Belordre et Réécriture
I : Bases de Gröbner
M2 - maths
FST - Université de la Réunion

Christian Delhommé

Département de mathématiques

octobre 2021

Plan

Table of Contents

$k[X_1, \ldots, X_n]$ est factoriel et nothérien (transfert), principal si $n = 1$.

Variété algébrique affine
$V(G) = \{x = (x_1, \cdots, x_n) \in k^n : \forall g \in G \ f(x) = 0\} = G^{\perp} \subseteq \mathbb{A}_k^n$,
$G \subseteq k[X_1, \ldots, X_n]$; $V(G) = V(\langle G \rangle)$.

$\cap_i V(G_i) = V(\cup_i G_i)$ et $V(G_1) \cup V(G_2) = V(\langle G_1 \rangle \cap \langle G_2 \rangle)$. Les variétés algébriques affines sont les fermés de la topologie de Zariski.

Fermé irréductible. Dimension et degré.

La division multivariée par une base de Gröbner fournit un représentant de la classe modulo l'idéal. Dans le cas d'une variable, elle correspond à la division euclidienne usuelle.

La base de Gröbner (minimale)-réduite d'un idéal correspond à son générateur unitaire dans le cas univarié (d'une seule indéterminée).

Maintes propriétés d'un idéal, de l'anneau quotient, de la variété algébrique affine, se lisent sur les bases de Gröbner.

Elles permettront en particulier de "résoudre" certains systèmes d'équations polynomiales ...

Un objet central sera le belordre produit sur $\mathbb{N}^n$, belordre comme produit de beaux ordres, les beaux ordres linéaires étant les bons ordres.

1. Les ordres monomiaux sont des extensions linéaires de $\mathbb{N}^n$.
   Les extensions linéaires des beaux ordres sont des bons ordres. (Et réciproquement avec du choix.)
2. Les idéaux monomiaux correspondront aux sections finales de $\mathbb{N}^n$. On peut en fait se dispenser de les considérer explicitement.
   Un ordre est un belordre ùssiù chacune de ses section finales est finiment engendrée, auquel cas l'ensemble de ses sections initiales est bien fondé pour l'inclusion (et réciproquement, avec du choix).
3. ...

Table of Contents

Les monômes $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathbb{M}_n$ s'identifient aux uplets $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ d'exposants.

L'ordre de divisibilité de $\mathbb{M}_n$ correspond à l'ordre produit sur $\mathbb{N}^n$.

L'ordre lexicographique sur les monômes :

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} <_{\text{Lex}} X_1^{\beta_1} \cdots X_n^{\beta_n} :\Leftrightarrow \exists i : (\alpha_i < \beta_i \wedge (j < i \rightarrow \alpha_j = \beta_j))$$

L'ordre gradué-lexicographique sur les monômes :

$$X^\alpha <_{\text{DegLex}} X^\beta :\Leftrightarrow |\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } X^\alpha <_{\text{Lex}} X^\beta)$$

$|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Il s'agit de bons ordres $\preccurlyeq$ de minimum $1 = X^0 \preccurlyeq X^\delta$ et pour lesquels les translations sont croissantes : $X^\alpha \preccurlyeq X^\beta \Rightarrow X^\gamma X^\alpha \preccurlyeq X^\gamma X^\beta$.
On parlera d'ordre monomiaux.
Ils étendent la divisibilité : $X^\alpha | X^\beta \Rightarrow X^\alpha \preccurlyeq X^\beta : X^\alpha (X^0 \preccurlyeq X^\delta)$.

On s'intéresse aux ordres totaux sur l'ensemble $\mathbb{M}_n$, des monômes de $k[X_1, \ldots, X_n]$, pour lesquels le monômes neutre est minimum et les homothéties sont croissantes. Rappelons qu'ils étendent la relation de divisibilité.

Il n'existe qu'un ordre monomial en une seule indéterminée : $X^m \prec X^n \Leftrightarrow m < n$ (l'ordre de divisibilité est déjà total).

Il résultera de considérations de belordre de base que ce sont des bons ordres.

(L'ordre de divisibilité de $\mathbb{M}_n$ est beau -et en particulier bien fondé-, de sorte que ses extensions sont belles, et en particulier bien fondées, et en particulier ses extensions linéaires sont bonnes.)

$|\alpha| = \alpha_1 + \cdots + \alpha_n$. $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. $X_1 > \cdots > X_n$.
$X_1^{\alpha_1} \cdots X_n^{\alpha_n} < X_1^{\beta_1} \cdots X_n^{\beta_n}$; $(\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n)$; $\alpha < \beta$:

1. Lex. $\exists i : (\alpha_i < \beta_i \wedge (j < i \to \alpha_j = \beta_j))$
2. DegLex : $(|\alpha| < |\beta|) \vee ((|\alpha| = |\beta|) \wedge (\alpha <_{\text{Lex}} \beta))$
3. DegRevLex : $(|\alpha| < |\beta|) \vee ((|\alpha| = |\beta|) \wedge (\alpha >_{\text{Lex}} \beta))$
   NB : Il correspond au précédent en renversant l'ordre des variables ET l'ordre sur les exposants.
4. Par blocs, lexicographiquement. $((\mathbb{N}^p, \leq_1) \times (\mathbb{N}^q, \leq_2), \leq_{\text{Lex}})$:
   $$X^\alpha X^{\alpha'} < X^\beta X^{\beta'} \iff (X^\alpha <_1 X^\beta) \vee (X^\alpha = X^\beta \wedge X^{\alpha'} <_2 X^{\beta'})$$
5. Pour un n-uplet $\lambda \in A_{\geq 0}$ $\mathbb{Z}$-libre d'un anneau ordonné A :
   $\alpha <_\lambda \beta \Leftrightarrow \lambda \cdot \alpha < \lambda \cdot \beta$. Ex : $A = \mathbb{R}$ et $\lambda = (1, \sqrt{2}, \sqrt{3})$.
6. Pour $A \in M_{n,n}(\mathbb{Z})$ non singulière et dont les premiers coefficients non nuls de chaque colonne sont positifs : $\alpha <_A \beta \Leftrightarrow A\alpha <_{\text{Lex}} A\beta \Leftrightarrow 0 <_{\text{Lex}} A(\beta - \alpha)$.
   Les trois premiers sont de cette forme. Ex : $A = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{smallmatrix}\right)$.

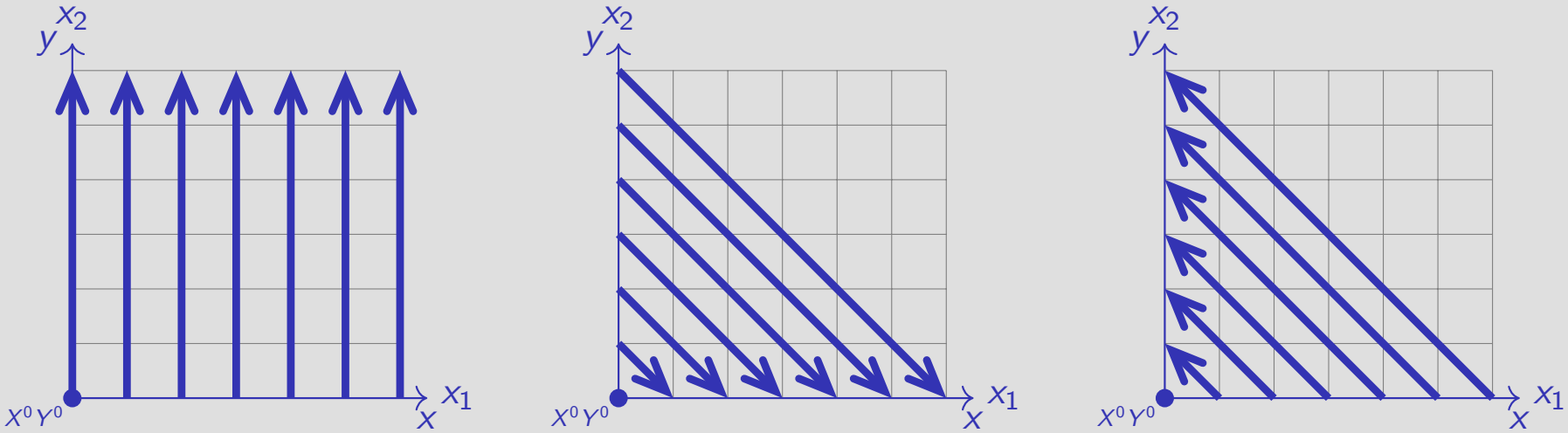
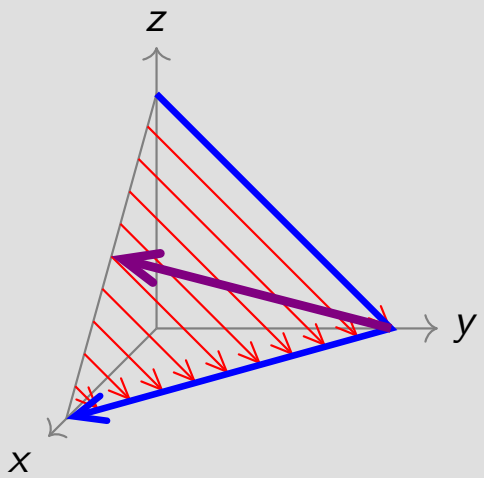


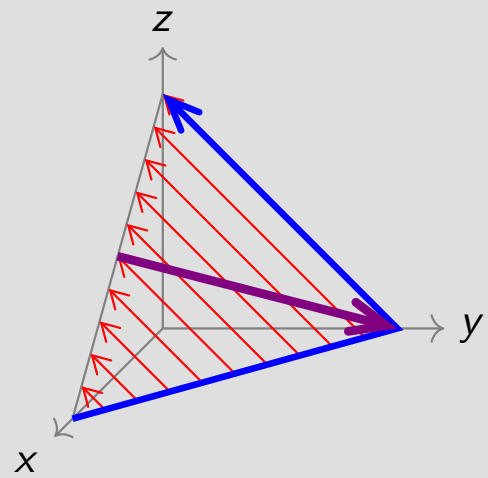
Figure – Trois ordres monomiaux en 2 variables

La distinction n'apparaît qu'à partir de trois indéterminées.

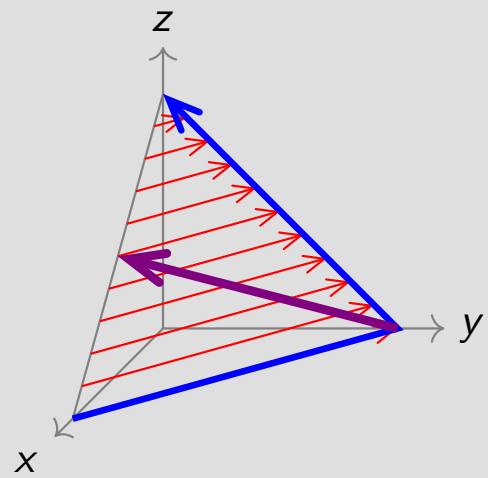
$x^{2n} \preccurlyeq x^k y^{2(n-k)} z^k \preccurlyeq y^{2n} \prec z^{2n}$ $\qquad$ $x^{2n} \prec y^{2n} \preccurlyeq x^k y^{2(n-k)} z^k \preccurlyeq z^{2n}$



$\mathrm{Lex}_{x \succ y \succ z}$



$\mathrm{RevLex}_{x \succ y \succ z}$ ou InvLex



$\mathrm{LexRev}_{x \succ y \succ z} = \mathrm{Lex}_{z \succ y \succ x}$

Figure – $d = 2n = 10$

monôme, exposant, terme, coefficient dominants ("L" pour Leading), d'un polynôme non nul f, relativement à un ordre total $\preccurlyeq$ sur les monômes :

$$f = \underbrace{\mathrm{Lc}_{\preccurlyeq}(f)\overbrace{X^{\mathrm{Le}_{\preccurlyeq}(f)}}^{\mathrm{Lm}_{\preccurlyeq}(f)}}_{\mathrm{Lt}_{\preccurlyeq}(f)} + \mathrm{Tail}_{\preccurlyeq}(f)$$

avec $\mathrm{Tail}_{\preccurlyeq}(f) = o_{\preccurlyeq}(f)$, où $o_{\preccurlyeq}(f)$, resp. $\mathcal{O}_{\preccurlyeq}(f)$, représente toute combinaison linéaire (éventuellement vide) de monômes strictement inférieurs, resp. inférieurs, au monôme dominant de f.

On conviendra : $\mathrm{Le}_{\preccurlyeq}(0) = -\infty$.
Comme dans le cas d'une seule indéterminée :
$\mathrm{Lt}_{\preccurlyeq}(fg) = \mathrm{Lt}_{\preccurlyeq}(f)\,\mathrm{Lt}_{\preccurlyeq}(g)$. $\mathrm{Lm}_{\preccurlyeq}(fg) = \mathrm{Lm}_{\preccurlyeq}(f)\,\mathrm{Lm}_{\preccurlyeq}(g)$.
$\mathrm{Lc}_{\preccurlyeq}(fg) = \mathrm{Lc}_{\preccurlyeq}(f)\,\mathrm{Lc}_{\preccurlyeq}(g)$. $\mathrm{Le}_{\preccurlyeq}(fg) \preccurlyeq \mathrm{Le}_{\preccurlyeq}(f) + \mathrm{Le}_{\preccurlyeq}(g)$.

$\mathrm{Le}_{\preccurlyeq}(f+g) \leq \mathrm{Le}_{\preccurlyeq}(f) \curlyvee \mathrm{Le}_{\preccurlyeq}(g)$. $\mathrm{Lm}_{\preccurlyeq}(f+g) \preccurlyeq \mathrm{Lm}_{\preccurlyeq}(f) \curlyvee \mathrm{Lm}_{\preccurlyeq}(g)$.

Chacune des deux propriétés suivantes caractérise l'ordre $\mathrm{Lex}_{X_1 \succ \ldots \succ X_n}$ parmi les ordres monomiaux.
D'abord informellement :

1. Les monômes en les dernières indéterminées constituent une section initiale.
2. Les monômes où apparaît une des premières indéterminées constituent une section finale.

Plus formellement (reformuler les choses sans faire apparaître le corps, également implicite dans la seconde formulation) :

1. Chaque $\mathbb{M}_n \cap k[X_i, \ldots, X_n]$ est une section intiale $(1 \leq i \leq n)$.
2. Chaque $\mathbb{M}_n \cap \langle X_1, \ldots, X_j \rangle$ est une section finale $(1 \leq j \leq n)$.

Anticipant, en termes de termes dominants des polynômes (ou du plus grand élément d'un ensemble fini de monômes) :

1. $\forall f \in k[X_1, \ldots, X_n] : \mathrm{Lt}_{\preccurlyeq}(f) \in k[X_i, \ldots, X_n] \Rightarrow f \in k[X_i, \ldots, X_n]$.
2. $\forall f \in k[X_1, \ldots, X_n] : \mathrm{Lt}_{\preccurlyeq}(f) \in \langle X_1, \ldots, X_j \rangle \Rightarrow f \in \langle X_1, \ldots, X_j \rangle$.

Chacune des deux propriétés suivantes caractérise l'ordre $\mathrm{RevLex}_{X_1 \succ \cdots \succ X_n}$ parmi les ordres monomiaux.

1. $\forall f \in k[X_1, \ldots, X_n] : \mathrm{Lt}_{\preccurlyeq}(f) \in \langle X_i, \ldots, X_n \rangle \Rightarrow f \in \langle X_i, \ldots, X_n \rangle$, $1 \leq i \leq n$.
2. $\forall f \in k[X_1, \ldots, X_n] : \mathrm{Lt}_{\preccurlyeq}(f) \in k[X_1, \ldots, X_j] \Rightarrow f \in k[X_1, \ldots, X_j]$, $1 \leq j \leq n$.

Parmi les ordre monomiaux pour lequel le degré croît avec l'ordre, chacune des deux propriétés suivantes caractérise l'ordre $\mathrm{DegRevLex}_{X_1 \succ \cdots \succ X_n}$, où $k[X_1, \ldots, X_n]_d$ désigne l'ensemble des polynômes homogènes [1] de degré d (ou nul).

1. $\forall f \in k[X_1, \ldots, X_n]_d : \mathrm{Lt}_{\preccurlyeq}(f) \in \langle X_i, \ldots, X_n \rangle \Rightarrow f \in \langle X_i, \ldots, X_n \rangle$, $1 \leq i \leq n$, $d \in \mathbb{N}$.
2. $\forall f \in k[X_1, \ldots, X_n]_d : \mathrm{Lt}_{\preccurlyeq}(f) \in k[X_1, \ldots, X_j] \Rightarrow f \in k[X_1, \ldots, X_j]$, $1 \leq j \leq n$, $d \in \mathbb{N}$.

1. $k_d[X_1, \ldots, X_n]$ désignera l'ensemble des polynômes de degré au plus d. Ainsi $k[X_1, \ldots, X_n] = \bigoplus_d k[X_1, \ldots, X_n]_d = \bigcup_d k_d[X_1, \ldots, X_n]$.

Étant donnés un corps k et un entier n, on considère la k-algèbre $A := k[X_1, \ldots, X_n]$. Soit en outre un ordre monomial $\preccurlyeq$. On constatera qu'un bon ordre quelconque sur les monômes suffit. Noter que pour un idéal I de A, qui en est en particulier un sous-k-espace vectoriel, l'anneau quotient A/I est également un k-espace vectoriel ; il s'agit même d'une k-algèbre.

Le théorème de Macaulay généralise au cas multivarié le fait que pour tout polynôme f en une indéterminée, l'espace vectoriel quotient $k[X]/(f)$ admet pour base l'ensemble de classes des monômes d'exposant strictement inférieurs au degré de f.

Théorème de la base de Macaulay : Étant donné un idéal I de $A = k[X_1, \ldots, X_n]$, la projection canonique de A sur A/I se restreint en un isomorphisme de k-espaces vectoriels à l'ensemble des polynômes dont aucun monôme n'est monôme dominant d'un élément de I. Autrement dit, A/I admet $(\overline{m}^I : m \in B)$ pour base, où $B := \mathbb{M}_n \setminus \mathrm{Lm}_{\preccurlyeq}[I]$.

Théorème de la base de Macaulay : Étant donné un idéal I de $A = k[X_1, \ldots, X_n]$, la projection canonique de A sur A/I se restreint en un isomorphisme de k-espaces vectoriels à l'ensemble des polynômes dont aucun terme n'est terme $\preccurlyeq$-dominant d'un élément de I. Autrement dit, A/I admet $(\overline{m}^I : m \in B)$ pour base, où $B := \mathbb{M}_n \setminus \mathrm{Lm}_{\preccurlyeq}[I]$.

B est bien générateur modulo I : Observer que si $\mathrm{Supp}(f) \not\subseteq B$, autrement dit si f a un monôme, m, qui est monôme dominant d'un $g \in I$, alors pour un sacalaire non nul c, $f - cg$ est un polynôme I-congru à f dont le support, inclus dans $(\mathrm{Supp}(f) \cup \mathrm{Supp}(g))\backslash\{m\}$, est strictement inférieur à $\mathrm{Supp}(f)$ pour le bon ordre lexicographique descendant de $\wp_{\mathrm{fin}}(\mathbb{M}_n)$: on y a remplacé l'élément m par des éléments strictement inférieurs.

B est libre modulo I : Si f est combinaison linéaire non triviale d'éléments de B, alors il est en particulier non nul, par liberté (absolue) de B, de sorte qu'on peut considérer son monôme $\preccurlyeq$-dominant. Par ailleurs, $\mathrm{Lm}_{\preccurlyeq}(f) \in \mathrm{Supp}(f) \subseteq B$, de sorte que $f \notin I$, par définition de B.

Exercice : Formaliser la notion de *base modulo un sous-espace vectoriel*, implicite dans la formulation ci-dessus du raisonnement.

Remarque : Quelque soit l'ordre total $\preccurlyeq$ considéré sur $\mathbb{M}_n$, B est I-libre. Quant au fait qu'il soit I-générateur, cela repose juste sur le fait que l'ordre total $\preccurlyeq$ est bien fondé. On n'a pas besoin qu'il soit compatible avec la divisibilité.

Exemple (*cf.* KrRob) : Considérer l'idéal $I := (X^2 - X)$ de $k[X]$. Pour l'ordre inverse de celui de divisibilité, $B = \{1\}$, tandis que A/I est de dimension 2. Noter d'ailleurs qu'ici, l'argument de preuve que nous donnons, appliqué au polynôme X, ne donne pas lieu à une convergence vers un élément congru engendré par B, mais à une suite divergente : $X \xrightarrow{X^2-X} X^2 \xrightarrow{X(X^2-X)} X^3 \xrightarrow{X^2(X^2-X)} X^4 \to \cdots$

Remarque : On peut contourner le recours à l'ordre des parties finies de $\mathbb{M}_n$, en procédant par l'absurde. Considérer en effet un contre-exemple (un f congru à aucune combinaison linéaire de B, qu'on peut supposer unitaire) de monôme dominant minimum m. La considération de $g := f - m$ conduit à une contradiction. En effet, g ne saurait être nul, sinon f serait congru à une combinaison d'éléments de B. Dans ce cas, le monôme dominant de g est strictement inférieur à celui de f, de sorte que, par minimalité de f, g doit être congru à une combinaison linéaire de B, tandis que $f - g = m$, ce qui proscrit $m \in B$ et $m \in \mathrm{Lm}_{\preccurlyeq}[I]$, contredisant leur complémentarité.
(Cette observation est vraisemblablement de portée générale.)

Anticipant, étant donnée une $\preccurlyeq$-base de Gröbner G de I, ces polynômes sont les polynômes $\xrightarrow[\mathsf{Lm}_{\preccurlyeq}\uparrow G]{}$-irréductibles.

Préciser, étant donnée une base de Gröbner G de I, les propriétés de l'application reste : $f \mapsto \overrightarrow{f}^{G,\preccurlyeq}$.

Préciser également ...

Observation : Pour un ordre monomial $\preccurlyeq$, l'ensemble $\mathrm{Lm}_{\preccurlyeq}[I] \subseteq \mathbb{M}_n$ des monômes dominants des éléments non nuls d'un idéal I de $A = k[X_1, \ldots, X_n]$ est stable par produit et donc est une section finale pour l'ordre de divisibilité (pas pour $\preccurlyeq$).

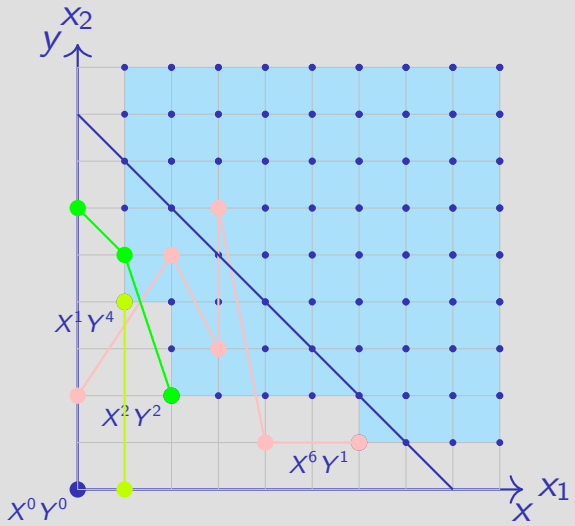


Figure – Noter les cas où A/I est de dimension finie. Il n'est pas sûr que le système de trois ensemble de monômes en question corresponde bien à une base de Gröbner. C'est le cas ssi l'escalier engendré est la partie bleue. Tout escalier est réalisable par un unique idéal monomial.

En pratique, pour déterminer l'escalier d'un idéal, relativement à un ordre **monomial**, on considère une base de Gröbner, qu'on obtient par l'alogorithme de Buchberger.

Table of Contents

$$f \xrightarrow[G,\prec]{g} f - \frac{\mathrm{Lt}^G_\prec(f)}{\mathrm{Lt}_\prec(g)} g = f - \frac{\mathrm{Lc}^G_\prec(f)}{\mathrm{Lc}_\prec(g)} X^{\mathrm{Le}^G_\prec(f) - \mathrm{Le}_\prec(g)} g$$

$\mathrm{Lt}^G_\prec(f)$ étant le plus haut terme de f divisible par le monôme dominant d'un élément de G, et $g \in G$ un témoin, éventuellement le premier pour une énumération $\overrightarrow{G} = (g_1, \ldots, g_k)$ de G : $\xrightarrow[\overrightarrow{G},\prec]{}$ est déterministe.

Observer que $\xrightarrow[G,\prec]{} \subseteq \equiv_{\langle G \rangle}$: $f_1 \xrightarrow[G,\prec]{} f_2 \Rightarrow f_2 - f_1 \in \langle G \rangle$, l'idéal engendré par G.

La procédure termine, par décroissance stricte de $\mathrm{Lm}^G_\prec(f)$:

$$f_1 \xrightarrow[G,\prec]{} f_2 \Longrightarrow \mathrm{Lm}^G_\prec(f_1) \succ \mathrm{Lm}^G_\prec(f_2)$$

tandis que $\mathrm{Lm}_\prec(f_1) \succcurlyeq \mathrm{Lm}_\prec(f_2)$ et $f_1 - f_2 = \mathcal{O}^G_\prec(f_1)$. (Notation à venir.)

$$\exists r : f \xrightarrow[G,\prec]{*!} r, \text{ resp. } f \xrightarrow[\overrightarrow{G},\prec]{*!} \overline{f}^{\overrightarrow{G},\prec}$$

aucun terme de r n'étant divisible par le monôme dominant d'un $g \in G$ et $f - r = \mathcal{O}^G_\prec(f)$.

Un tel reste r n'est en général pas unique (il peut dépendre de l'énumération de G). Il peut également appartenir à $\langle G \rangle \setminus \{0\}$.

La relation binaire $\xrightarrow[\{xy-1,y^2-1\},\mathrm{Lex}_{x\succ y}]{}$ n'est pas confluente :

$$\begin{aligned} x^2y+xy^2+y^2 &= (x+y)\cdot(xy-1)+1\cdot(y^2-1)+(x+y+1)\\ &= (x+1)\cdot(y^2-1)+x\cdot(xy-1)+(2x+1)\end{aligned}$$

$$\begin{cases} \overline{x^2y+xy^2+y^2}^{(xy-1,y^2-1),\mathrm{Lex}_{x\succ y}} = x+y+1\\ \overline{x^2y+xy^2+y^2}^{(y^2-1,xy-1),\mathrm{Lex}_{x\succ y}} = 2x+1\end{cases}$$

$$\begin{aligned} xy^2-x &= y\cdot(xy-1)+0\cdot(y^2-1)+(-x+y)\\ &= x\cdot(y^2-1)+0\cdot(xy-1)+0\end{aligned}$$

$-x+y$ est un élément $\xrightarrow[\{xy-1,y^2-1\},\mathrm{Lex}_{x\succ y}]{}$-irréductible non nul de $\langle xy-1,y^2-1\rangle$.

```
R.<x,y>=PolynomialRing(QQ,order='lex')

def division(f,G) : # G liste ou uplet de polynomes
    k=len(G) ; Q=[0]*k ; r=0*x
    while f!= 0*x :
        t=f.lt()
        for i in range(k) :
            g=G[i] ; ti=g.lt()
            if R.monomial_divides(ti,t) :
                q=R.monomial_quotient(t,ti,coeff=True)
                Q[i]=Q[i]+q ; f=f-q*g
                break
        else :
            f=f-t ; r=r+t
    return (Q,r)

division(x^2+1,[])
> ([], x^2 + 1)
```

```
1  def divisionRec(f,G) : # G liste ou uplet de polynomes
2      k=len(G) ; Q=[0]*k ; r=0*x
3      return divisionAux(f,G,Q,r,0,k)
4
5  def divisionAux(f,G,Q,r,i,k) : # 0<= i <= k
6      if f==0*x :
7          return (Q,r) # retour final
8      t=f.lt()
9      if i==k : return divisionAux(f-t,G,Q,r+t,0,k)
10     g=G[i] ; ti=g.lt()
11     if not R.monomial_divides(ti,t) :
12         return divisionAux(f,G,Q,r,i+1,k)
13     q=R.monomial_quotient(t,ti,coeff=True)
14     Q[i]=Q[i]+q ; f=f-q*g
15     return divisionAux(f,G,Q,r,0,k)
```

```
1  R.<x,y>=PolynomialRing(QQ,order='lex')
2
3  def divisionsComparaison(f,T) : #T tuple de polyn mes
4      (g,h)=T ; G=[g,h] ; H=[h,g]
5      print('division(',f,',',G,')=',division(f,G))
6      print('divisionRec(',f,',',G,')=',divisionRec(f,G))
7      print('(',f,').reduce(',G,')=',f.reduce(G))
8      print('division(',f,',',H,')=',division(f,H))
9      print('divisionRec(',f,',',H,')=',divisionRec(f,H))
10     print('(',f,').reduce(',H,')=',f.reduce(H))
```

```
1  R.<x,y>=PolynomialRing(QQ,order='lex')
2
3  divisionsComparaison(x*y^2+1,(x*y+1,y+1))
4  > division( x*y^2 + 1 , [x*y + 1, y + 1] )= ([y, -1], 2)
5  > divisionRec( x*y^2 + 1 , [x*y + 1, y + 1] )= ([y, -1],
6  > ( x*y^2 + 1 ).reduce( [x*y + 1, y + 1] )= x + 1
7  > division( x*y^2 + 1 , [y + 1, x*y + 1] )= ([x*y - x, 0]
8  > divisionRec( x*y^2 + 1 , [y + 1, x*y + 1] )= ([x*y - x
9  > ( x*y^2 + 1 ).reduce( [y + 1, x*y + 1] )= x + 1
10
11 divisionsComparaison(x*y-x,(x-y,x-y^2)) # BookSage page
12 > division( x*y - x , [x - y, x - y^2] )= ([y - 1, 0], y
13 > divisionRec( x*y - x , [x - y, x - y^2] )= ([y - 1, 0]
14 > ( x*y - x ).reduce( [x - y, x - y^2] )= y^3 - y^2
15 > division( x*y - x , [x - y^2, x - y] )= ([y - 1, 0], y
16 > divisionRec( x*y - x , [x - y^2, x - y] )= ([y - 1, 0]
17 > ( x*y - x ).reduce( [x - y^2, x - y] )= y^2 - y
```

On peut considérer la relation plus générale ci-dessous :

$$f \xrightarrow[\mathsf{Lm}_{\preccurlyeq}\restriction G]{} f - \frac{t}{\mathsf{Lt}_{\preccurlyeq}(g)} g = f - \frac{c}{\mathsf{Lc}_{\preccurlyeq}(g)} X^{\alpha - \mathsf{Le}_{\preccurlyeq}(g)} g$$

où $t = cX^{\alpha}$ est **un** terme non nul de f divisible par le monôme dominant d'**un** élément g de G, pas nécessairement le plus haut possible.
On ne se soucie pas d'ordonner les termes du dividende, ni l'ensemble des diviseurs. On isole juste le terme dominant de chacun des diviseurs.
Noter ce que dit cette observation dans le cas d'une variable.

La procédure termine, par décroissance stricte de l'ensemble des monômes de f, pour l'ordre des ensemble finis de monôme, correspondant à l'ordre lexicographique droite de $2^{(\mathbb{M}_n \preccurlyeq)}_{\leq}$: $f \mapsto \mathsf{Supp}(f)$ est un morphisme de $(k[X_1, \ldots, X_n], \xrightarrow[\mathsf{Lm}_{\preccurlyeq}\restriction G]{})$ vers $(\wp_{\mathrm{fin}}(\mathbb{M}_n), \overset{\text{droite}}{\underset{\text{Lex}}{\succ}})$ ($\xleftarrow[\mathsf{Lm}_{\preccurlyeq}\restriction G]{}$ vers $\overset{\text{droite}}{\underset{\text{Lex}}{\prec}}$).

On introduit ainsi du non déterminisme (éventuellement supplémentaire pour le cas où on ne considère pas d'ordre particulier sur G). Cela n'élimine pas de formes irréductibles. Préciser si les formes réduites d'un polynôme en sont les restes pour les énumérations de G.

Le $(\overrightarrow{G}, \preccurlyeq)$-reste d'un polynôme peut dépendre de l'ordre de G.

En particulier un polynôme peut admettre plusieurs formes $\xrightarrow[\mathsf{Lm}_{\preccurlyeq} \restriction G]{}$-réduites, et en particulier la relation $\xrightarrow[\mathsf{Lm}_{\preccurlyeq} \restriction G]{}$ peut ne pas être confluente.

En outre, des éléments non nuls de $\langle G \rangle$ peuvent être $(\overrightarrow{G}, \preccurlyeq)$-irréductibles, resp. $\xrightarrow[\mathsf{Lm}_{\preccurlyeq} \restriction G]{}$-irréductibles.

Il se trouve que toutes ces propriétés "indésirables" sont équivalentes.

Dans le cas "désirable", on dit que G est une base de Gröbner.

L'existence de bases de Gröbner d'un idéal (pas l'équivalence entre les diverses caractérisations ?) repose sur des considérations du belordre, au travers du Lemme de Dickson et de son corollaire, le théorème de la base de Hilbert. La terminaison de l'algorithme de Buchberger, permettant d'en construire, repose également dessus (*via* la nothérianité).

$$f \xrightarrow[G,\prec]{g} f - \frac{\mathrm{Lt}^G_\prec(f)}{\mathrm{Lt}_\prec(g)} g = f - \frac{\mathrm{Lc}^G_\prec(f)}{\mathrm{Lc}_\prec(g)} X^{\mathrm{Le}^G_\prec(f) - \mathrm{Le}_\prec(g)} g$$

$\mathrm{Lt}^G_\prec(f)$ étant le plus haut terme divisible par le monôme dominant d'un élément de G. On peut être moins restrictif :

$$f \xrightarrow[\mathrm{Lm}_\prec \restriction G]{g} f - \frac{t}{\mathrm{Lt}_\prec(g)} g = f - \frac{c}{\mathrm{Lc}_\prec(g)} X^{e - \mathrm{Le}_\prec(g)} g$$

$t = cX^e$ étant un terme non nul de f. On peut, au contraire l'être plus :

$$f \xrightarrow[\overrightarrow{G},\prec]{g} f - \frac{\mathrm{Lt}^G_\prec(f)}{\mathrm{Lt}_\prec(g)} g = f - \frac{\mathrm{Lc}^G_\prec(f)}{\mathrm{Lc}_\prec(g)} X^{\mathrm{Le}^G_\prec(f) - \mathrm{Le}_\prec(g)} g$$

où $\overrightarrow{G} = (g_1, \ldots, g_k)$ est une énumération de G et g est la première composante possible suivant cette énumération. La relation $\xrightarrow[\mathrm{Lm}_\prec \restriction G]{}$ (et *a fortiori* les autres) termine, mais $\xrightarrow[G,\prec]{}$ (et *a fortiori* $\xrightarrow[\mathrm{Lm}_\prec \restriction G]{}$) peut ne pas converger. Quant à $\xrightarrow[\overrightarrow{G},\prec]{}$, elle est déterministe.

Comme, de plus, elle termine, on note $\overline{f}^{\overrightarrow{G},\prec}$ la forme réduite du polynôme f.

De la réductibilité des éléments de $\langle G \rangle$

La division multivariée, même non déterministe, ne permet pas toujours d'exprimer un élément d'un idéal en fonction de générateurs, même en une seule indéterminée.

Exemple d'un élément de le l'idéal ne se réduisant pas en 0 : $G = \{X^4, X^3 - X\}$

$$\langle G \rangle \ni 1X^4 - X(X^3 - X) = X^2 \not\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$$

En général, il se peut que, dans une décomposition d'un élément de $\langle G \rangle$:

$$f = \sum_g h_g g, \text{ resp. } f = \sum_i t_i g_i \text{ où les } t_i \text{ sont des termes}$$

les grands termes dominants d'une telle somme se compensent, et ainsi que $\mathrm{Lt}_{\preccurlyeq}(f) \prec \mathrm{Max}_{\preccurlyeq} \mathrm{Lt}_{\preccurlyeq}(h_g g)$, resp. $\mathrm{Lt}_{\preccurlyeq}(f) \prec \mathrm{Max}_{\preccurlyeq} \mathrm{Lt}_{\preccurlyeq}(t_i g_i)$. En particulier, il se peut que le terme dominant de f ne soit divisible par celui d'aucun élément de G.

Il se trouve que si cela se produit alors cela se produit pour des décompositions en fonction de deux générateurs seulement. On y reviendra. Ainsi, l'exemple ci-dessus est-il "générique".

C'est sur cette observation qu'est basé l'algorithme de Buchberger, qui permet de construire une base de Gröbner à partir d'une partie génératrice finie.

Notation $\mathcal{O}^G_{\preccurlyeq}(f)$

Notation : Étant donné un ordre monomial $\preccurlyeq$, pour chaque partie G de $A := k[X_1, \ldots, X_n]$, on désigne pour chaque $f \in A$, par $\mathcal{O}^G_{\preccurlyeq}(f)$ l'ensemble des polynômes admettant une décomposition comme somme à support fini ("expression de f comme élément de $\langle G \rangle$, par le bas") :

$$\sum_{g \in G} h_g g, \text{ où } \mathrm{Lm}_{\preccurlyeq}(h_g g) \preccurlyeq \mathrm{Lm}_{\preccurlyeq}(f)$$

Noter qu'on peut supposer que les h_g sont des termes t_i, quitte à répliquer les g :

$$\sum_i t_i g_i, \text{ où } \mathrm{Lm}_{\preccurlyeq}(t_i g_i) \preccurlyeq \mathrm{Lm}_{\preccurlyeq}(f)$$

Noter que $0 \in \mathcal{O}^G_{\preccurlyeq}(f) \subseteq \langle G \rangle$ et que $\mathcal{O}^G_{\preccurlyeq}(0) = \{0\}$, et que $\mathcal{O}^G_{\preccurlyeq}(f)$ est un k-ev.

Observation :

$$\boxed{f_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} f_2 \Longrightarrow f_2 - f_1 \in \mathcal{O}^G_{\preccurlyeq}(f_1)}$$

On envisagera ultérieurement le cas d'un ordre compatible partiel.

1. Terminaison :
   - 1.1 $\xleftarrow[G,\succcurlyeq]{} \subseteq (\mathsf{Lt}^G_{\succcurlyeq})^* \succcurlyeq$ *i.e.*, $f_2 \xleftarrow[G,\succcurlyeq]{} f_1 \Rightarrow \mathsf{Lt}^G_{\succcurlyeq}(f_2) \succcurlyeq \mathsf{Lt}^G_{\succcurlyeq}(f_1)$.
   - 1.2 $\xleftarrow[G,\succcurlyeq]{} \subseteq (\mathsf{Lt}_{\overrightarrow{G},\succcurlyeq})^* \succcurlyeq$.
   - 1.3 $\xleftarrow[\mathsf{Lm}_{\succcurlyeq}\restriction G]{} \subseteq \mathsf{Supp}^*(\succcurlyeq^{\text{droite}}_{\text{Lex}} \restriction \wp_{\text{fin}}(\mathbb{M}_n))$, *i.e.*,
     $f_2 \xleftarrow[\mathsf{Lm}_{\succcurlyeq}\restriction G]{} f_1 \Rightarrow \mathsf{Supp}(f_2) \succcurlyeq^{\text{droite}}_{\text{Lex}} \mathsf{Supp}(f_1)$.
2. $\xleftrightarrow[\mathsf{Lm}_{\succcurlyeq}\restriction G]{*}$ est la congruence modulo I.
3. $\xrightarrow[\mathsf{Lm}_{\succcurlyeq}\restriction G]{}$ peut ne PAS être confluente.

Terminaison

En général, pour toute relation binaire $\leftarrow$ sur un ensemble donné, la relation $\overset{*}{\leftarrow}$ est un préordre sur cet ensemble. Ce préordre est un ordre bien fondé ùssiù $\leftarrow$ admet un morphisme dans une relation bien fondée.
A priori :

$$\xleftarrow[\mathsf{Lm}_{\preccurlyeq} \restriction G]{} \subseteq \mathsf{Supp}^*(\preccurlyeq_{\mathrm{Lex}}^{\mathrm{droite}} \restriction \wp_{\mathrm{fin}}(\mathbb{M}_n)) \implies$$

$$\mathrm{ht}(k[X_1, \ldots, X_n], \xleftarrow[\mathsf{Lm}_{\preccurlyeq} \restriction G]{}) \leq \mathrm{ht}(\wp_{\mathrm{fin}}(\mathbb{M}_n), \preccurlyeq_{\mathrm{Lex}}^{\mathrm{droite}}) = 2^{\mathrm{ht}(\mathbb{M}_n, \preccurlyeq)}$$

$$\xleftarrow[G, \preccurlyeq]{} \subseteq (\mathsf{Lt}_{\preccurlyeq}^{G})^* \preccurlyeq \implies \mathrm{ht}(k[X_1, \ldots, X_n], \xleftarrow[G, \preccurlyeq]{}) \leq \mathrm{ht}(\mathbb{M}_n, \preccurlyeq)$$

$$\xleftarrow[\overrightarrow{G}, \preccurlyeq]{} \subseteq (\mathsf{Lt}_{\preccurlyeq}^{G})^* \preccurlyeq \implies \mathrm{ht}(k[X_1, \ldots, X_n], \xleftarrow[\overrightarrow{G}, \preccurlyeq]{}) \leq \mathrm{haut}(\mathbb{M}_n, \preccurlyeq)$$

La plus grande valeur possible de $\mathrm{ht}(\mathbb{M}_n, \preccurlyeq)$ est ω^n (obtenue en particulier pour l'ordre lexicographique ; vérifier s'il y en a d'autres). Noter que $2^{\omega^n} = \omega^{\omega^{n-1}}$.

En fait, chacune des ces relation est de hauteur ω lorsque G est fini, étant donné que pour chaque polynôme f_1, il n'existe qu'un nombre fini de f_2 tels que $f_1 \to f$, majoré par le produit du cardinal de G et du nombre de termes de f.
Préciser ce qu'il en est lorsque G est infini.

Propriétés de compatibilité entre $\xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{}$ et la structure d'anneau.

1. $\xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{}\subseteq\equiv_I$.
2. $\forall f_1, f_2 \in R : f_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{cX^e g} f_2 \Longrightarrow \forall t \in k^*\mathbb{M}_n : tf_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{tcX^e g} tf_2$
3. $\forall f_1, f_2 \in R : f_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{cX^e g} f_2 \Longrightarrow \forall f \in R :$

$$\begin{cases} c + c' = 0 \Rightarrow f_1 + f \boxed{\xleftarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{c'X^e g} f_2 + f} \\ c + c' \neq 0 \Rightarrow \exists h \in R : f_1 + f \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{(c+c')X^e g} h \boxed{\xleftarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{c'X^e g} f_2 + f} \end{cases}$$

où $c' \in k$ est le coefficient du terme de f d'exposant $e + \mathrm{Le}_{\preccurlyeq}(g)$.
C'est en fait vrai avec $\xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G]{}$, mais pas avec $\xrightarrow[G,\preccurlyeq]{}$ (f peut avoir un terme plus grand que $cX^e \mathrm{Lt}_{\preccurlyeq}(g)$ divisible par un élément de $\mathrm{Lt}_{\preccurlyeq}[G]$, qui n'est alors pas un terme de f_1, ni de f_2, qui ne diffère de f_1 qu'en deça de $cX^e \mathrm{Lt}_{\preccurlyeq}(g)$).

Rappel :

1. $\xrightarrow[\mathrm{Lm}_{\preccurlyeq}\uparrow G]{}\subseteq\equiv_I$.
2. $\forall f_1, f_2 \in R : f_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\uparrow G]{} f_2 \Rightarrow \forall t \in k^*\mathbb{M}_n : tf_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\uparrow G]{} tf_2$
3. $\forall f_1, f_2 \in R : f_1 \xrightarrow[\mathrm{Lm}_{\preccurlyeq}\uparrow G]{} f_2 \Rightarrow \forall f \in R\ \exists h \in R : f_1 + f \overset{*}{\underset{\mathrm{Lm}_{\preccurlyeq}\uparrow G}{\longrightarrow}} h \overset{*}{\underset{\mathrm{Lm}_{\preccurlyeq}\uparrow G}{\longleftarrow}} f_2 + f$.

PREUVE de $\overset{*}{\underset{\mathrm{Lm}_{\preccurlyeq}\uparrow G}{\longleftrightarrow}}=\equiv_{\langle G\rangle}$:

Remarque : Préciser les cas de $\overset{*}{\underset{G,\preccurlyeq}{\longleftrightarrow}}$ et de $\overset{*}{\underset{\overrightarrow{G},\preccurlyeq}{\longleftrightarrow}}$.

Table of Contents

Bases de Gröbner, relativement à un ordre monomial $\preccurlyeq$

Pour $G \subseteq k[X_1, \ldots, X_n]$ et $I := \langle G \rangle$, équivalence :

1. Tout élément non nul de I est $\xrightarrow[G,\preccurlyeq]{}$-réductible.
2. $\forall f \in I : f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, resp. $f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f)$, resp. $f = \mathcal{O}^G_{\preccurlyeq}(f)$.
3. $\mathrm{Lm}_{\preccurlyeq}[I] \subseteq \mathbb{M}_n \mathrm{Lm}_{\preccurlyeq}[G] : \uparrow_{\leq} \mathrm{Le}[G] = \uparrow_{\leq} \mathrm{Le}[I]$.
4. $\mathrm{Lm}_{\preccurlyeq}[I] \subseteq \langle \mathrm{Lm}_{\preccurlyeq}[G] \rangle$.
5. Les polynômes $\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{}$-irréductibles forment une section de $\equiv_I$.
6. Deux polynômes $\langle G \rangle$-équivalents ont une réduction commune.
7. $\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{}$ est convergente : On notera $\overline{f}^{G,\preccurlyeq}$ la forme réduite de f.
8. La fonction $f \mapsto \overline{f}^{\overrightarrow{G},\preccurlyeq}$ est indépendante de l'énumération de G.
9. la relation $\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{}$ est confluente.
10. Toute paire critique $\xleftarrow{g_1} \mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2) \xrightarrow{g_2}$ conflue (est joignable).
11. $\forall (g_1, g_2) \in G^2$, $S_{\preccurlyeq}(g_1, g_2) \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, resp. $\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} o^G_{\preccurlyeq}(\mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2))$.
12. Relèvement des syzygies $(G, \preccurlyeq)$-homogènes de $\mathrm{Lt}_{\preccurlyeq} \restriction G$, en syzygies de G.

Une telle G est une **base de Gröbner** (de l'idéal qu'elle engendre).

Définition : Étant donné un ordre monomial $\preccurlyeq$, une partie G d'un idéal I en est une base de Gröbner si le monôme dominant de tout élément non nul de I est divisible par celui d'un élément de G : $\cup\{\mathrm{Lm}_{\preccurlyeq}[\langle g\rangle] : g \in G\} = \mathrm{Lm}_{\preccurlyeq}[\langle G\rangle]$.

Ainsi, tout élément non nul de l'idéal peut être réduit au niveau de la tête, le reste étant nul ou de tête strictement inférieure, de sorte qu'en recommençant avec ce reste, et ainsi de suite, on finit par aboutir à un reste nul 0. Autrement dit, chaque élément de l'idéal se $\xrightarrow[G,\preccurlyeq]{*}$-réduit en 0 (en fait, même, toute réduction itérée termine en un élément irréductible, qui ne peut être que nul). En particulier :

Lemme : Une base de Gröbner d'un idéal est génératrice.

On peut alternativement considérer un potentiel élément dont l'ensemble des monômes serait minimum pour l'ordre lexicographique du bon ordre monomial $\preccurlyeq$.

On sait que dans le cas univarié (d'une seule indéterminé), les idéaux sont principaux, et chaque idéal non nul admet un unique générateur unitaire.

Rappelons qu'il n'y a qu'un ordre monomial dans la cas univarié : $X^0 \prec X^1 \prec X^2 \prec \cdots$

Un base de Gröbner d'un idéal I non nul de $k[X]$ en est toute partie contenant un générateur (autrement dit un multiple scalaire non nul du générateur unitaire).

Anticipant, sa base réduite sera le singleton contenant ce générateur unitaire.

De la propriété $f \in \langle G \rangle \Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, **resp.** $\Rightarrow f = \mathcal{O}^G_{\preccurlyeq}(f)$, **resp.** $\Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f)$, **resp.** $\overset{f \neq 0}{\Longrightarrow} f \in \mathrm{Red}(G, \preccurlyeq)$, **resp.** $\overset{f \neq 0}{\Longrightarrow} f \in \mathrm{LeadRed}(G, \preccurlyeq)$

Pour chaque $f \in A$, on dispose des implications suivantes, indépendantes de la terminaison :

$$f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0 \Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} f' \in \mathcal{O}^G_{\preccurlyeq}(f)$$

$$\Leftrightarrow f \in \mathcal{O}^G_{\preccurlyeq}(f) \qquad f - f', f' \in \mathcal{O}^G_{\preccurlyeq}(f) \Rightarrow (f - f') + f' \in \mathcal{O}^G_{\preccurlyeq}(f)$$

$$\overset{\text{si } f \neq 0}{\Longrightarrow} f \in \mathrm{LeadRed}^G_{\preccurlyeq} \qquad \mathrm{Lm}\, f \preccurlyeq \mathrm{Lm} \sum_i t_i g_i \preccurlyeq \mathrm{Max}_i\, \mathrm{Lm}\, t_i g_i \preccurlyeq \mathrm{Lm}\, f$$

$$\Rightarrow f \in \mathrm{Red}^G_{\preccurlyeq}$$

Par ailleurs, si tout $f \in \langle G \rangle$ non nul est $(G, \preccurlyeq)$-réductible, alors tout $f \in \langle G \rangle$ se réduit en 0 : par terminaison, considérer $f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*!} r$; un tel r appartient à $\langle G \rangle$ donc ne saurait être non nul.

De la propriété $f \in \langle G \rangle \Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, **resp.** $\Rightarrow f = \mathcal{O}^G_{\preccurlyeq}(f)$, **resp.** $\Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f)$, **resp.** $\overset{f \neq 0}{\Longrightarrow} f \in \mathrm{Red}(G, \preccurlyeq)$, **resp.** $\overset{f \neq 0}{\Longrightarrow} f \in \mathrm{LeadRed}(G, \preccurlyeq)$

Pour chaque $f \in A$, on dispose des implications suivantes, indépendantes de la terminaison :

$$f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0 \Rightarrow f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f) \Rightarrow f \in \mathcal{O}^G_{\preccurlyeq}(f) \overset{\text{si } f \neq 0}{\Longrightarrow} f \in \mathrm{LeadRed}^G_{\preccurlyeq} \Rightarrow f \in \mathrm{Red}^G_{\preccurlyeq}$$

Par ailleurs, si tout $f \in \langle G \rangle$ non nul est $(G, \preccurlyeq)$-réductible, alors tout $f \in \langle G \rangle$ se réduit en 0.
Ainsi les propriétés suivantes sont équivalentes :
$\forall f \in \langle G \rangle \backslash \{0\} : f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, $\forall f \in \langle G \rangle : f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$,
$\forall f \in \langle G \rangle \backslash \{0\} : f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f)$, $\forall f \in \langle G \rangle : f \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} \mathcal{O}^G_{\preccurlyeq}(f)$,
$\forall f \in \langle G \rangle \backslash \{0\} : f \in \mathcal{O}^G_{\preccurlyeq}(f)$, $\forall f \in \langle G \rangle : f \in \mathcal{O}^G_{\preccurlyeq}(f)$,
$\forall f \in \langle G \rangle \backslash \{0\} : f \in \mathrm{LeadRed}^G_{\preccurlyeq}$: G est une base de Gröbner,
$\forall f \in \langle G \rangle \backslash \{0\} : f \in \mathrm{Red}^G_{\preccurlyeq}$.
On peut supprimer la restriction de non nullité des trois premières propriétés.
L'avant dernière correspond à la définition "officielle" de base de Gröbner.

Observation triviale : Une partie G d'un idéal I en est une base de Gröbner (au sens où le monôme dominant de tout élément de I divise celui d'un élément de G) ùssiù tout élément de $\mathrm{Lm}_{\preccurlyeq}[I]$ est divisible par un élément de $\mathrm{Lm}_{\preccurlyeq}[G]$.

Noter que $\mathrm{Lm}_{\preccurlyeq}[I]$ peut ne pas être un idéal, mais il est stable par multiplication par les monômes, autrement dit, il s'agit d'une section finale de $\mathbb{M}_n$ pour son ordre de divisibilité (pas de $(\mathbb{M}_n, \preccurlyeq)$!). Autrement dit, $\mathrm{Le}_{\preccurlyeq}[I]$ est une section finale de $(\mathbb{N}^n, \leq)$.

Ainsi G est une base de Gröbner ùssi $\mathrm{Lm}_{\preccurlyeq}[G]$ engendre la section finale $\mathrm{Lm}_{\preccurlyeq}[I]$ de $\mathbb{M}_n$, autrement ùssiù $\mathrm{Le}_{\preccurlyeq}[I] = \uparrow_{\leq} \mathrm{Le}_{\preccurlyeq}[G]$ (pas $\uparrow_{\preccurlyeq} \mathrm{Le}_{\preccurlyeq}[G]$!).

Il résultera alors du Lemme de Dickson que I admet une base de Gröbner finie, puis, comme une base de Gröbner est génératrice, le théorème de la base de Hilbert en découlera.

Le lemme de Dickson exprime essentiellement que $(\mathbb{N}, \leq)$ est un belordre.

Modulo l'*Axiome des Choix Dépendants* (**DC**), les propriétés suivantes d'un ensemble ordonné $(P, \leq)$ sont équivalentes :

1. Bien fondé et sans antichaîne infinie.
2. Toute section finale est finiment engendrée.
3. L'ensemble des sections initiales est bien fondé pour l'inclusion.
4. Toute extension linéaire est un bon ordre.
5. Toute suite (infinie) admet une sous-suite (infinie) croissante.

Un tel $(P, \leq)$ est dit **belordonné** (**WPO** en anglais).

1. Les bons ordres sont les beaux ordres totaux.
2. Tout produit fini de beaux ordres est un belordre.
3. Toute extension (par des comparaisons) d'un belordre est un belordre.

En particulier $\mathbb{N}^n$ est belordonné par l'ordre produit (terme à terme) de celui de $\mathbb{N}$.

$\mathbb{N}^n$ est un **belordre** : ses sections finales sont finiment engendrées.

Incidemment :
$\mathrm{haut}(\mathbb{N}^n, \leq) = \omega$, $\mathrm{long}(\mathbb{N}^n, \leq) = \mathrm{haut}(\mathrm{SectInit}\ \mathbb{N}^n, \subseteq) - 1 = \omega^n$

$$\mathrm{long}(\mathrm{SectInit}\ \mathbb{N}^n, \subseteq) = \omega^{\frac{1}{\omega}(\omega+1)^{\otimes n}} + 1$$

Le monôme $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ s'identifie à l'uplet $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ de ses exposants.

Cette identification est un isomorphisme entre le monoïde commutatif $(\mathbb{M}_n, \cdot)$ des monômes en n indéterminées et $(\mathbb{N}^n, +) = (\mathbb{N}, +)^n$.

Les préordre de divisibilité d'un monoïde commutatif (non ambigu) est compatible avec l'opération : $(a|b) \wedge (a'|b') \Rightarrow aa'|bb'$, et l'élément neutre est minimum ; un préordre compatible admettant l'élément neutre comme minimum est plus fin que le préordre de divisibilité.

Le préordre de monoïde de $(\mathbb{N}, +)$ étant un bon ordre, et en particulier un belordre, celui de $(\mathbb{N}^n, +) = (\mathbb{N}, +)^n$ est un belordre.

Ses extensions linéaires sont les ordres compatibles totaux pour lesquels l'élément neutre est minimum. Ce sont des bons ordres. Réciproquement, pour qu'un ordre compatible soit bien fondé il faut que l'élément neutre soit minimal, minimum dans le cas linéaire.

Rappel : Étant donné un ordre monomial $\preccurlyeq$, une partie G d'un idéal I en est une base de Gröbner ùssiù $\mathrm{Lm}_{\preccurlyeq}[G]$ engendre la section finale $\mathrm{Lm}_{\preccurlyeq}[I]$ de $(\mathbb{M}_n, |)$, resp. $\mathrm{Le}_{\preccurlyeq}[G]$ engendre la section finale $\mathrm{Le}_{\preccurlyeq}[I]$ de $(\mathbb{N}_n, \leq)$.

Le fait que $(\mathbb{N}_n, \leq)$ soit un belordre correspond précisément au :

Lemme de Dickson : Toute section finale de $(\mathbb{N}_n, \leq)$ est finiment engendrée (par ses éléments minimaux).

En particulier, d'après le rappel ci-dessus, dans $k[X_1, \ldots, X_n]$:

Corollaire : Tout idéal I admet une base de Gröbner finie.
Il admet même des bases de Gröbner minimales : les G tels que $\mathrm{Lm}_{\preccurlyeq}[G]$ soit égal à l'ensemble des éléments minimaux de $\mathrm{Lm}_{\preccurlyeq}[I]$.

En particulier, comme les base de Gröbner sont génératrices :

Théorème de la base de Hilbert : Tout idéal est finiment engendré.

NB : Les bases de Gröbner minimales d'un idéal I sont équipotentes (avec l'ensemble des éléments minimaux de $\mathrm{Lm}_{\preccurlyeq}[I]$). L'idéal peut avoir des parties génératrices avec strictement moins d'éléments.

Du fait que tout idéal est finiment engendré découle que tout ensemble non vide d'idéaux a un élément maximal, et en particulier il n'existe pas de suite strictement croissante d'idéaux : noethérianité.

Une base de Gröbner est dite **minimale** si ses éléments sont unitaires et qu'elle est minimale pour l'inclusion.

Pour une base de Gröbner G de I constituée de polynômes unitaires, les propriétés suivantes sont équivalentes :

1. Minimalité comme base de Gröbner.
2. Minimalité comme partie génératrice.
3. Aucun monôme dominant d'un élément de G n'est divisible par celui d'un autre.
4. $g \in G \mapsto \mathrm{Lm}_{\preccurlyeq}(g)$ est une bijection dans l'ensemble des éléments minimaux de $\mathrm{Lm}_{\preccurlyeq}[I]$ (pour la divisibilité). ($G \subseteq I$ suffit.)

Une base de Gröbner G est dite **réduite** si ses éléments sont unitaires et qu'aucun monôme d'un élément de G n'est divisible par le monôme dominant d'un autre.

Il existe une unique base de Gröbner réduite. Elle est minimale.

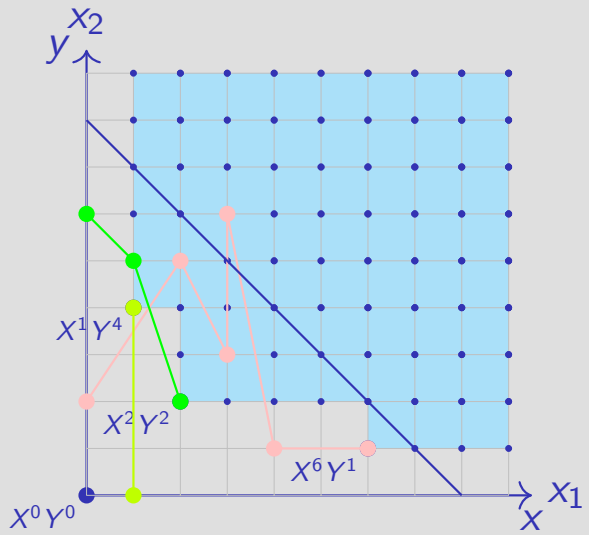


Figure – La section finale de $\mathbb{N}^2$ de l'idéal monomial $\langle XY^4, X^2Y^2, X^6Y\rangle$. Une base de Gröbner pour $\mathrm{Lex}_{x\succ y}$ minimale non réduite. Il n'est pas sûr que le système de trois ensemble de monômes en question corresponde bien à une base de Gröbner. Fournir de vrais exemples ! C'est le cas ssi l'escalier engendré est la partie bleue. Tout escalier est réalisable par un unique idéal monomial.

Incidemment noter que les parties finies, resp. chemins monotones, dans ce diagramme correspondent aux polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

Une base de Gröbner est dite **réduite** si ses éléments sont unitaires et qu'aucun monôme d'un élément de G n'est divisible par le monôme dominant d'un autre :
$\forall g \in G : g \not\xrightarrow[\mathrm{Lm}_{\preccurlyeq}\restriction G\setminus\{g\}]{}$.

Proposition : Étant donné un ordre monomial, chaque idéal de $k[X_1, \ldots, X_n]$ admet une et une seule base de Gröbner réduite. Elle est minimale.

Pour l'existence d'une base de Gröbner réduite, partir d'une base de Gröbner minimale G, en remplacer chaque élément g par $\mathrm{Lt}_{\preccurlyeq}(g) + \overline{\mathrm{Tail}_{\preccurlyeq}(g)}^{G,\preccurlyeq}$. On peut procéder à ces remplacements successivement (en actualisant G à chaque étape), ou simultanément. (Noter incidemment qu'il suffit en fait de réduire la somme des termes de g qui ne figurent pas strictement sous l'escalier.)

Pour l'unicité, si la différence entre deux éléments de même monôme dominant de deux bases réduites est non nul, en considérer un terme, qui doit d'une part être un terme de l'un des deux éléments en question, et d'autre part doit être divisible par le momôme dominant d'un autre élément de la base en question, en contredisant le caractère réduit.

Table of Contents

Le *S*-**polynôme** de f et g :

$$S_{\prec}(f,g) = \frac{\mathrm{Lm}_{\prec}(f) \vee \mathrm{Lm}_{\prec}(g)}{\mathrm{Lt}_{\prec}(f)} f - \frac{\mathrm{Lm}_{\prec}(f) \vee \mathrm{Lm}_{\prec}(g)}{\mathrm{Lt}_{\prec}(g)} g$$

$\mathrm{Lm}(f) \vee \mathrm{Lm}(g)$ est le plus petit monôme (pour l'ordre produit, et également pour chaque ordre monomial) auquel on peut appliquer $\xrightarrow{f}$ et $\xrightarrow{g}$. En outre $S(f,g) \in \langle f,g \rangle$, et $\mathrm{Lm}(S(f,g)) \prec \mathrm{Lm}(f) \vee \mathrm{Lm}(g)$, car les deux polynômes dont la différence définit $S(f,g)$ ont pour terme dominant $\mathrm{Lm}(f) \vee \mathrm{Lm}(g)$. (Par convention $\mathrm{Lm}(0) = -\infty$.)

Théorème : Un ensemble G de polynômes est une base de Gröbner ùssiù pour tous $g_1 \neq g_2$ dans G, $S_{\prec}(g_1,g_2) \xrightarrow[\mathrm{Lm}_{\prec} \restriction G]{*} 0$. resp.

$S_{\prec}(g_1,g_2) \xrightarrow[\mathrm{Lm}_{\prec} \restriction G]{*} o^G_{\prec}(\mathrm{Lm}_{\prec}(g_1) \vee \mathrm{Lm}_{\prec}(g_2))$, resp. la "paire critique" $\xleftarrow{g_1} \mathrm{Lm}_{\prec}(g_1) \vee \mathrm{Lm}_{\prec}(g_2) \xrightarrow{g_2}$ conflue (est joignable).

Théorème : Un ensemble G de polynômes est une base de Gröbner ùssiù pour tous $g_1 \neq g_2$ dans G, $S_{\preccurlyeq}(g_1, g_2) \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$.

Procédure : Partir d'un système générateur G de I. Pour chaque $g_1 \neq g_2$ dans G t.q. $S_{\preccurlyeq}(g_1, g_2) \not\xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$, enrichir G d'un r tel que $S_{\preccurlyeq}(g_1, g_2) \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} r$, *e.g.* $r = S_{\preccurlyeq}(g_1, g_2)$, ou, mieux, un irréductible, et recommencer avec le G ainsi enrichi, tant que possible. Noter que $r \in \langle G \rangle \setminus \langle \mathrm{Lm}_{\preccurlyeq}[G] \rangle$.

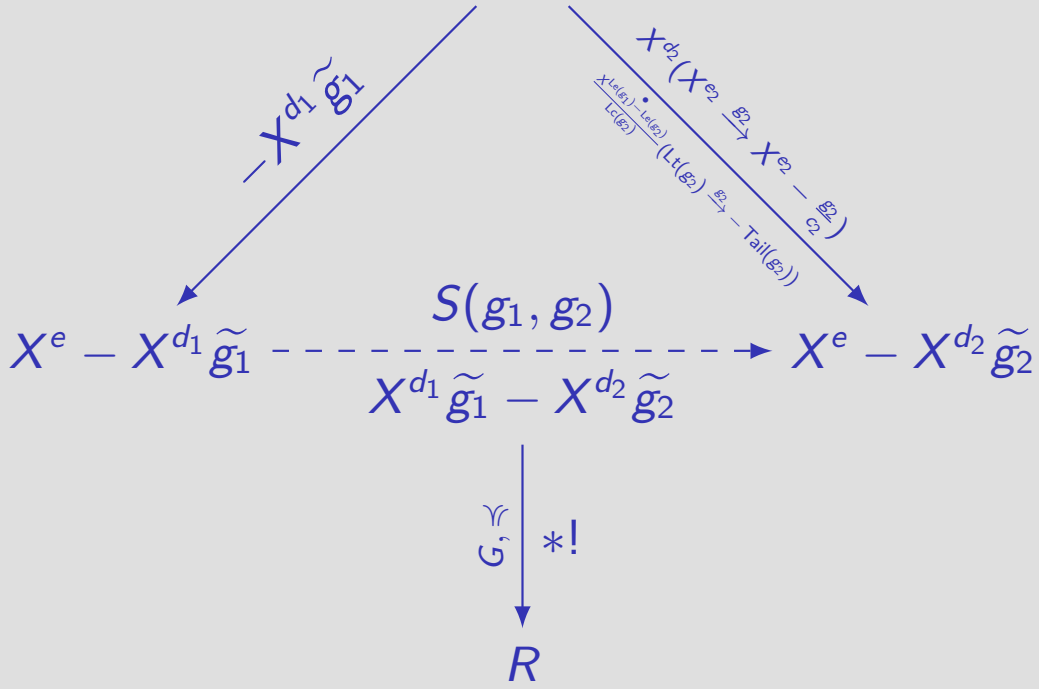
La procédure termine, par nothérianité, car $\langle \mathrm{Lm}_{\preccurlyeq}[G] \rangle$ croît strictement. (Plus basiquement, il suffit d'observer que la section finale de $\mathrm{Lm}_{\preccurlyeq}[G]$ de $\mathbb{N}^n$ croît strictement.) Le G final est une base de Gröbner de I, car on ne peut pas continuer précisément si on a affaire à une base de Gröbner, d'après le théorème.

Il restera donc à prouver ce théorème.

Algorithme de Buchberger

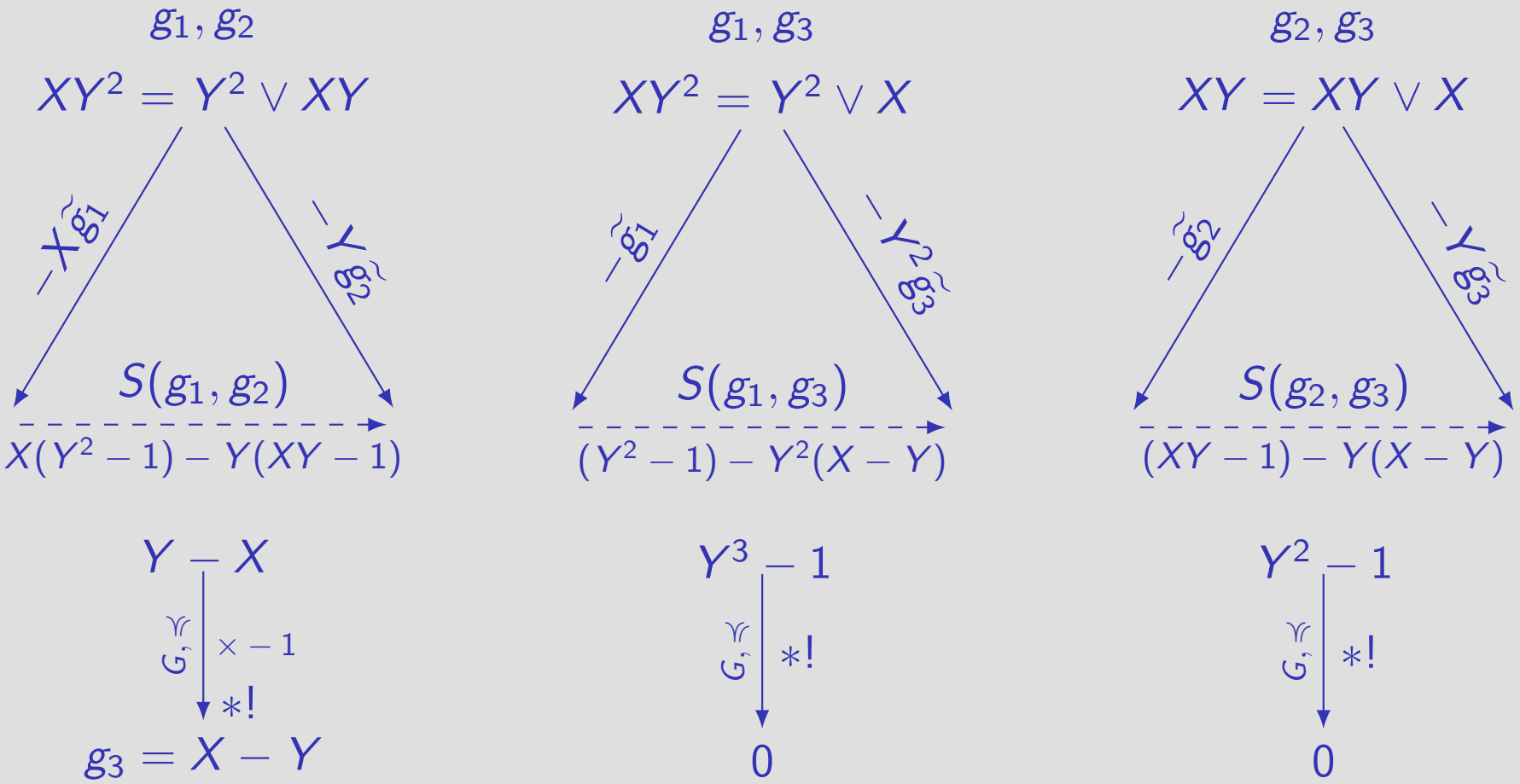
$\mathrm{Lm}_{\preccurlyeq}(g_i) = X^{e_i}$, $\mathrm{Lc}_{\preccurlyeq}(g_i) = c_i$, $\widetilde{g_i} = \frac{g_i}{c_i}$, $e := e_1 \vee e_2 = d_i + e_i$, $S(g_1, g_2) = X^{d_1}\widetilde{g_1} - X^{d_2}\widetilde{g_2}$.

$$X^e = \mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2) = X^{e_1} \vee X^{e_2} = X^{d_1}X^{e_1} = X^{d_2}X^{e_2}$$



$S(g_1, g_2)$ se réduit en R, dont on enrichit la base s'il est non nul.
Ainsi, dans la base éventuellement enrichie, $S(g_1, g_2)$ se réduit en 0.
Noter incidemment qu'on pourrait se contenter d'ajouter $S(g_1, g_2)$ à la base, sans le réduire, ou tout autre polynôme en "dérivant". Bien entendu, "il semble plus efficace" d'ajouter de "petits" éléments.

$$g_1 = Y^2 - 1,\ g_2 = XY - 1,\ \mathrm{Lex}_{X \succ Y}$$



$$G' = \{g_1, g_3\}$$

Voir

Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra by David A. Cox, John Little, Donal O'Shea

et

Calcul mathématique avec SAGE (2013). En particulier, la page 211.

NB : Une grossière erreur dans chacun des articles WkP en français et en anglais.

Théorème : Pour $G \subseteq k[X_1, \ldots, X_n]$, les conditions suivantes sont équivalentes :

1. G est une base de Gröbner, caractérisé par : $f \in \langle G \rangle \Rightarrow f = \mathcal{O}^G_{\preccurlyeq}(f)$.
2. $\forall g_1 \neq g_2 \in G,\ S_{\preccurlyeq}(g_1, g_2) \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} 0$.
3. $\forall g_1 \neq g_2 \in G,\ S_{\preccurlyeq}(g_1, g_2) \xrightarrow[\mathrm{Lm}_{\preccurlyeq} \restriction G]{*} o^G_{\preccurlyeq}(\mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2))$.
4. $\forall g_1 \neq g_2 \in G,\ \xleftarrow{g_1} \mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2) \xrightarrow{g_2}$ conflue (est joignable).

où $\mathcal{O}^G_{\preccurlyeq}(f)$, resp. $o^G_{\preccurlyeq}(f)$, désigne toute somme de produits hg t.q. $g \in G$ et $\mathrm{Lm}_{\preccurlyeq}(hg) \preccurlyeq \mathrm{Lm}_{\preccurlyeq}(f)$, resp. $\prec \mathrm{Lm}_{\preccurlyeq}(f)$. $\mathcal{O}^G_{\preccurlyeq}(f) \subseteq \langle G \rangle \cap \mathcal{O}_{\preccurlyeq}(f)$.

Comme $S_{\preccurlyeq}(g_1, g_2) \in \langle G \rangle$, $1 \Rightarrow 2$. Clairement $2 \Rightarrow 3$. On va prouver $3 \Rightarrow 1$ (suffisant pour justifier l'algorithme de Buchberger). Comme $1 \Rightarrow 4$, il restera à prouver $4 \Rightarrow 3$ pour boucler le théorème (cette implication justifiera la "variante" de l'algorithme, le rapprochant de l'algorithme de complétion de Knuth-Bendix).

Rappel : Un ensemble G de polynômes est une base de Gröbner ùssiù le terme dominant de chaque $f \in \langle G \rangle \backslash \{0\}$ est divisible par celui d'un élément de G, resp. pour chaque $f \in \langle G \rangle$, $f = \mathcal{O}^G_{\preccurlyeq}(f)$.

Justification de l'algorithme de Buchberger. Preuve de $3 \Rightarrow 1$

Soit $f \in \langle G \rangle \backslash \{0\}$. Par hypothèse, il admet une décomposition $f = \sum_i h_i g_i$. Isolant les $h_i g_i$ de plus haut monôme, soit X^γ :

$$f = \sum_i h_i g_i + o^G_{\prec}(X^\gamma),\ g_i \in G$$

Ainsi $f = \mathcal{O}^G_{\prec}(X^\gamma)$. Il s'agit de justifier que, si $\mathrm{Le}_{\prec}(f) \prec \gamma$, alors on peut baisser strictement γ. Supposons donc $\mathrm{Le}_{\prec}(f) \prec \gamma$. Soit $c_i \in k$ t.q. $\mathrm{Lt}_{\prec}(h_i g_i) = c_i X^\gamma$.

$$f = (\sum_i c_i) X^\gamma + o^G_{\prec}(X^\gamma) \qquad \mathrm{Le}_{\prec}(f) \prec \gamma \Rightarrow \sum_i c_i = 0$$

$$= \sum_i c_i X^{e_i} \widetilde{g_i} + o^G_{\prec}(X^\gamma) \qquad e_i = \mathrm{Le}_{\prec}(h_i),\ \widetilde{g_i} = \frac{g_i}{\mathrm{Lc}_{\prec}(g_i)}$$

$$= \sum_i c_i (X^{e_i} \widetilde{g_i} - X^{e_1} \widetilde{g_1}) + o^G_{\prec}(X^\gamma) \qquad \text{car } \sum_i c_i = 0$$

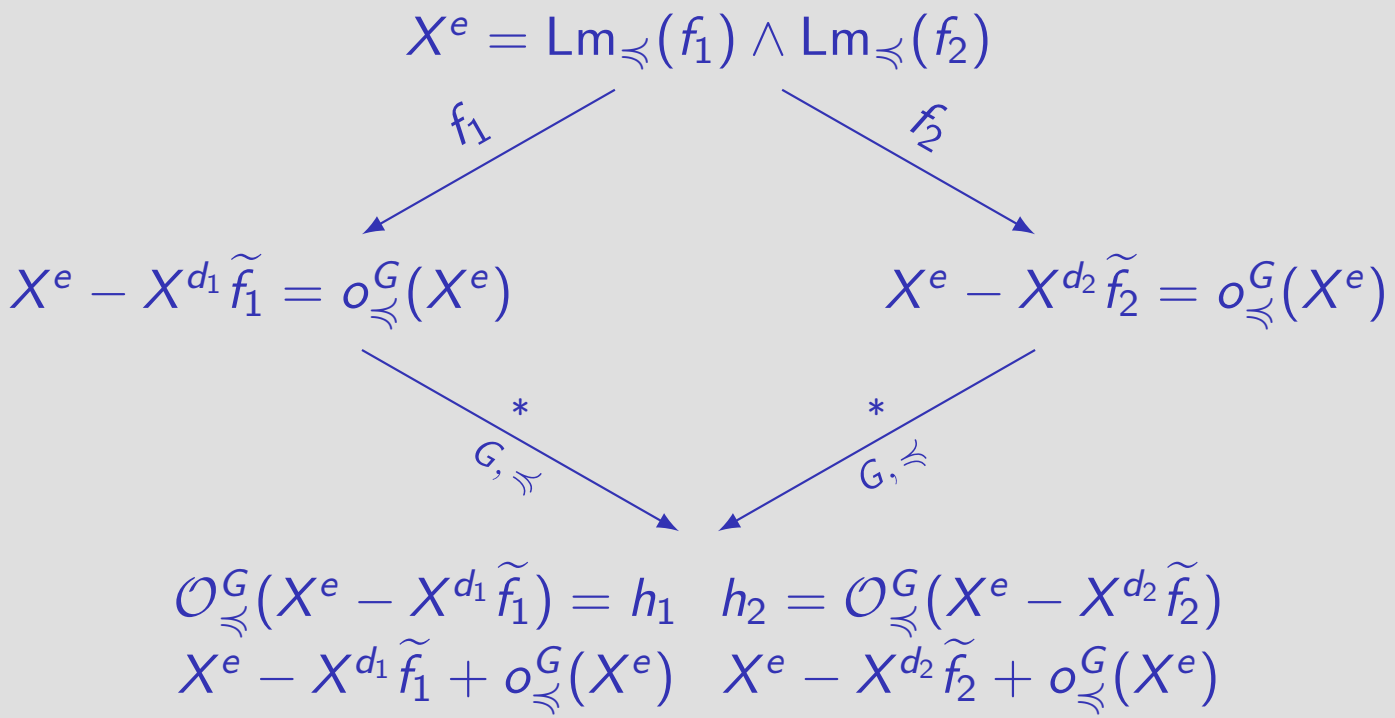
$$= \sum_i c_i (X^{e'_i} S(g_i, g_1)) + o^G_{\prec}(X^\gamma) \qquad \gamma = e'_i + (\mathrm{Le}_{\prec}(g_i) \vee \mathrm{Le}_{\prec}(g_1))$$

$$S(g_i, g_1) \xrightarrow[\mathrm{Lm}_{\prec} \restriction G]{*} o^G_{\prec}(\mathrm{Lm}_{\prec}(g_1) \vee \mathrm{Lm}_{\prec}(g_2)) \Rightarrow$$

$$X^{e'_i} S(g_i, g_1) = o^G_{\prec}(X^{e'_i}(\mathrm{Lm}_{\prec}(g_1) \vee \mathrm{Lm}_{\prec}(g_2))) = o^G_{\prec}(X^\gamma)$$

Paires critiques. Preuve de $4 \Rightarrow 3$

On considère deux polynômes non nuls f_1 et f_2 tels que $\xleftarrow[\prec]{f_1} \mathrm{Lm}_\prec(f_1) \vee \mathrm{Lm}_\prec(f_2) \xrightarrow[\prec]{f_2}$ conflue pour $\xrightarrow[\mathrm{Lm}_\prec \restriction G]{}$, et on justifie que $S_\prec(f_1, f_2) \in o^G_\prec(\mathrm{Lm}_\prec(f_1) \vee \mathrm{Lm}_\prec(f_2))$.
Observer que cela est vrai même si f_1 et f_2 ne sont pas dans G.
Ci-dessous $\widetilde{f} := \frac{f}{\mathrm{Lc}_\prec(f)}$.



$$S_\prec(f_1, f_2) = X^{d_1}\widetilde{f_1} - X^{d_2}\widetilde{f_2} = \underbrace{h_2 - h_1}_{0} + o^G_\prec(X^e) = o^G_\prec(X^e) = o^G_\prec(\mathrm{Lm}_\prec(f_1) \vee \mathrm{Lm}_\prec(f_2)).$$

1. $\mathrm{Lm}_{\prec}(g_1) \wedge \mathrm{Lm}_{\prec}(g_2) = 1 \Longrightarrow S(g_1, g_2) \xrightarrow{*} 0$.
2. Si $\mathrm{Lt}_{\prec}(g_0) \mid \mathrm{Lt}_{\prec}(g_1) \vee \mathrm{Lt}_{\prec}(g_2)$ et que les paire $\{g_0, g_1\}$ et $\{g_0, g_2\}$ ont été traitées, alors la paire $\{g_1, g_2\}$ n'a pas besoin de l'être. Plus précisément :

$$\begin{cases} S(g_0, g_1) = o^G_{\prec}(\mathrm{Lm}_{\prec}(g_0) \vee \mathrm{Lm}_{\prec}(g_1)) \\ S(g_0, g_2) = o^G_{\prec}(\mathrm{Lm}_{\prec}(g_0) \vee \mathrm{Lm}_{\prec}(g_2)) \\ \mathrm{Lt}_{\prec}(g_0) \mid \mathrm{Lt}_{\prec}(g_1) \vee \mathrm{Lt}_{\prec}(g_2) \end{cases}$$
$$\Longrightarrow S(g_1, g_2) = o^G_{\prec}(\mathrm{Lm}_{\prec}(g_1) \vee \mathrm{Lm}_{\prec}(g_2))$$

```
R.<x,y>=PolynomialRing(QQ,order='lex')

def Buchb(G) : # G liste ou uplet de polynomes
    k=len(G) ;
    P={(i,j) for j in range(k) for i in range(j)} ;
    while not P==set() :
        p=P.pop() ; i=p[0] ; j=p[1] ;
        gi=G[i] ; gj=G[j] ; mi=gi.lm() ; mj=gj.lm() ;
        ngi=gi/gi.lc() ; ngj=gj/gj.lc() ;
        m=R.monomial_lcm(mi,mj) ;
        di=R.monomial_quotient(m,mi) ; dj=R.monomial_quo
        s=di*ngi-dj*ngj ;
        r=division(s,G)[1] ;
        if not r==0*x :
            G=G+[r] ;
            P=P.union({(i,k) for i in range(k)}) ;
            k=k+1
    return G

Buchb([x*y,x+1,x^2+x*y-3,x^2*y])
```

```
1  R.<x,y>=PolynomialRing(QQ,order='lex')
2
3  def Minimise(G) : # G liste ou uplet base de Grobner
4      k=len(G) ; N=[0]*k
5      for i in range(k) :
6          mi=G[i].lm() ;
7          for j in range(i+1,k) :
8              mj=G[j].lm()
9              if R.monomial_divides(mi,mj) : N[j]=N[j]+1
10             elif R.monomial_divides(mj,mi) : N[i]=N[i]+1
11     return [G[i]/G[i].lc() for i in range(k) if N[i]==0]
12
13 G=[x*y+5,x^2+x*y,x^2*y,x^2,y^3+1,x*y^2+x,x^2*y+1,3*x*y]
14 Minimise(G)
15 > [x*y + 5, x^2 + x*y - 3, y^3 + 1]
```

$$N[j] > 0 \Leftrightarrow \begin{cases} \exists i < j : mi \leq mj \text{ ou} \\ \exists i > j : mi < mj \end{cases}$$

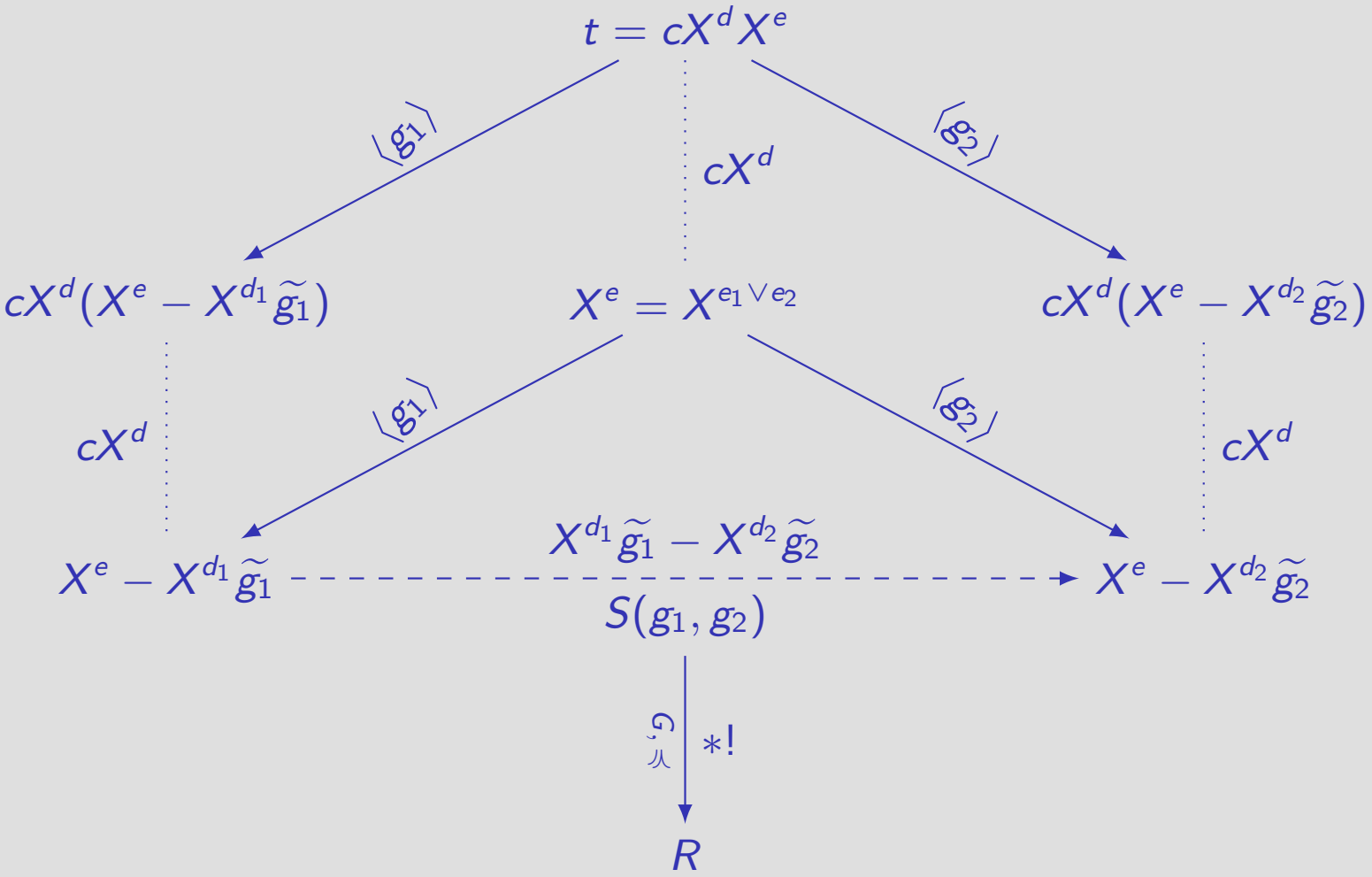
Ainsi élimine-t-on les termes qui sont L-strictement divisés ou qui sont équivalents à un terme antérieur.

```
1  R.<x,y>=PolynomialRing(QQ,order='lex')
2
3  def Reduction(G) : # G liste de Grobner minimale
4      k=len(G) ; L=range(len(G)) ; Red=[]
5      for i in L :
6          g=G[i] ; m=g.lm() ; tail=g-m
7          r=division(tail,[G[j] for j in L if not j==i])[1]
8          Red.append(m+r)
9      return Red
10
11 def GrobMinRed(G) : # G liste de polynomes
12     G0=G ; print('G0=',G0)
13     G1=Buchb(G0) ; print('G1=',G1)
14     G2=Minimise(G1) ; print('G2=',G2)
15     G3=Reduction(G2) ; print('G3=',G3)
```

Gröbnerisation-Minimisation-Réduction - Exemples

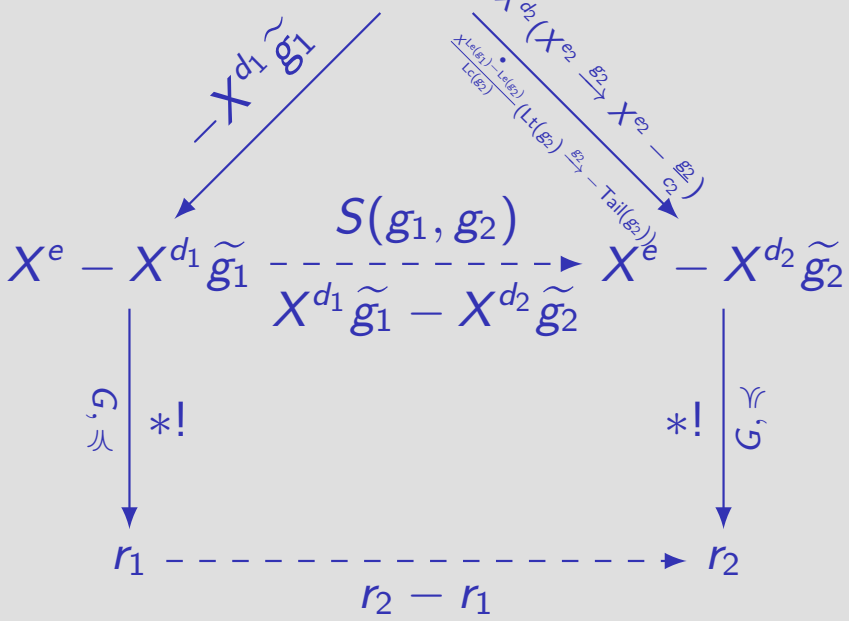
```
#Exemple de BookSage page 210
R.<x,y>=PolynomialRing(QQ,order='lex')
GrobMinRed([x-y,x-y^2])
> G0= [x - y, x - y^2]
> G1= [x - y, x - y^2, y^2 - y]
> G2= [x - y, y^2 - y]
> G3= [x - y, y^2 - y]

#Exemple de Cox-Little-OShea, page 88
R.<x,y>=PolynomialRing(QQ,order='deglex')
GrobMinRed([x^3-2*x*y,x^2*y-2*y^2+x])
> G0=[x^3-2*x*y, x^2*y-2*y^2+x]
> G1=[x^3-2*x*y, x^2*y-2*y^2+x, -x^2, -2*x*y, -2*y^2+x]
> G2=[-x^2, -2*x*y, -2*y^2+x]
> G3=[x^2, x*y, y^2-1/2*x]

#Exemple de Kreuzer-Robbiano page 100
R.<x,y,z>=PolynomialRing(QQ,order='deglex')
GrobMinRed([x^2-y^2-x,x*y^2-z^3])
> G0=[x^2-y^2-x,x*y^2-z^3]
> G1=[x^2-y^2-x,x*y^2-z^3,x*z^3-y^4-z^3,y^6-z^6+y^2*z^3]
> G2=[x^2-y^2-x,x*y^2-z^3,x*z^3-y^4-z^3,y^6-z^6+y^2*z^3]
> G3=[x^2-y^2-x,x*y^2-z^3,x*z^3-y^4-z^3,y^6-z^6+y^2*z^3]
```

$\mathrm{Lt}_{\preccurlyeq}(g_i) = c_i X^{e_i}$, $e = e_1 \vee e_2 = d_i + e_i$, $g_i = c_i \widetilde{g_i}$, $S(g_1, g_2) = X^{d_1}\widetilde{g_1} - X^{d_2}\widetilde{g_2}$.



$\mathrm{Lm}_{\preccurlyeq}(g_i) = X^{e_i}$, $\mathrm{Lc}_{\preccurlyeq}(g_i) = c_i$, $\widetilde{g_i} = \frac{g_i}{c_i}$, $e := e_1 \vee e_2 = d_i + e_i$, $S(g_1, g_2) = X^{d_1}\widetilde{g_1} - X^{d_2}\widetilde{g_2}$.

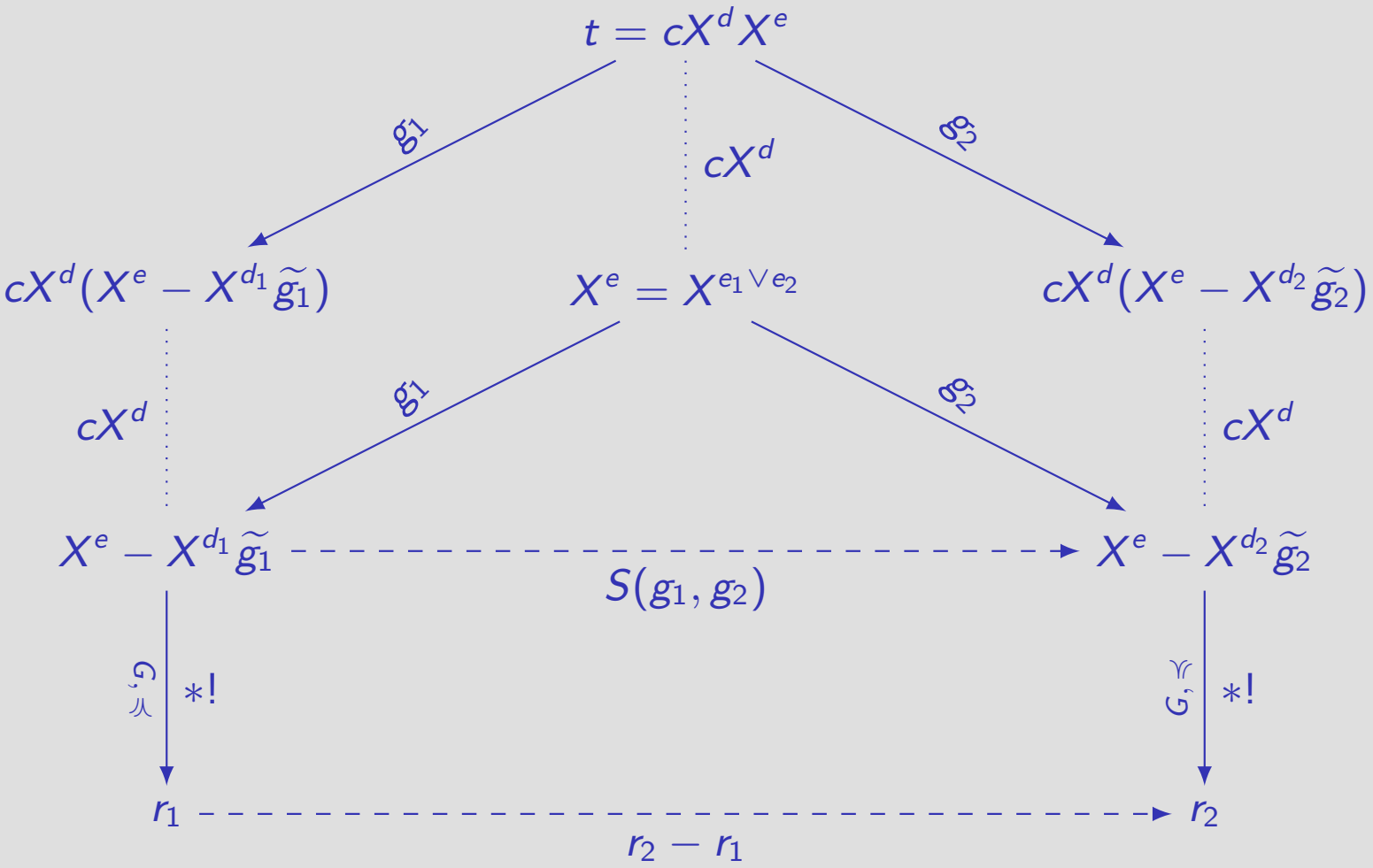
$$X^e = \mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2) = X^{e_1} \vee X^{e_2} = X^{d_1}X^{e_1} = X^{d_2}X^{e_2}$$



Au lieu d'enrichir par une forme réduite de la différence $S(g_1, g_2) = (X^e - X^{d_2}\widetilde{g_2}) - (X^e - X^{d_1}\widetilde{g_1})$, on enrichit par la différence $r_2 - r_1$ de deux formes réduites des termes de cette différence. Ainsi, dans la base enrichie, la paire $\xleftarrow{g_1} \mathrm{Lm}_{\preccurlyeq}(g_1) \vee \mathrm{Lm}_{\preccurlyeq}(g_2) \xrightarrow{g_2}$ est joignable.

Noter qu'on N'affirme PAS que $S(g_1, g_2) \xrightarrow[G, \preccurlyeq]{*} r_2 - r_1$. Préciser tout de même ce qu'il en est.

$\mathrm{Lt}_{\preccurlyeq}(g_i) = c_i X^{e_i}$, $e = e_1 \vee e_2 = d_i + e_i$, $g_i = c_i \widetilde{g_i}$, $S(g_1, g_2) = X^{d_1}\widetilde{g_1} - X^{d_2}\widetilde{g_2}$.



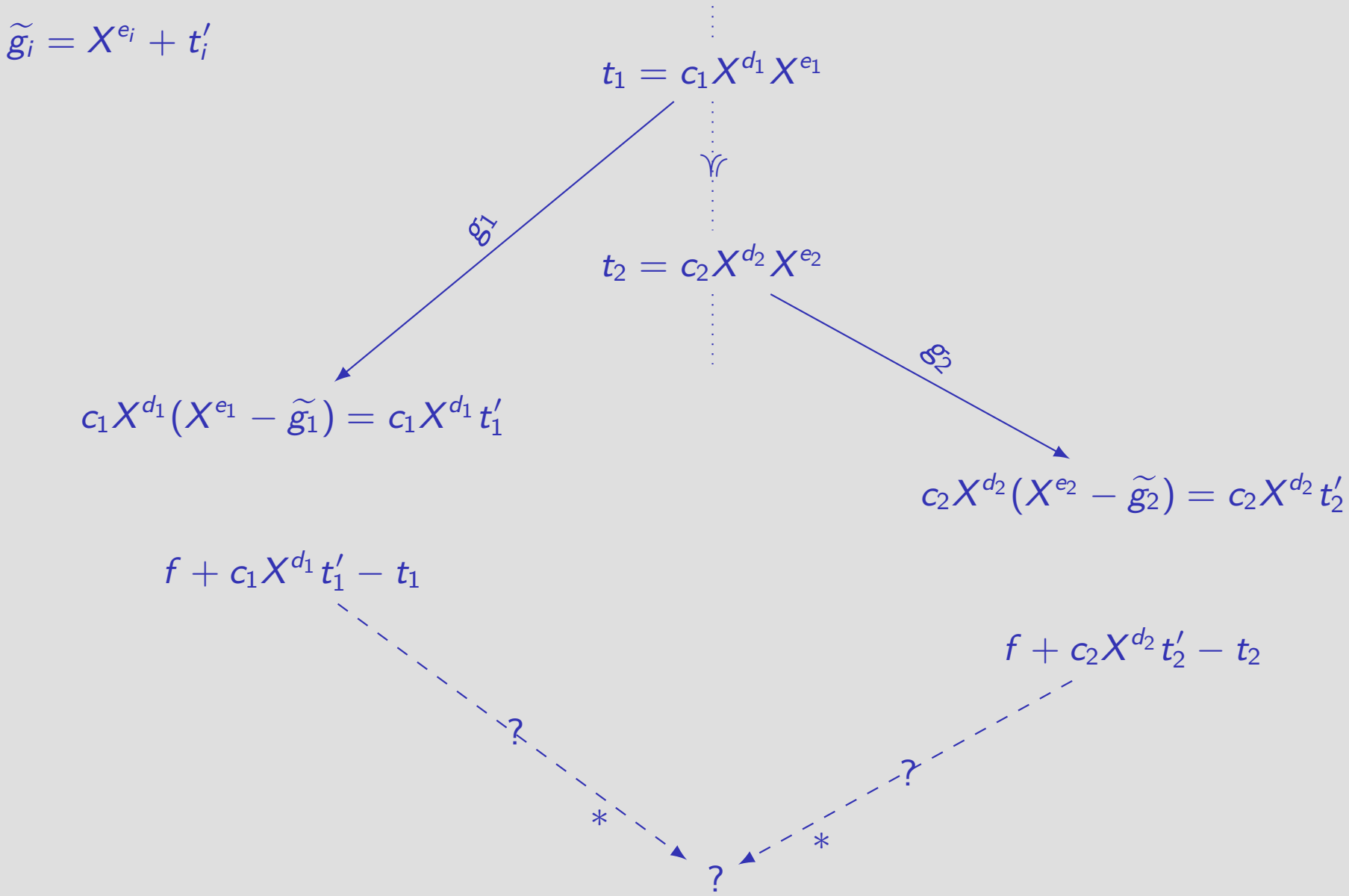
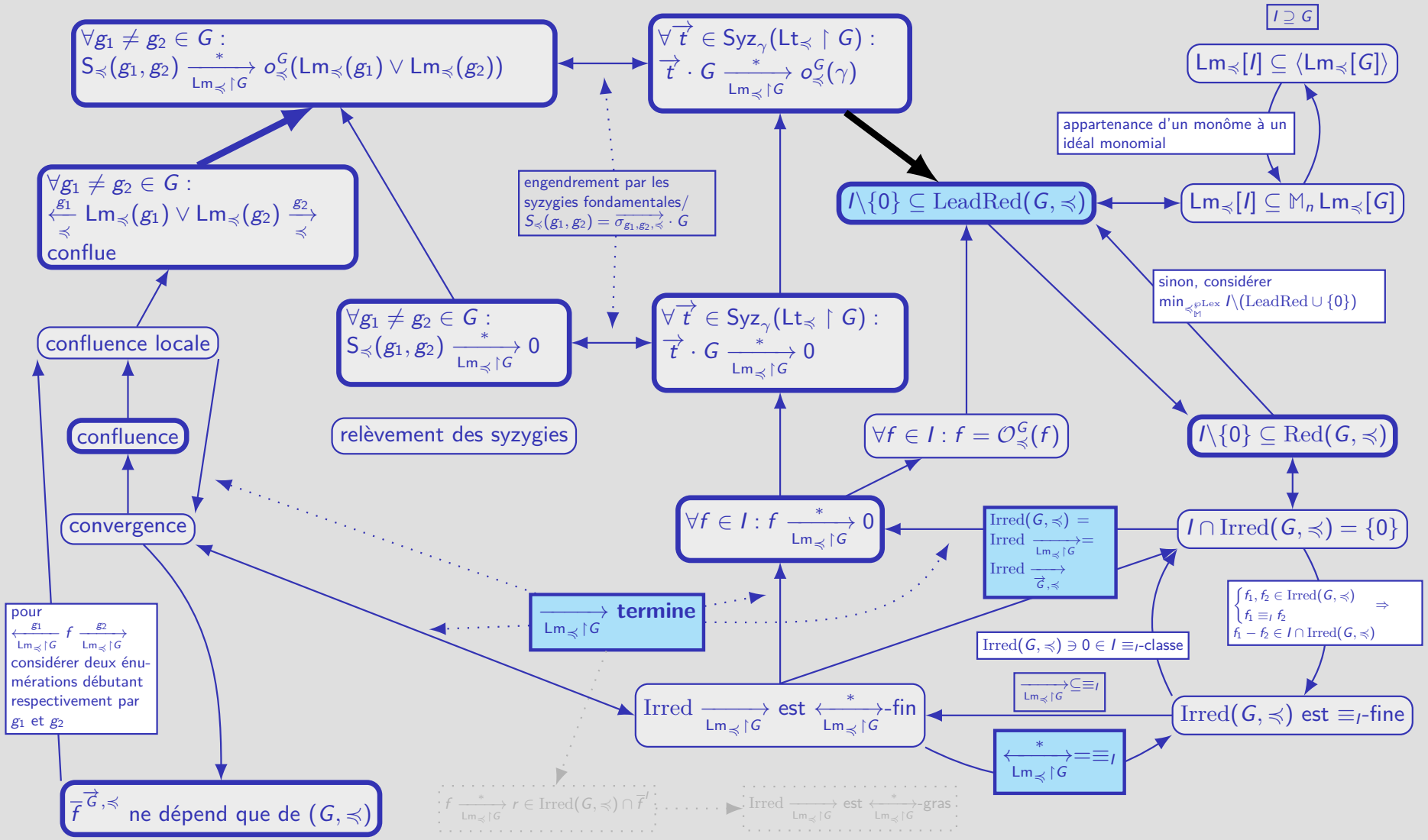

$\widetilde{g_i} = X^{e_i} + t'_i$
$t_1 = c_1 X^{d_1} X^{e_1}$
g_1
$t_2 = c_2 X^{d_2} X^{e_2}$
g_2
$c_1 X^{d_1}(X^{e_1} - \widetilde{g_1}) = c_1 X^{d_1} t'_1$
$c_2 X^{d_2}(X^{e_2} - \widetilde{g_2}) = c_2 X^{d_2} t'_2$
$f + c_1 X^{d_1} t'_1 - t_1$
$f + c_2 X^{d_2} t'_2 - t_2$
?
*
?
*
?

Table of Contents

Bases de Gröbner. Diagramme de synthèse



f est $(G,\preccurlyeq)$-réductible, resp. $(G,\preccurlyeq)$-lead- réductible, s'il admet un terme (non nul), resp. si son terme $\preccurlyeq$-dominant est divisible par le monôme $\preccurlyeq$-dominant d'un élément de G.

Table of Contents

Une base de Gröbner permet de déterminer un représentant de chaque classe modulo l'idéal.

Pour décider de l'appartenance d'un polynôme f à $\langle g_1, \ldots, g_d \rangle$, on en détermine une base de Gröbner pour un ordre monomial donné, puis on effectue la division multivariée par cette base.

Pour décider de l'inclusion entre deux idéaux ainsi spécifiés (ce qui permettra en particulier de décider de leur égalité), on vérifie l'appartenance des générateur de l'un à l'autre.

Pour l'égalité entre deux idéaux, on peut également en déterminer les bases de Gröbner réduites puis vérifier si elles sont égales.

Lemme : Si G est une base de Gröbner, alors $f \mapsto \overline{f}^{G,\preccurlyeq}$ est linéaire.

En effet, d'une part une combinaison linéaire de formes irréductibles est irréductible, autrement, l'ensemble des formes irréductible est un sous-espace vectoriel. D'autre part, cet ensemble de formes irréductibles est transverse à la $\langle G \rangle$-congruence précisément lorsque G est une base de Gröbner, tandis que la $\langle G \rangle$-congruence est bien compatible avec la structure linéaire.

Lemme :

La détermination de base de Gröbner en utilisant l'ordre lexicographique est souvent lente. L'ordre DegRevLex est souvent plus efficace.

Ce sont ceux dont l'anneau quotient est de dimension finie. Ce quotient admet pour base, dans tous les cas, les classes des monômes non divisible par la tête d'un élément non nul de l'idéal. En particulier le nombre de ces monômes est indépendant de l'ordre monomial.

La division mutivariée par un polynôme à une seule indéterminée, par une famille de polynômes à une seule indéterminées, par une famille de polynôme homogènes de degré 1.

Exemple

Théorie équationnelle (universelle) des groupes.

Table of Contents

Idéal monomial : Engendré par des monômes.

Un polynôme appartient à l'idéal engendré par des monomes m_i ùssiù chacun de ses termes est divisible par un m_i : chaque terme $c_{ij} m_i m_{ij}$ d'une somme de produits de m_i par des polynômes $p_i = \sum_{J_i} c_{ij} m_{ij}$ est divisible par un m_i. Après simplification, les monômes ne peuvent pas apparaître ; il ne peuvent que disparaître ou demeurer.
En particulier, un monôme m appartient à l'idéal monomial engendré par les m_i ùsss'il est divisible par un m_i.

Un idéal monomial est caractérisé par sa trace sur l'ensemble des monômes. Ces traces sont les sections finales de monômes pour la divisibilité, resp. les sections finales de $\mathbb{N}^n$ muni de son ordre produit.
Noter que tout ensemble de monômes est une base de Gröbner.

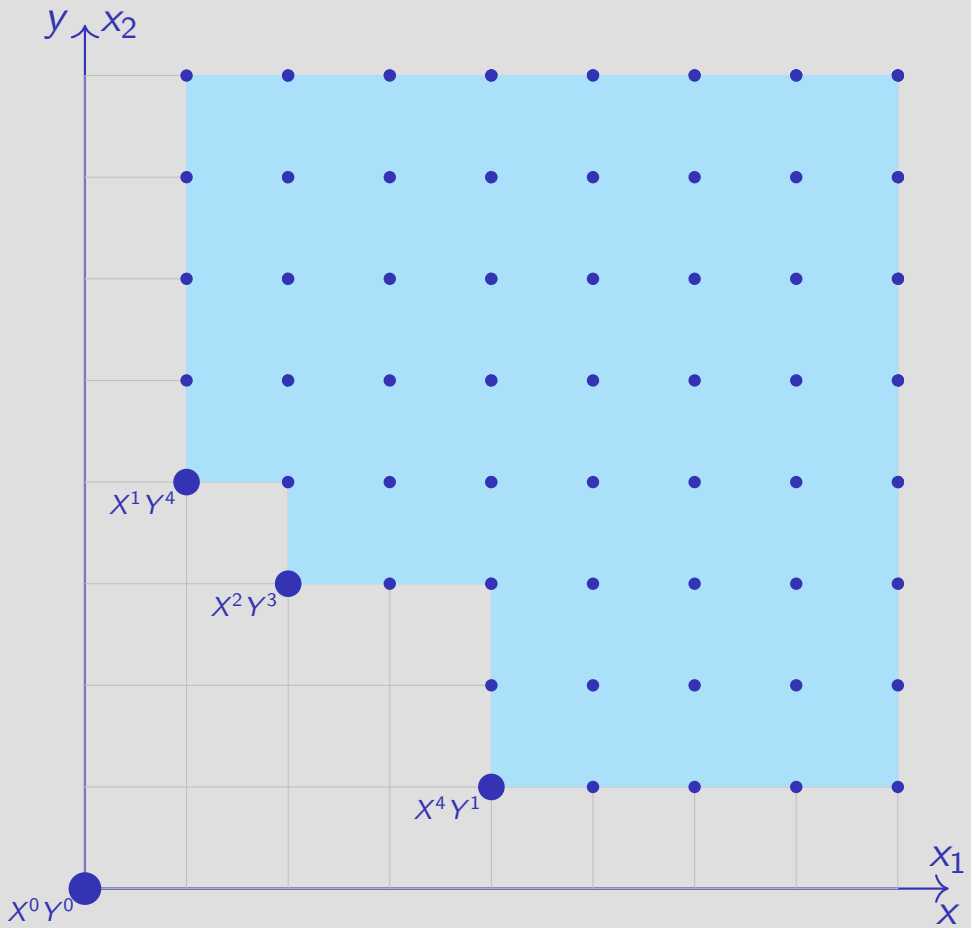


Figure – La section finale de $\mathbb{N}^2$, resp. de $\mathbb{M}_2$, associée à l'idéal monomial $\langle XY^4, X^2Y^2, X^6Y \rangle$

Idéal monomial : Engendré par des monômes.

Un idéal monomial est caractérisé par sa trace sur l'ensemble des monômes. Ces traces sont les sections finales de monômes pour la divisibilité, resp. les sections finales de $\mathbb{N}^n$ muni de son ordre produit.

$\mathbb{N}^n$ est un **belordre** : ses sections finales sont finiment engendrées.

Le théorème de la base de Hilbert

Tout idéal de $k[X_1, \ldots, X_n]$ est finiment engendré.

À un idéal I, on associe l'idéal monomial $\langle \mathrm{Lm}_{\preccurlyeq}[I] \rangle$ engendré par les monômes dominants de ses éléments. Tous les monômes qu'il contient sont monômes dominant d'un élément de I. Comme tout idéal monomial, il est engendré par un nombre fini de monômes. Ces monômes sont monômes dominants d'éléments de I qui engendrent I.

Plus généralement, si A est noethérien, alors $A[X]$ l'est également.

Les générateurs de I fournis par l'argument ci-dessus en constituent des bases de Gröbner.

$\langle \mathrm{Lm}_{\preccurlyeq}[I] \rangle$ admet un plus petit ensemble générateur de monômes, constitué par ses monômes minimaux pour l'ordre produit des n-uplets d'exposants. Les parties génératrices correspondantes de I en sont **les** bases de Gröbner *minimales*.

$\mathrm{Lm}_{\prec}[I]$ peut ne pas être un idéal, mais il est stable par multiplication par des monômes. Autrement dit, $\mathrm{Le}_{\prec}[I]$ est une section finale de $(\mathbb{N}^n, \leq)$, pas de $(\mathbb{N}^n, \prec)$!

Observation triviale : un partie G d'un idéal I en est une base de Gröbner (au sens où le monôme dominant de tout élément de I divise celui d'un élément de G), *i.e.* $\mathrm{Lm}_{\prec}[G]$ engendre la section finale pour la relation de divisibilité $\mathrm{Lm}_{\prec}[I]$ de $\mathbb{M}_n$, autrement ùssiù $\mathrm{Le}_{\prec}[I] = \uparrow_{\leq} \mathrm{Le}_{\prec}[G]$ (pas $\uparrow_{\prec} \mathrm{Le}_{\prec}[G]$!).

Il résulte du Lemme de Dickson qu'il existe une telle G finie. C'est le théorème de la base de Hilbert (compte tenu de l'observation ci-dessous).

Ce qui n'est pas trivial, bien que facile, c'est qu'une base de Gröbner à ce sens est génératrice : Considérer un éventuel contre-exemple dont l'ensemble des monômes serait minimum pour l'ordre lexicographique du bon ordre monomial considéré. On peut, alternativement, reconsidérer un reste de la division de $f \in I$ par une telle G. Un tel reste, devant appartenir à I mais ne pouvant être réduit est nul, tandis que la différence appartient à l'idéal engendré par G.

$\langle \mathrm{Lm}_{\prec}[I] \rangle$ admet un plus petit ensemble générateur de monômes, constitué par ses monômes minimaux pour l'ordre produit des n-uplets d'exposants. Les parties génératrices correspondantes de I en sont **les** bases de Gröbner *minimales*.

Une équation diophantienne est une équation polynomiale en plusieurs indéterminées à coefficients entiers.

Dixième problème de Hilbert, 1900 (reformulation) : Décrire une procédure permettant de décider si un équation diophantienne a une solution à coefficients entiers.

Noter que, comme un uplet de réels, et en particulier d'entiers, est nul si et seulement si la somme des carrés de ses composantes est nulle. Toute réponse pour les équations en fournit une réponse pour les systèmes.

Matiyasevich (1970) : Il n'existe en fait pas de telle procédure.

Plus précisément, les ensembles récursivement énumérables sont les projections des ensembles de solutions des systèmes diophantiens.

On ne sait pas si on peut décider si un tel système a des solutions rationnelles.

On sait en revanche décider si un système d'équations réelles a une solution réelle.

On ne peut pas décider si un système d'équations polynomiales à coefficients entiers a une solution entière.

On ne sait pas si on peut décider si un tel système a des solutions rationnelles.

On sait en revanche décider si un système d'équations réelles a une solution réelle (Tarski, élimination des quantificateurs de la théorie du premier ordre de $\mathbb{R}$, au demeurant celle des corps réels clos. Incidemment on ne sait pas si on peut étendre à l'exponentielle, mais on ne peut avec la fonction sinus).

Pour le cas de $\mathbb{C}$, et plus généralement d'un corps algébriquement clos, on dispose du théorème des Zéros de Hilbert, dont une variante nous dit qu'un système $\mathbb{K}$-polynomial en n variables a une solution dans la clôture algébrique $\overline{\mathbb{K}}^n$ dès que (donc ssi) l'idéal de $\mathbb{K}[X_1, \ldots, X_n]$ correspondant est non trivial, autrement dit ne contient pas 1, tandis que les bases de Gröbner permettent de décider si un polynôme appartient à un idéal.

Matiyasevich : On ne peut pas décider si un système d'équations polynomiales à coefficients entiers a une solution entière.

Le résultat d'indécidabilité de Matiyasevich s'étend aux anneaux des entiers des corps de nombres (extension finie de $\mathbb{Q}$) dont le groupe de Galois est abélien.

Matiyasevich : Les ensembles récursivement énumérables sont les projections des ensembles de solutions des systèmes diophantiens.

Il existe un polynôme $p(n, x_0, x_1, \ldots, x_n)$ tel que les ensembles
$E_n = \{x_0 : \exists x_1 \cdots x_n = p(n, x_0, x_1, \ldots, x_n) = 0\}$.
p de degré 4 (produit de somme de carrés).
$n = 13$ suffit, 9 est insuffisant.

On considère une graduation d'un anneau R par un monoïde commutatif Γ préordonné.

$$R = \bigoplus_{\gamma \in \Gamma} R_\gamma$$

Ne supposant pas l'ordre sur Γ total, on considérera une division sur R par une partie G de R dont chaque élément non nul ait un terme dominant, ùcadù une composante de plus grand indice.

1. L'anneau est intègre et le monoïde est régulier (au sens simplifiable).
2. $\gamma_1 \preccurlyeq \gamma_2 \Longrightarrow \gamma + \gamma_1 \preccurlyeq \gamma + \gamma_2$.
3. $R_{\gamma_1} R_{\gamma_2} \subseteq R_{\gamma_1 + \gamma_2}$

Il faudra se décider entre noter additivement et multiplicativement l'opération de Γ.

$$R = \bigoplus_{\gamma \in \Gamma} R_\gamma$$

Les éléments non nuls de R_γ sont les γ-termes, ou termes d'indice γ. Soit $f \in R$. Sa composante, éventuellement nulle, d'indice γ est notée f_γ. Ainsi $f = \sum_{\gamma \in \Gamma} f_\gamma$, seul un nombre fini de termes étant non nuls. Le support de f est l'ensemble, fini, $\mathrm{Supp}_\Gamma(f) \Subset \Gamma$ des indices de ses termes (non nuls). L'ensemble des éléments maximaux de ce support est noté $\mathrm{MaxSupp}_\Gamma(f)$. Noter que $\mathrm{Supp}_\Gamma(f)$, resp. $\mathrm{MaxSupp}_\Gamma(f)$, est vide ùssiù f est nul. f est γ-homogène s'il appartient à un R_γ. Un terme de f est prédominant si son indice est maximal. Ainsi, on demandera aux éléments de G d'avoir un et un seul terme prédominant, alors qualifié de dominant. La somme des termes prédominants de f est noté $\mathrm{Lt}_\Gamma(f) = \sum_{\gamma \in \mathrm{MaxSupp}(f)} f_\gamma$. De l'intégrité de R et de la croissance des translations de Γ résulte que si f et g ont une composante de plus grand indice, alors fg également, et $\mathrm{Lt}\,\Gamma(fg) = \mathrm{Lt}\,\Gamma(f) + \mathrm{Lt}\,\Gamma(g)$. Toutefois, si cela n'est pas le cas, $L_\Gamma(fg)$ peut ne pas être inclus dans $L_\Gamma(f) + L_\Gamma(g)$.

On pourra également en fait vouloir considérer des R-modules Γ-gradués.

Il peut être également question de monoïdes agissant sur des anneaux.

Soit G une partie de R dont chaque élément g a un terme dominant $\mathrm{Lt}_\Gamma(g)$, ùcadù une composante de plus grand indice.
Un G-uplet $\overrightarrow{h} = (h_g : g \in G) \in R^{(G)}$ est homogène si toutes ses valeurs sont Γ-homogènes ; il est alors de (G,Γ)-degré γ, si $h_g \neq 0 \Rightarrow h_g \,\mathrm{Lt}_\Gamma(g) \in R_\gamma$. NB : $\overrightarrow{h}$ peut être homogène sans avoir de (G,Γ)-degré.
On considère la division sur $R = \bigoplus_{\gamma\in\Gamma} R_\gamma$ par G :

$$f \xrightarrow[G,\Gamma]{\gamma} f - \overrightarrow{h} \cdot G$$

où $\overrightarrow{h}$ est (G,Γ)-γ-homogène et $\overrightarrow{h} \cdot G := \sum_g h_g \,\mathrm{Lt}_\Gamma(g) = f_\gamma \neq 0$.

Conditions sur la graduation Γ, garantissant notamment la terminaison :

1. Bonne fondation du préordre de Γ, alors supposé être un ordre.

Décroissance dans l'ensemble des parties de Γ, lexicographiquement préordonnées par les multiensembles des hauteurs des termes.

Définition : G est une $(\Gamma, \preccurlyeq)$-base de Gröbner si tout élément non nul de $\langle G \rangle$ a un terme prédominant divisible par le terme dominant d'un élément de G.

Noter que "le" quotient correspondant doit être Γ-homogène.

CNS :

$$\forall f \in R : f \in \langle G \rangle \Longrightarrow \begin{cases} f \xrightarrow[G,\Gamma]{*} 0, \text{ resp.} \\ f = \mathcal{O}_\Gamma^G(\mathrm{Supp}(f)), \text{ resp.} \\ f \xrightarrow[G,\Gamma]{*} \mathcal{O}_\Gamma^G(\mathrm{Supp}(f)) \end{cases}$$

où, pour $F \subseteq \Gamma$, $\mathcal{O}_\Gamma^G(F)$ désigne la classe des sommes de produits d'un terme t et d'un élément g de G tels que $tg \in R_{\downarrow_\preccurlyeq F}$.

Définition : Une syzygie de G est un G-uplet $\overrightarrow{h} \in R^{(G)}$ t.q. $\overrightarrow{h} \cdot G = 0_R$, autrement dit un élément du noyau de $\overrightarrow{h} \in R^{(G)} \mapsto \overrightarrow{h} \cdot G \in R$.
Proposition : G est une Γ-base ùssiù pour toute syzygie homogène $\overrightarrow{t}$ de $\mathrm{Lt}_\Gamma \restriction G$, de (G,Γ)-degré γ :

$$\begin{cases} \overrightarrow{t} \cdot G \xrightarrow[G,\Gamma]{*} 0, \text{ resp. } \overrightarrow{t} \cdot G = o_\Gamma^G(\gamma), \text{ resp. } \overrightarrow{t} \cdot G \xrightarrow[G,\Gamma]{*} o_\Gamma^G(\gamma), \text{ resp.} \\ \exists \overrightarrow{h} \in \mathrm{Syz}(G) : (\overrightarrow{h} - \overrightarrow{t})G \in R^{(G)}_{\prec\gamma} \end{cases}$$

($\Leftarrow$) : Pour $f \in \langle G \rangle$, considérer une décomposition $f = \sum_i t_i g_i$ où les t_i sont des termes (ainsi, les g_i peuvent se répéter). Regroupant ces $t_i g_i$ en fonction de l'indice de $\mathrm{Lt}_\Gamma(t_i g_i)$, cette somme se réécrit, compte tenu de l'hypothèse de régularité : $f = \sum_{\gamma \in F} \overrightarrow{t}_\gamma \cdot G$ **(*)**. Observer que si μ est maximal dans $F \setminus \mathrm{Supp}(f)$, alors $\overrightarrow{t}_\mu$ est une syzygie homogène de $\mathrm{Lt}_\Gamma \restriction G$, de (G,Γ)-degré μ. Ainsi $\overrightarrow{t}_\mu \cdot G = o_\Gamma^G(\mu)$, de sorte que $f = \mathcal{O}_\Gamma^G(F')$, ou $f = \sum_{\gamma \in F'} \overrightarrow{t}'_\gamma \cdot G$, avec $F' := F \setminus \{\mu\} \cup \downarrow_\prec \mu \prec F$. Ainsi, une F $\preccurlyeq$-minimale pour laquelle on dispose d'une décomposition (*) doit être incluse dans le support de f, et donc $f = \mathcal{O}_\Gamma^G(\mathrm{Supp}(f))$.

Proposition : G est une Γ-base ùssiù pour toute syzygie homogène $\overrightarrow{t}$ de $\mathrm{Lt}_\Gamma \restriction G$, de (G,Γ)-degré γ :

$$\begin{cases} \overrightarrow{t}\cdot G \xrightarrow[G,\Gamma]{*} 0, \text{ resp. } \overrightarrow{t}\cdot G = o_\Gamma^G(\gamma), \text{ resp. } \overrightarrow{t}\cdot G \xrightarrow[G,\Gamma]{*} o_\Gamma^G(\gamma), \text{ resp.} \\ \exists\, \overrightarrow{h} \in \mathrm{Syz}(G) : (\overrightarrow{h} - \overrightarrow{t})G \in R^{(G)}_{\prec\gamma} \end{cases}$$

Observation 1 : Tout élément de $\langle G\rangle$ admet une décomposition :

$$f = \sum_{\gamma\in F} \overrightarrow{t}_\gamma \cdot G \tag{1}$$

où chaque $\overrightarrow{t}_\gamma$ est un G-uplet de R t.q. pour chaque $g\in G$, $(\overrightarrow{t}_\gamma)_g \,\mathrm{Lt}_\Gamma(g) \in R_\gamma$. De plus $f = \mathcal{O}_\Gamma^G(\mathrm{Supp}(f))$ ùsss'il existe une telle décomposition pour laquelle $F \subseteq \mathrm{Supp}(f)$.

Observation 2 : Si, dans (1), μ est un élément $\preccurlyeq$-maximal de $F\setminus \mathrm{Supp}(f)$, alors $\overrightarrow{t}_\mu$ est une syzygie homogène de $\mathrm{Lt}_\Gamma \restriction G$, de (G,Γ)-degré μ.

Ainsi, pour justifier l'implication non triviale ($\Leftarrow$), il suffit d'observer que, TERMINER !

La (G,Γ)-homogénéisation $\overrightarrow{f} \in R^{(G)} \mapsto (\mathrm{Lt}_\Gamma / G)(\overrightarrow{f}) \in R^{(G)}$ et relèvement des syzygies

C'est une fonction partielle, définie en les uplets homogènes qui admettent un (G,Γ)-degré ! !

FAIRE ! Ci-dessous, brouillon.

$(\overrightarrow{h} - \overrightarrow{t})G \in R^{(G)}_{\prec\gamma}$

La syzygie $\overrightarrow{h}$ de G relève la syzygie $\overrightarrow{t}$ de $\mathrm{Lt} \restriction G$, pour $\overrightarrow{h} \mapsto (\mathrm{Lt}_\Gamma / G)(\overrightarrow{h})$ homogène, associant à $g \in G$, $\mathrm{Lt}_\Gamma(h_g)$ ou 0, suivant que le terme $\mathrm{Lt}_\Gamma(h_g)\,\mathrm{Lt}_\Gamma(g)$ est d'indice maximum ou pas, où chaque composante non nulle de $\overrightarrow{h}$ a un terme d'indice maximum.

Préciser ! Et péciser le lien avec les autres critères de la proposition, et d'ailleurs entre tous ces critères.

Justifier également l'implication "facile" de la proposition.

$R = k[X, Y, Z]$. $\Gamma = \mathbb{M}_{\mathrm{GradLex}_{X \succ Y \succ Z}}$.
Soit :

$$\overrightarrow{G} = (g_1, g_2) = (X^2 - Y - 2 - X, XY^2 - Z^2)$$

Soit $\overrightarrow{f} = (Y^2Z - X, -4X^2 - Y - 3) \in R^{(G)}$. Il est de G-degré X^3Y^2, le $\preccurlyeq$-maximum des indices dominants des $f_g g$, et

$$(\mathrm{Lt}_\Gamma / G)(Y^2Z - X, -4X^2 - Y - 3) = (0, -4X^2)$$

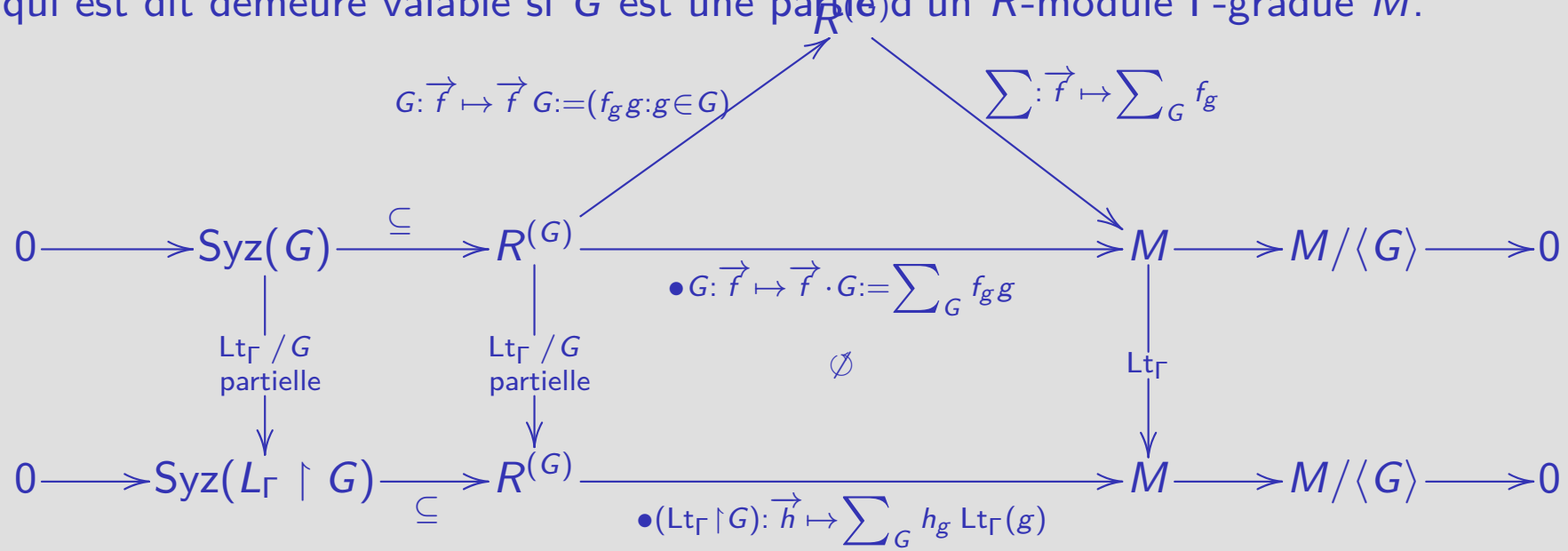
est le G-uplet des termes correspondant à ce maximum.

Soit $(\frac{1}{2}Y^2Z, -4XZ) \in R^{(G)}$. Il est de G-degré X^2Y^2Z, et

$$(\mathrm{Lt}_\Gamma / G)(\frac{1}{2}Y^2Z, -4XZ) = (\frac{1}{2}Y^2Z, -4XZ)$$

Le diagramme, en général NON commutatif

Rappeler qu'un idéal de R n'est autre qu'un sous R-module de R, et observer que tout ce qui est dit demeure valable si G est une partie d'un R-module Γ-gradué M.



Le domaine de $\mathrm{Lt}_\Gamma\,/G$ (qui est totale si l'ordre de Γ est total), est formé des G-uplets $\overrightarrow{f}$ nul ou pour lesquels il y a un terme $\mathrm{Lt}_\Gamma(f_g g)$ de plus grand indice

Préciser dans quels cas le diagramme est commutatif.

Précier pour quels types de morphismes c'est un diagramme (ùcfù Kreuz-Rob, p. 101).

On a besoin, ci-dessous, de supposer que Γ est un treillis pour son préordre de monoïde dont $\preccurlyeq$ est une extension telle que ... Attention à bien considérer les ordres convenables !

Lemme : Les syzygies de G sont les G-uplets de la forme

$$\sum_{f,g\in G} t_{f,g}\overrightarrow{\sigma_{f,g}}$$

où les $t_{f,g}$ sont des éléments homogènes de R et $\overrightarrow{\sigma_{f,g}}$ est la syzygie, élémentaire (ou fondamentale) :

$$\overrightarrow{\sigma_{f,g}} : \begin{cases} f \mapsto \sigma_{f,g} := \frac{\mathrm{Lm}(f)\vee\mathrm{Lm}(g)}{\mathrm{Lt}(g)} \\ g \mapsto -\sigma_{g,f} \\ h \in G\backslash\{f,g\} \mapsto 0 \end{cases}$$

de sorte que :

$$\sigma_{f,g}\mathrm{Lt}(g) = \mathrm{Lm}(f)\vee\mathrm{Lm}(g) \text{ et } S_{\preccurlyeq}(f,g) = \overrightarrow{\sigma_{f,g}}\cdot G$$

Corollaire 1 : Justification de l'algorithme de Buchberger.

Si l'ordre du monoïde Γ n'est pas total, il n'est pas garanti que $S(g_1, g_2)$, ou certains de ses dérivés, ait un terme de plus haut indice.

Reprendre les énoncés dans le cadre "restreint" qui nous intéresse.

Corollaire 2 : Le module des syzygies d'une famille finie est finiment engendré.

On peut ainsi, compte tenu du choix d'un système de générateurs, envisager d'en considérer le module des syzygies, et ainsi de suite.

On parle en fait du module des syzygies d'un module de type fini. Il dépend du choix d'un sytème de générateur fini, mais deux tels modules ont un complément libre dans un même module (ùcfù la régularité). On peut alors itérer. Le théorème des syzygies de Hilbert dit alors que pour $R = k[X_1, \ldots, X_n]$, le n-ième module de syzygies est nul, autrement dit avant la n-ième itération, l'un est libre.Il permet en particulier de montrer que certains espaces d'invariants sont de dimension finie (ou finiment engendré ?).

Noter que, comme les polynômes sont à support fini, on se contente d'hypothèses de bonne fondation, du moins dans un premier temps. On fera des hypothèses de belordre pour des séries ...