq x$, alors $x = y$ ($\preceq$ est anti-symétrique).*

(3) *Si $x \preceq y$ et $y \preceq z$, alors $x \preceq z$ ($\preceq$ est transitive).*

De plus, cette relation est dite d'ordre total si pour tout $(x, y) \in A^2$, soit $x \preceq y$ soit $y \preceq x$.

Les ordres que nous utiliseront sont appelés *ordres monomiaux*. Ils sont définis de la manière suivante.

Définition 1.2. *Un ordre monomial $\preceq$ sur $\mathbb{N}^n$ est une relation d'ordre total sur $\mathbb{N}^n$ qui vérifie les deux propriétés suivantes.*

(1) *Si $\alpha \preceq \beta$, alors $\alpha + \gamma \preceq \beta + \gamma$.*

(2) *Tout ensemble non vide de $\mathbb{N}^n$ admet un plus petit élément.*

On note alors $\alpha \prec \beta$ si $\alpha \preceq \beta$ et si $\alpha \neq \beta$. Par abus de language, on parlera d'ordre monomial indifféremment pour $\prec$ ou pour $\preceq$. Enfin, on dit que $X^\alpha \preceq X^\beta$ (resp. $X^\alpha \prec X^\beta$) si $\alpha \preceq \beta$ (resp. $\alpha \prec \beta$).

Exemples.

- L'ordre lexicographique. On le note $\prec_{\text{lex}}$. On dit que $\alpha \prec_{\text{lex}} \beta$ si $\alpha \neq \beta$ et si le premier coefficient non nul de $\alpha - \beta$ est strictement négatif. Ainsi, $(1, 1, 2, 3) \prec_{\text{lex}} (1, 3, 2, 1)$ et donc $X_1 X_2 X_3^2 X_4^3 \prec_{\text{lex}} X_1 X_2^3 X_3^2 X_4$.
- . L'ordre lexicographique gradué. On le note $\prec_{\text{grlex}}$.

$$\alpha \prec_{\text{grlex}} \beta \text{ si } \begin{cases} \sum \alpha_i < \sum \beta_i \\ \text{ou } \left(\sum \alpha_i = \sum \beta_i \text{ et } \alpha \prec_{\text{lex}} \beta \right) \end{cases}$$

  Ainsi, $(1, 1, 2, 3) \prec_{\text{grlex}} (1, 3, 2, 1)$, et $(2, 0, 0, 0) \prec_{\text{grlex}} (1, 1, 1, 1)$ (alors que $(1, 1, 1, 1) \prec_{\text{lex}} (2, 0, 0, 0)$).

Définition 1.3. *Soit $\prec$ un ordre monomial fixé. Soit $f \in R$. Cet élément s'écrit*

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$$

où $\{\alpha \ : \ c_\alpha \neq 0\}$ est fini. On définit les termes suivants.

- *Terme de f : tout $c_\alpha X^\alpha$ tel que $c_\alpha \neq 0$.*
- *Multidegré : $mdeg(f) = \max\{\alpha \in \mathbb{N}^n \ : \ c_\alpha \neq 0\}$.*
- *Coefficient dominant : $lc(f) = c_{mdeg(f)}$.*
- *Monôme dominant : $lm(f) = X^{mdeg(f)}$.*
- *Terme dominant : $lt(f) = c_{mdeg(f)} X^{mdeg(f)}$.*

Venons en maintenant à la division multivariée. On veut diviser f par $f_1, \ldots, f_s$. Au debut, le reste r est égal à 0. On pose aussi $p = f$. Si $\mathrm{lt}(p)$ est divisible par l'un des $\mathrm{lt}(f_i)$, on effectue la division. Sinon, on remplace p par $p - \mathrm{lt}(p)$ et r par $r + \mathrm{lt}(p)$. On continue ainsi jusqu'à arriver à $p = 0$.

Mais voyons plutôt un exemple.

Notation. L'écriture

$$a \longleftarrow b$$

signifie que l'on affecte à la variable a la valeur de b.

Exemple. Dans $K[x, y]$, divisons $f = x^2y + xy^2 + y^2$ par $f_1 = xy - 1$ et $f_2 = y^2 - 1$, en utilisant l'ordre lexicographique $\preceq$ tel que $x \succeq y$. Partons de $p \longleftarrow f$, $r \longleftarrow 0$, $q_1 \longleftarrow 0$ et $q_1 \longleftarrow 0$. Alors $f = p + q_1 f_1 + q_2 f_2 + r$, égalité qui restera vraie tout au long de la division. On voit que $(2, 1) \succeq (1, 2) \succeq (0, 2)$, donc $\mathrm{lt}(p) = x^2y$. Ce terme est divisible par $\mathrm{lt}(f_1) = xy$. On fait donc la division.

$$\begin{aligned} p &\longleftarrow p - xf_1 = xy^2 + x + y^2 \\ q_1 &\longleftarrow q_1 + x = x \end{aligned}$$

Après ces opérations, $\mathrm{lt}(p) = xy^2$ est encore divisible par $\mathrm{lt}(f_1)$.

$$\begin{aligned} p &\longleftarrow p - yf_1 = x + y^2 + y \\ q_1 &\longleftarrow q_1 + y = x + y \end{aligned}$$

Maintenant, $\mathrm{lt}(p) = x$ n'est plus divisible ni par $\mathrm{lt}(f_1)$ ni par $\mathrm{lt}(f_2)$. On fait alors

$$\begin{aligned} r &\longleftarrow r + x = x \\ p &\longleftarrow p - x = y^2 + y \end{aligned}$$

Après cela, $\mathrm{lt}(p) = y^2$ est divisible par $\mathrm{lt}(f_2) = y^2$.

$$\begin{aligned} p &\longleftarrow p - f_2 = x + y + 1 \\ q_2 &\longleftarrow q_2 + 1 = 1 \end{aligned}$$

À présent, $\mathrm{lt}(p) = x$ n'est plus divisible ni par $\mathrm{lt}(f_1)$ ni par $\mathrm{lt}(f_2)$.

$$\begin{aligned} r &\longleftarrow r + x = x \\ p &\longleftarrow p - x = y + 1 \end{aligned}$$

Maintenant encore, $\mathrm{lt}(p) = y$ n'est divisible ni par $\mathrm{lt}(f_1)$ ni par $\mathrm{lt}(f_2)$.

$$\begin{aligned} r &\longleftarrow r + y = x + y \\ p &\longleftarrow p - y = 1 \end{aligned}$$

Et enfin

$$\begin{aligned} r &\longleftarrow r + 1 = x + y + 1 \\ p &\longleftarrow p - 1 = 0 \end{aligned}$$

On obtient finalement

$$\begin{aligned} f &= q_1 f_1 + q_2 f_2 + r \\ &= (x + y) f_1 + f_2 + x + y + 1 \end{aligned}$$

On peut présenter ces calculs dans un tableau.

$x^2y + xy^2 + y^2$	$xy - 1$	$y^2 - 1$
$xy^2 + x + y^2$	x	
$x + y^2 + y$	y	
$x + y + 1$		1

Remarquons que nous aurions pu faire ces opérations dans en ordre différent, comme par exemple celui décrit dans le tableau suivant.

$x^2y + xy^2 + y^2$	$xy - 1$	$y^2 - 1$
$xy^2 + x + y^2$	x	
$2x + y^2$		x
$2x + 1$		1

On obtient alors

$$f = x f_1 + (x + 1) f_2 + 2x + 1.$$

Il n'y a donc pas unicité dans l'écriture

$$f = q_1 f_1 + q_2 f_2 + r.$$

Le plus ennuyeux, c'est qu'il n'y a pas unicité du reste r. Ainsi, si la question est l'appartenance ou non de f à un idéal I, et si cette division donne $r = 0$, on peut répondre « oui, f appartient à I ». Par contre, si le reste est non nul, on ne peux rien dire à priori.

Il existe cependant des systèmes de générateurs pour lesquels il y a unicité du reste dans cette division multivariée. C'est l'objet de la section suivante.

Avant d'aborder cette prochaine section, on termine celle ci en écrivant l'algorithme de la division multivariée.

Algorithme. Division multivariée avec reste.
Entrée. $f, f_1, \dots, f_s \in K[X_1, \dots X_n]$ et un ordre monomial $\preceq$
Sortie. $q_1, \dots, q_s, r \in K[X_1, \dots X_n]$ tels que $f = \sum q_i f_i + r$ et tels qu'aucun terme de r n'est divisible par aucun $\mathrm{lt}(f_i)$

$r \longleftarrow 0$
$q_i \longleftarrow 0 \ \forall i \in [[1, n]]$
$p \longleftarrow f$
Tant que $p \neq 0$ faire
    Si $\mathrm{lt}(p)$ est divisible par l'un des $\mathrm{lt}(f_i)$:
        $p \longleftarrow p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$
        $q_i \longleftarrow q_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$
    Sinon :
        $r \longleftarrow r + \mathrm{lt}(p)$
        $p \longleftarrow p - \mathrm{lt}(p)$
Sortir $q_1, \dots, q_n, r$

La preuve de la proposition suivante (qui permet de prouver l'algorithme) est laissée en exercice.

Proposition 1.4. *Après chaque exécution d'un pas de la boucle « Tant que » de cet algorithme, les égalités suivantes sont vérifiées.*

(1) $mdeg(p) \preceq mdeg(f)$.
(2) $f = p + \sum_{i=1}^{s} q_i f_s + r$.
(3) *Si* $q_i \neq 0$, *alors* $mdeg(q_i f_i) \preceq mdeg(f)$ *pour* $1 \leq i \leq s$.
(4) *Pour tout* i, *aucun terme de* r *n'est divisible par* $lt(f_i)$.

2. Bases de Gröbner

Si $\mathcal{P}$ est une partie de R, on note

$$< \mathrm{lt}(\mathcal{P}) > = < \mathrm{lt}(f) \ : \ f \in \mathcal{P} >$$

c'est-à-dire l'idéal engendré par les $\mathrm{lt}(f)$, où f parcourt $\mathcal{P}$.

Soit I un idéal de R. Il est clair que si

$$I = < f_1, \dots, f_s >$$

alors

$$< \mathrm{lt}(f_1) \ldots, \mathrm{lt}(f_s) > \subset < \mathrm{lt}(I) > .$$

Mais en général, ces deux idéaux ne sont pas forcément égaux : il arrive fréquemment que

$$< \mathrm{lt}(f_1) \ldots, \mathrm{lt}(f_s) > \neq < \mathrm{lt}(I) > .$$

Exemple. Dans $R = \mathbb{Q}[x, y]$, nous utilisons l'ordre lexicographique gradué $\prec_{\mathrm{grlex}}$ tel que $x \succ_{\mathrm{grlex}} y$. Soient $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$. Alors $\mathrm{lt}(f_1) = x^3$ et $\mathrm{lt}(f_2) = x^2y$.

$$< \mathrm{lt}(f_1), \mathrm{lt}(f_2) > = < x^3, x^2y > .$$

Or, $-yf_1 + xf_2 = x^2 \in I$, donc $x^2 \in < \mathrm{lt}(I) >$, mais $x^2 \notin < \mathrm{lt}(f_1), \mathrm{lt}(f_2) >$.

Définition 2.1. *Soit G une partie finie de I. On dit que G est une base de Gröbner de I si $< lt(I) > = < lt(G) >$.*

Remarquons qu'il n'est pas imposé dans cette définition que G engendre I. Ce n'est pas nécessaire : les choses se passent ici joliment, comme l'indique le résultat suivant.

Théorème 2.2. *Si G est une base de Gröbner de I, alors $I = G$.*

Pour montrer ce théorème, et pour plusieurs raisonnements dans la suite du paragraphe, nous utiliserons le résultat élémentaire suivant, dont la preuve est laissée en exercice.

Lemme 2.3. *Soient $\alpha, \alpha_1, \ldots, \alpha_t$ des éléments de $\mathbb{N}^n$. Si X^α appartient à $< lt(X^{\alpha_1}), \ldots, lt(X^{\alpha_t}) >$, alors il existe $i \in [[1, t]]$ tel que X^{α_i} divise X^α.*

Preuve du théorème 2.2. Par l'absurde, on suppose qu'il existe un élément f dans $I \setminus < G >$, et on choisit cet élément de telle sorte que $\mathrm{mdeg}(f)$ soit minimal. Comme $\mathrm{lt}(f) \in < \mathrm{lt}(G) >$, et en vertu du lemme 2.3, on en déduit qu'il existe $g \in G$ tel que $\mathrm{lt}(g)$ divise $\mathrm{lt}(f)$. Soit alors

$$f_1 = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g.$$

Alors $f_1 \in I$ et $\mathrm{mdeg}(f_1) \prec \mathrm{mdeg}(f)$. Par minimalité de $\mathrm{mdeg}(f)$, on conclut que $f_1 \in G$, donc que $f \in G$, ce qui est contraire à l'hypothèse. □

Venons en au résultat que nous souhaitions, c'est-à-dire l'unicité du reste dans la division multivariée.

Proposition 2.4. *Soit $G = \{f_1, \ldots, f_s\}$ une base de Gröbner. S'il existe $q_1, \ldots, q_s, q'_1 \ldots, q'_s, r, r' \in R$ tels que*

$$\sum q_i f_i + r = \sum q_i^{'} f_i + r'$$

de telle sorte que pour tout i, aucun des termes de r ni de r' n'est divisible par $lt(f_i)$, alors $r = r'$.

Preuve. Si $\sum q_i f_i + r = \sum q_i^{'} f_i + r'$, alors $r - r' \in I =< G >$. Si $r - r' \neq 0$, on considère $\mathrm{lt}(r - r')$. Cet élément appartient à $< \mathrm{lt}(I) >=< \mathrm{lt}(G) >$. Le lemme 2.3 permet de déduire qu'il existe i tel que $\mathrm{lt}(f_i)$ divise $\mathrm{lt}(r - r')$, et donc que $\mathrm{lt}(f_i)$ divise l'un des termes de r ou de r', ce qui contredit l'hypothèse. □

On déduit facilement le résultat suivant.

Corollaire 2.5. *Si G est une base de Gröbner de I, alors pour tout élément f de R, $f \in I$ si et seulement si le reste de la division multivariée de f par G est nul.*

Ainsi, si l'on connaît une base de Gröbner de I, il est plus facile de travailler sur cet idéal. Reste à savoir si tout idéal I possède une base de Gröbner, et aussi comment calculer une telle base. Nous répondons ici à ces questions.

Théorème 2.6. *Tout idéal de R possède une base de Gröbner.*

Ce résultat à pour conséquence immédiate le célèbre théorème de la base de Hilbert.

Corollaire 2.7 (Théorème de la base de Hilbert)**.** *Tout idéal de R est de type fini. Autrement dit, R est Noethérien.*

Le théorème 2.6 est une conséquence du lemme de Dickson suivant.

Lemme 2.8 (Dickson)**.** *Pour toute partie A de $\mathbb{N}^n$, il existe une partie finie B de A telle que*

$$< X^\alpha \ : \ \alpha \in A >=< X^\beta \ : \ \beta \in B > .$$

Avant de démontrer ce lemme, nous introduisons quelques notations.

Notations.

(1) Pour toute partie $\mathcal{P}$ de $\mathbb{N}^n$, on note

$$< X^{\mathcal{P}} >=< X^\alpha \ : \ \alpha \in \mathcal{P} > .$$

(2) Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n)$ deux éléments de $\mathbb{N}^n$. On écrit :

$$\alpha \leq \beta \text{ si } \forall i,\ \alpha_i \leq \beta_i.$$

$$\alpha < \beta \text{ si } \alpha \leq \beta \text{ et } \alpha \neq \beta.$$

Alors $\leq$ est une relation d'ordre partiel si $n > 1$. Par exemple, dans $\mathbb{N}^2$, les couples $(1, 0)$ et $(0, 1)$ ne sont pas comparables.

Preuve du lemme 2.8. Soit B l'ensemble des éléments minimaux de A pour la relation $\leq$, c'est-à-dire :

$$B = \{\alpha \in A \ :\ \forall \beta \in A,\ \beta \leq \alpha \Rightarrow \beta = \alpha\}.$$

Soit $\alpha \in \mathbb{N}^n$. Alors l'ensemble

$$\mathcal{M}_\alpha = \{\beta \in \mathbb{N}^n \ :\ \beta \leq \alpha\}$$

est fini. Cet ensemble est en effet égal à

$$[[0, \alpha_1]] \times \cdots \times [[0, \alpha_n]].$$

Il n'existe donc pas de suites infinies (a_i) de $\mathbb{N}^n$ telles que $a_i > a_{i+1}$ pour tout i, et par conséquent, si $\alpha \in A$, alors $M_\alpha \cap B$ est non vide.

Nous allons démontrer les deux faits suivant.

(1) $< X^A >=< X^B >$.

(2) B est fini.

Le point (1) n'est pas difficile. Il est clair que $< X^B > \subset < X^A >$ puisque $B \subset A$. Réciproquement, si $\alpha \in A$. Soit β un élément de B tel que $\beta \leq \alpha$ (c'est-à-dire un élément de M_α). Alors

$$X^\alpha = X^\beta X^{\alpha-\beta} \in < X^B > .$$

Le point (2), qui est un résultat de combinatoire, est plus délicat.

Voyons un exemple. Si $A = \{\alpha \in \mathbb{N}^2 \ :\ \alpha_1 + \alpha_2 \geq 2\}$, alors $B = \{(2, 0), (1, 1), (0, 2)\}$ est bien fini.

Nous démontrons (2) par récurrence sur n.

Si $n = 1$, comme toute partie de $\mathbb{N}$ admet un plus petit élément, B est réduit à un élément.

On suppose maintenant que $n \geq 2$. Nous allons montrer qu'il existe un élément $\gamma \in \mathbb{N}^n$ tel que pour tout élément β de B vérifie $\beta \leq \gamma$, c'est-à-dire tel que $\mathcal{M}_\gamma$ contient B. Comme on sait déjà que $\mathcal{M}_\gamma$ est fini, cela montrera la finitude de B.

Pour cela, nous montrons qu'il existe $b \in \mathbb{N}$ tel que pour tout $\beta \in B$, la n-ème coordonnée de β est inférieure à b. Pour cela , on définit

$$A^* = \{\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1} \ : \exists \alpha_n \in \mathbb{N} \text{ vérifiant } (\alpha_1, \ldots, \alpha_n) \in A\}$$

et B^* l'ensemble des éléments minimaux de A^*. Alors par hypothèse de récurrence, l'ensemble B^* est fini. Pour tout $\beta = (\beta_1, \dots, \beta_{n-1}) \in B^*$, on choisit $b_\beta \in \mathbb{N}$ tel que $(\beta_1, \dots, \beta_{n-1}, b_\beta) \in A$. Comme B^* est fini, on peut définir l'élément

$$b = \max_{\beta \in B^*} b_\beta$$

qui sera la borne cherchée. Soit donc $\alpha = (\alpha_1, \dots, \alpha_n) \in B$, montrons que $\alpha_n \leq b$. Par l'absurde, supposons que

$$\alpha_n > b.$$

Comme $\alpha \in A$, alors $(\alpha_1, \dots, \alpha_{n-1}) \in A^*$. Soit $\beta = (\beta_1, \dots, \beta_{n-1}) \in B^*$ tel que $\beta \leq \alpha$. Alors

$$(\beta_1, \dots, \beta_{n-1}, b_\beta) \leq (\beta_1, \dots, \beta_{n-1}, b) < (\alpha_1, \dots, \alpha_n)$$

Ce qui contredit le fait que $\alpha \in B$, c'est-à-dire que α est minimal dans A. □

3. Algorithme de Buchberger

Maintenant, étant donné un idéal I de R, nous voudrions pouvoir calculer une base de Gröbner de I. L'algorithme de Buchberger résout ce problème. Cet algorithme est basé sur le calcul de *S-polynômes* que nous définissons ici.

Définition 3.1. *Soient f et g deux éléments de R. On note $\alpha = (\alpha_1, \dots, \alpha_n) = mdeg(f)$ et $\beta = (\beta_1, \dots, \beta_n) = mdeg(g)$. Soit*

$$\gamma = (\max(\alpha_i, \beta_i))_{i \in [[1,n]]} \in \mathbb{N}^n.$$

On appelle S-polynôme associé à f et g le polynôme

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

Exemple. Dans $\mathbb{Q}[x,y]$, on utilise l'ordre monomial $\prec_{\text{lex}}$ tel que $y \prec_{\text{lex}} x$. Soient $f = 2x^2y - 3xy$ et $g = x^3 + y^5$. Alors $\text{lt}(f) = 2x^2y$ et $\text{lt}(g) = x^3$. Ainsi, $\alpha = (2,1)$, $\beta = (3,0))$ et $\gamma = (3,1)$. Enfin :

$$\begin{aligned} S(f,g) &= \frac{x^3y}{2x^2y}(2x^2y - 3xy) - \frac{x^3y}{x^3}(x^3 + y^5) \\ &= -\frac{3}{2}x^2y - y^6. \end{aligned}$$

Dans la différence définissant $S(f,g)$, les termes dominants s'annulent. Autrement dit,

$$\text{mdeg} S(f,g) \prec \gamma.$$

Le lemme suivant exprime le fait que si dans une somme on constate l'élimination des termes de plus haut degré, cela "provient" de S-polynômes.

Lemme 3.2. *Soient $g_1, \ldots, g_s \in R$, $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^n$, $c_1, \ldots, c_s \in K^*$,*

$$f = \sum_{i=1}^{s} c_i X^{\alpha_i} g_i \in R$$

et $\delta \in \mathbb{N}^n$ tel que $\alpha_i + mdeg(g_i) = \delta$ pour tout $i \in [[1, s]]$ et tel que $mdeg(f) \prec \delta$ (c'est-à-dire que les termes dominants s'éliminent). Pour $i < j$, on définit $\gamma_{ij} \in \mathbb{N}^n$ tel que

$$X^{\gamma_{ij}} = ppcm(lm(g_i), lm(g_j))$$

(c'est le γ de la définition 3.1 correspondant à $S(g_i, g_j)$). Alors les propriétés suivantes sont vérifiées.

1. *$X^{\gamma_{ij}}$ divise X^δ pour tout (i, j) tel que $1 \leq i < j \leq s$.*
2. *$mdeg(X^{\delta - \gamma_{ij}} S(g_i, g_j)) \prec \delta$ pour tout (i, j) tel que $1 \leq i < j \leq s$.*
3. *Il existe des éléments c_{ij} dans K tels que*

$$f = \sum_{1 \leq i < j \leq s} c_{ij} X^{\delta - \gamma_{ij}} S(g_i, g_j).$$

Preuve. Exercice. Pour le (3), procéder par récurrence comme suit. En multipliant chaque c_i par $\mathrm{lc}(g_i)$ et en divisant chaque g_i par ce même coefficient $\mathrm{lc}(g_i)$, on se ramène au cas où $\mathrm{lc}(g_i) = 1$ pour tout i. Si $s > 1$, on définit $g = f - c_1 X^{\delta - \gamma_{12}} S(g_1, g_2)$ puis on montre que

$$g = (c_1 + c_2) X^{\alpha_2} g_2 + \sum_{i=3}^{s} c_i X^{\alpha_i} g_i.$$

Le polynôme g est de la même forme que f, mais avec $s - 1$ ou $s - 2$ termes.

Si $s = 1$, il ne peut y avoir annulation des termes dominants. Dans ce cas, le lemme est vide, donc vrai. □

Théorème 3.3. *Soit $G = \{g_1, \ldots, g_s\} \subset R$. Alors G est une base de Gröbner de I si et seulement si les deux conditions suivantes sont vérifiées.*

1. *$I =< g_1, \ldots, g_s >$.*
2. *Pour tout $(i, j) \in [[1, s]]^2$ tel que $1 \leq i < j \leq s$, le reste de la division de $S(g_i, g_j)$ par G est égale à 0.*

Preuve. Le sens direct est clair. Réciproquement, supposons les conditions (1) et (2) vérifiées. Montrons que $< \mathrm{lt}(I) >=< \mathrm{lt}(G) >$, c'est-à-dire que $< \mathrm{lt}(I) > \subset < \mathrm{lt}(G) >$, l'autre inclusion étant évidente. Soit donc $f \in I$. Comme G engendre I, ce polynôme f s'écrit

$$f = \sum_{g \in G} q_g g \tag{1}$$

où $q_g \in R$ pour tout $g \in G$. On veut montrer que $\mathrm{lt}(f) \in \mathrm{lt}(G)$. On note $\alpha = \mathrm{mdeg}(f)$. Si $\mathrm{mdeg}(q_g g) \preceq \alpha$ pour tout $g \in G$, alors il n'y a pas de simplification des termes de plus haut degré des $q_g g$ dans l'expression de f donnée par l'égalité (1). Ainsi :

$$\begin{aligned} \mathrm{lt}(f) &= \sum_{\mathrm{g} \,:\, \mathrm{mdeg}_{(q_g g)=\alpha}} \mathrm{lt}(q_g g) \\ &= \sum_{\mathrm{g} \,:\, \mathrm{mdeg}_{(q_g g)=\alpha}} \mathrm{lt}(q_g)\mathrm{lt}(g) \in < \mathrm{lt}(G) > \end{aligned}$$

Cela règle la question dans ce cas là. Mais il se peut qu'il y ait des simplifications des termes de plus haut degré. Alors

$$\alpha \prec \max_{g \in G} \mathrm{lt}(q_g g).$$

On raisonne par récurrence. On suppose donc le résultat vrai si

$$\max_{g \in G} \mathrm{lt}(q_g g) \prec \beta$$

et prouvons le dans le cas où

$$\max_{g \in G} \mathrm{lt}(q_g g) = \beta.$$

Posons

$$f^* = \sum_{g \in G} \mathrm{lt}(q_g) g.$$

Alors le lemme 3.2 montre l'existence de $\lambda_{h,g} \in K$ et $\alpha_{h,g} \in \mathbb{N}^n$ (pour $g, h \in G$) tels que

$$f^* = \sum_{g,h} \lambda_{g,h} X^{\alpha_{g,h}} S(g,h)$$

de telle sorte que pour tout $(g,h) \in G^2$,

$$\mathrm{mdeg}(X^{\alpha_{g,h}} S(g,h)) \prec \beta.$$

Alors si l'on fait la division de f^* par G, on obtient

$$f^* = \sum_{g \in G} q_g^* g$$

où d'après le point (3) de la proposition 1.4

$$\mathrm{mdeg}(q_g^* g) \prec \mathrm{mdeg}(f^*) \prec \beta$$

pour tout g. Finalement, $f = (f - f^*) + f^*$ où $f - f^*$ et f^* s'écrivent tous deux sous la forme d'une somme $\sum_{g \in G} p_g g$ où les p_g sont des éléments de R tels que $\mathrm{lt}(p_g g) \prec \beta$ pour tout $g \in G$. □

L'algorithme de Buchberger prend en entrée une famille $F = (f_1, \ldots, f_s)$ d'éléments de R et rend en sortie une base de Gröbner de l'idéal $I =< f_1, \ldots, f_s >$. L'idée est de calculer le reste r de chaque $S(f_i, f_j)$ divisé par F, et d'ajouter ce reste à la famille s'il est non nul.

Algorithme. Buchberger.
Entrée. $f_1, \ldots, f_s \in K[X_1, \ldots X_n]$ et un ordre monomial $\prec$
Sortie. Une base de Gröbner G pour $\prec$ de $I =< f_1, \ldots, f_s >$

```
G ⟵ {f_1, ..., f_s}
S ⟵ G
Tant que S ≠ ∅ :
    S ⟵ ∅
    {g_1, ..., g_t} ⟵ G (on numérote les éléments de G de 1 à t)
    Pour i de 1 à t − 1 :
        Pour j de i + 1 à t :
            r ⟵ S(g_i, g_j)  mod G
            Si r ≠ 0 :
                S ⟵ S ∪ {r}
        G ⟵ G ∪ S
    Sortir G
```

Preuve. L'algorithme se termine dès que $\mathcal{S} = \emptyset$. Alors le théorème 3.3 montre que l'ensemble G obtenu est une base de Gröbner.

Montrons que l'algorithme se termine. Soient $G_1, \ldots, G_k, \ldots$ la suite des ensembles G successifs de l'algorithme. Alors $G_i \subset G_{i+1}$ pour tout i donc $< \mathrm{lt}(G_i) >\subset< \mathrm{lt}(G_{i+1} >$ pour tout i. Comme l'anneau R est noethérien, il existe i tel que $< \mathrm{lt}(G_i) >=< \mathrm{lt}(G_{i+1} >$. Montrons qu'alors $G_i = G_{i+1}$: cela prouvera qu'à cette étape, $\mathcal{S} = \emptyset$ et donc que l'algorithme se termine. Pour plus de commodité, posons $G = G_i$ et $G' = G_{i+1}$. Alors $G' = G \cup \mathcal{S}$. On pose aussi

$$G = \{g_i \ : \ i \in \{1, \ldots, t\}\}.$$

Pour tout (i, j) tel que $i < j$, soit $r_{i,j}$ le reste de la division de $S(g_i, g_j)$ par G. Comme $< \mathrm{lt}(G) >=< \mathrm{lt}(G' >$, c'est que $\mathrm{lt}(r_{i,j}) \in< \mathrm{lt}(G) >$ pour tout (i, j). Mais comme $r_{i,j}$ est un reste de la division par G, alors

si $\mathrm{lt}(r_{i,j}) \neq 0$, il n'est divisible par aucun des éléments de $\mathrm{lt}(G)$. On en déduit que $r_{i,j} = 0$ pour tout (i,j), donc que $\mathcal{S} = \emptyset$. □

4. Base de Gröbner réduite

Lemme 4.1. *Soit G une base de Gröbner de I. Soit $g \in G$ tel que*

$$lt(g) \in < lt(G \setminus \{g\}) > .$$

Alors $(G \setminus \{g\})$ est une base de Gröbner de I

Preuve. Si $\mathrm{lt}(g) \in < \mathrm{lt}\,(G \setminus \{g\}) >$, alors $< \mathrm{lt}(G) > = < \mathrm{lt}\,(G \setminus \{g\}) >$. On en déduit que $< \mathrm{lt}(I) > = < \mathrm{lt}\,(G \setminus \{g\}) >$ puisque $< \mathrm{lt}(I) > = < \mathrm{lt}\,(G) >$. □

Définition 4.2. *Une base de Gröbner G est dite minimale si pour tout $g \in G$, les deux propriétés suivantes sont réalisées.*

1. $lc(g) = 1$.
2. $lt(g) \notin < lt(G \setminus \{g\}) >$.

Définition 4.3. *Un élément g d'une base de Gröbner G est réduit pour G si aucun terme de g n'appartient à $< lt(G \setminus \{g\}) >$.*

Définition 4.4. *Une base de Gröbner minimale G est réduite si tous ses éléments sont réduits pour G.*

Théorème 4.5. *Tout idéal de R admet une unique base de Gröbner réduite.*

Preuve. La preuve de l'existence est laissée en exercice.

Montrons l'unicité. Soient donc G et G' deux bases de Gröbner réduites dun idéal I. Donc

$$< \mathrm{lt}(I) > = < \mathrm{lt}(G) > = < \mathrm{lt}(G') > .$$

Montrons d'abord que $\mathrm{lt}(G) = \mathrm{lt}(G')$. Soit $g \in G$. Montrons que $\mathrm{lt}(g) \in \mathrm{lt}(G')$. Comme $\mathrm{lt}(g) \in < \mathrm{lt}(G) > = < \mathrm{lt}(G') >$, il existe $g' \in G'$ tel que $\mathrm{lt}(g')$ divise $\mathrm{lt}(g)$. De même, il existe $g'' \in G$ tel que $\mathrm{lt}(g'')$ divise $\mathrm{lt}(g')$. Ainsi, $\mathrm{lt}(g'')$ divise $\mathrm{lt}(g)$. Comme G est une base de Gröbner réduite, on en déduit que $g = g''$. Comme $\mathrm{lt}(g)$ divise $\mathrm{lt}(g')$ et $\mathrm{lt}(g')$ divise $\mathrm{lt}(g)$, et comme $\mathrm{lc}(g) = \mathrm{lc}(g') = 1$ c'est donc que $\mathrm{lt}(g) = \mathrm{lt}(g')$, d'où l'inclusion $\mathrm{lt}(G) \subset \mathrm{lt}(G')$, puis l'égalité $\mathrm{lt}(G) = \mathrm{lt}(G')$.

On peut maintenant montrer que $G = G'$. Soit $g \in G$. Comme $\mathrm{lt}(G) = \mathrm{lt}(G')$, il existe $g' \in G'$ tel que $\mathrm{lt}(g) = \mathrm{lt}(g')$. Alors, les termes dominants de g et de g' s'annulent dans $g - g'$. Comme G et G' sont des bases réduites, et comme $\mathrm{lt}(G) = \mathrm{lt}(G')$, aucun des termes de g ne de g' n'est divisible par un élément de $< \mathrm{lt}(G) \setminus \{g\} >$, donc aucun des termes de $g - g'$ n'est divisible par un élément de $< \mathrm{lt}(G) >$, ce qui

veut dire que le reste de la division de $g - g'$ par G est égal à $g - g'$. Or, comme $g - g' \in I$, ce reste est égal à 0. On en déduit que $g = g'$. Ainsi, $G \subset G'$, et par symétrie $G = G'$. □

5. Applications

5.1. **Monômes standards.** On considère toujours $R = K[X_1, \ldots, X_n]$ (qu'on note aussi $K[X]$), muni d'un ordre monomial $\prec$. Soit I un idéal de R et B une base de Gröbner de I pour $\prec$.

Définition 5.1. *Soit $\alpha \in \mathbb{N}^n$. Le monôme X^α est un monôme standard de R relativement à G si pour tout $g \in G$, le terme $lt(g)$ ne divise pas X^α.*

Théorème 5.2. *L'ensemble des monômes standards relativement à G est une base du K-espace vectoriel $K[X]/I$.*

Preuve. Tout polynôme f de R s'écrit

$$f = \sum_{g \in G} c_g g + r \tag{2}$$

où aucun des termes de r n'est divisible par un élément de $< \mathrm{lt}(G) >$, c'est à dire que les monômes apparaissant dans r sont des monômes standards. L'ensemble des monômes standards est donc une famille génératrice du K-espace vectoriel $K[X]/I$. L'unicité du reste dans la division (2) montre que la famille est libre.

Exemple. Soit $R = \mathbb{Q}[x, y]$, muni de l'ordre lexicographique gradué $\prec$ tel que $x \succ y$. Soient $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$ et $I =< f_1, f_2 >$. Alors la base de Gröbner réduite de I est égale à $G = (x^2, xy, y^2 - x/2)$. Alors, l'ensemble des monômes standards pour G est égal à

$$\mathcal{M} = \{1, x, y\}.$$

On peut visualiser ces monômes sur un graphique. Je renvoie pour cela à vos notes de cours.

Le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[x, y]/I$ est donc de dimension 3.

$$\mathbb{Q}[x, y]/I = \left\{ a_0 + a_1 x + a_2 y \ : \ (a_0, a_1, a_2) \in \mathbb{Q}^3 \right\}$$

Pour additionner deux éléments de $\mathbb{Q}[x, y]/I$, il suffit d'ajouter leurs composantes. Pour la multiplication, on établit la table de multiplication des monômes standards.

$\times$	1	x	y
1	1	x	y
x	x	0	0
y	y	0	$x/2$

Ainsi, les bases de Gröbner permettent de calculer dans de tels quotients

5.2. **Résolution de systèmes algébriques.** . Il arrive fréquemment qu'un problème se ramène à la résolution d'un système d'équations polynomiales. Soit à résoudre

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases} \tag{3}$$

Soient $I =< f_1, \ldots, f_s$ et $G = (g_1, \ldots, g_t)$ une base de Gröbner de I. Alors le système (3) est équivalent au système

$$\begin{cases} g_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ g_t(x_1, \ldots, x_n) = 0 \end{cases} \tag{4}$$

Souvent, ce nouveau système est lus facile à résoudre, car certaines variables peuvent avoir été éliminées dans certaines équations.

Reprenons l'exemple où $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$ dans $\mathbb{Q}[x, y]$. Alors

$$\begin{cases} f_1(x,y) = 0 \\ f_2(x,y) = 0 \end{cases} \iff \begin{cases} x^2 = 0 \\ xy = 0 \\ y^2 - x/2 = 0 \end{cases} \iff \begin{cases} x = 0 \\ y = 0 \end{cases}$$

Dans cet exemple, l'ordre monomial choisi est l'ordre lexicographique gradué. Ce n'est pas forcément le meilleur choix en général.

L'ordre lexicographique se prête particulièrement bien à l'élimination des variables. Pour tout idéal I de R, on note

$$I_l = I \cap K[X_{l+1}, \ldots, X_n].$$

C'est un idéal de $K[X_{l+1}, \ldots, X_n]$, appelé l-ème idéal d'élimination de I.

Théorème 5.3. *Soit $\prec$ l'ordre lexicographique tel que $X_1 \succ \cdots \succ X_n$. Soit G une base de Gröbner de I. Alors*

$$G_l = G \cap K[X_{l+1}, \ldots, X_n]$$

est une base de Gröbner de I_l.

Preuve. Voir la feuille 13, exercice 4.

Exemple. Soit à résoudre dans $\mathbb{R}$ le système suivant.

$$\begin{cases} f_1(x,y,z) = 0 \\ f_2(x,y,z) = 0 \\ f_3(x,y,z) = 0 \end{cases} \quad \text{où} \quad \begin{aligned} f_1(x,y,z) &= x^2 + y + z - 1 \\ f_2(x,y,z) &= x + y^2 + z - 1 \\ f_3(x,y,z) &= x + y + z^2 - 1 \end{aligned}$$

Soit I l'idéal $< f_1, f_2, f_3 >$ de $\mathbb{Q}[x,y,z]$. On munit $\mathbb{Q}[x,y,z]$ de l'ordre lexicographique $\prec$ tel que $x \succ y \succ z$. Alors la base de Gröbner réduite de I est $G = (g_1, g_2, g_3, g_4)$, où

$$\begin{aligned} g_1 &= x + y + z^2 - 1 \\ g_2 &= y^2 - y - z^2 + z \\ g_3 &= z^2(y + z^2/2 - 1/2) \\ g_4 &= z^2(z-1)^2(z^2 + 2z - 1) \end{aligned}$$

On remarque que g_4 ne dépend que de z et que g_2 et g_3 ne dépendent que de y et z. Il est alors facile de résoudre le système et on trouve comme ensemble des solutions

$$\begin{aligned} \mathcal{S} = \big\{ &(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), \\ &(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}) \big\}. \end{aligned}$$