CHAPITRE
III

Algorithmes de division

Sommaire

§ 1 Préliminaires : systèmes d'équations linéaires

III.1.1. Systèmes d'équations linéaires.— L'algorithme d'élimination de Gauss-Jordan permet de déterminer les solutions d'un système d'équations linéaires, *i.e.*, des systèmes d'équations de la forme

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

où tous les polynômes $f_1,\dots,f_s$ de $\mathbb{K}[x_1,\dots,x_n]$ sont linéaires en les indéterminées $x_1,\dots,x_n$.

III.1.2. Exemple.— Considérons les polynômes linéaires suivants

$$f_1 = x+y-z, \quad f_2 = 2x+3y+2z$$

de $\mathbb{R}[x,y,z]$. Soit $I=\langle f_1,f_2\rangle$ l'idéal engendré par ces deux polynômes et soit $\mathbf{V}(f_1,f_2)$ l'ensemble algébrique affine formé des solutions du système linéaire suivant

$$\begin{cases} x+y-z=0 \\ 2x+3y+2z=0 \end{cases}$$

La méthode d'élimination de Gauss-Jordan pour la résolution de ce système consiste à choisir un pivot, par exemple l'indéterminée x dans la première équation et à éliminer les termes contenant cette indéterminée dans les autres équations. Le système se réduit ainsi au système suivant

$$\begin{cases} \boxed{x}+y-z=0 \\ y+4z=0 \end{cases}$$

Les solutions du système satisfont ainsi

$$y=-4z, \quad x=5z.$$

Cette méthode d'élimination par ligne consiste à changer l'ensemble générateur de l'idéal $I=\langle f_1,f_2\rangle$ par un autre ensemble générateur. On soustrait deux fois la première ligne à la seconde et on remplace la seconde ligne par cette nouvelle ligne. On construit ainsi un nouveau polynôme

$$f_3 = f_2 - 2f_1 = y+4z,$$

qui remplace le polynôme f_2 dans le système. Comme $f_3=f_2-2f_1$, on a $f_3\in I$ et comme $f_2=2f_1+f_3$, on a $f_2\in\langle f_1,f_3\rangle$, ainsi

$$I=\langle f_1,f_2\rangle=\langle f_1,f_3\rangle\,.$$

On modifie ainsi l'ensemble des générateurs de I permettant de déterminer plus facilement l'ensemble algébrique affine :

$$\mathbf{V}(f_1,f_2)=\mathbf{V}(f_1,f_3)=\{(5z,-4z,z)\ \mid\ z\in\mathbb{R}\}.$$

Le processus par lequel le polynôme f_2 est remplacé par f_3 en utilisant f_1 est appelé une *réduction* de f_2 par f_1, on note

$$f_2 \xrightarrow{f_1} f_3.$$

Le nouveau polynôme f_3 apparaît comme un reste de la division du polynôme $2x+3y+2z$ par $x+y-z$:

$$\begin{array}{rrr|l} 2x & +3y & +2z & x\ +y\ -z \\ \cline{4-4} 2x & +2y & -2z & 2 \\ \cline{1-3} & y & +4z & \end{array}$$

III.1.3. Question de l'appartenance à un idéal.— Étant donné un polynôme f de $\mathbb{R}[x,y,z]$, a-t-on $f\in I=\langle f_1,f_3\rangle$? Si f est dans I, il peut s'écrire comme combinaison des polynômes générateurs de I :

$$f=h_1f_1+h_3f_3,$$

avec $h_1,h_3\in\mathbb{R}[x,y,z]$. Si le « *terme dominant* » (le pivot !) de f_1 est x et le « *terme dominant* » de f_3 est y, tout polynôme de $\mathbb{R}[x,y,z]$ se réduit via f_1 et f_3 en un polynôme d'indéterminée z. De plus, un polynôme en z ne peut pas être réduit par réduction via f_1 et f_3. On a

$$f\in I=\langle f_1,f_2\rangle=\langle f_1,f_3\rangle \quad \text{si, et seulement si,} \quad f\xrightarrow{f_1,f_3}0.$$

III.1.4. Exemple.— Considérons maintenant la situation de 3 polynômes linéaires

$$f_1 = y - z, \quad f_2 = x + 2y + 3z, \quad f_3 = 3x - 4y + 2z$$

de $\mathbb{R}[x,y,z]$. On considère l'idéal engendré par ces trois polynômes, $I = \langle f_1, f_2, f_3 \rangle$ et l'ensemble algébrique affine $\mathbf{V}(f_1, f_2, f_3)$ formée des solutions du système suivant

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ 3x - 4y + 2z = 0 \end{cases}$$

Par élimination, on peut réduire ce système au suivant

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ -10y - 7z = 0 \end{cases}$$

en retranchant 3 fois la seconde ligne à la troisième, puis au système

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ -17z = 0 \end{cases}$$

en retranchant -10 fois la première ligne à la troisième On a les réduction

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z.$$

On a un nouvel ensemble générateur pour I :

$$I = \langle f_1, f_2, f_3 \rangle = \langle f_1, f_2, -17z \rangle .$$

L'objectif est d'étudier la situation plus générale où les polynômes ne sont pas linéaires. Pour faire la division, on doit choisir un ordre sur les indéterminées. En effet, dans le deuxième exemple, on a considéré comme premier pivot x, fait l'élimination dans la troisième équation, puis l'élimination de y. Le choix de cet ordre est essentiel pour la généralisation aux polynômes non linéaires. L'ordre est ici

$$x < y < z.$$

Avec cet ordre, le terme dominant de f_1 est y, celui de f_2 est x et celui de f_3 est $3x$. La réduction

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z.$$

consiste à soustraire des multiples de f_1 et f_2 dans f_3. On utilise les termes dominants de f_1 et f_2. Le terme $-17z$ ne peut être réduit plus en utilisant les termes dominants de f_1 et f_2.

§ 2 Structure des idéaux d'un anneau euclidien

On commence notre étude par le cas des polynômes à une indéterminée.

III.2.1. Retour sur les anneaux euclidiens.— On rappelle qu'un anneau euclidien est un anneau commutatif A vérifiant les deux propriétés suivantes

i) A est *intègre*, i.e., pour tous éléments a et b de A,

$$ab = 0 \Rightarrow (\, a = 0 \text{ ou } b = 0\,).$$

ii) il existe sur A un algorithme euclidien, i.e., une application

$$\varphi : A - \{0\} \longrightarrow \mathbb{N},$$

telle que, pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq + r, \quad \text{avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

III.1 Théorème. — Si A est un anneau euclidien, tout idéal de A est engendré par un élément.

Preuve. Soit A un anneau euclidien, muni d'un algorithme euclidien φ, et soit I un idéal de A. Si I est nul, il est engendré par 0, on a $I = \langle 0 \rangle$. Si I est non nul, alors $\varphi(I - \{0\})$ est une partie non vide de $\mathbb{N}$, elle a donc un plus petit élément n. Soit $b \in I - \{0\}$, tel que $\varphi(b) = n$. Tout élément a de I s'écrit $a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b) = n$. Or

$$r = a - bq \in I,$$

donc par minimalité de n, on ne peut pas avoir $\varphi(r) < n$, d'où nécessairement $r = 0$. Par suite, tout élément a de I s'écrit $a = bq$, ainsi $I = \langle b \rangle$. □

III.2.2. Anneaux principaux.— Soit A un anneau et I un idéal de A. On dit que I est *principal* s'il est engendré par un élément, c'est-à-dire, s'il existe un élément a de A, tel que $I = \langle a \rangle$. Un anneau est dit *principal* s'il est intègre et si tout idéal de A est principal. Le théorème III.1 montre l'implication

$$\text{euclidien} \quad \Rightarrow \quad \text{principal}.$$

III.2 Théorème. —

i) L'anneau $\mathbb{Z}$ est principal.

ii) Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est principal.

Preuve. C'est une conséquence immédiate du fait que les anneaux $\mathbb{Z}$ et $\mathbb{K}[x]$ sont euclidiens. □

Exercice 59. —

1. Montrer que l'anneau $\mathbb{Z}[x]$ n'est pas principal. [indication : considérer l'idéal engendré par les polynômes 2 et x]
2. Montrer que si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x,y]$ n'est pas principal. [indication : considérer l'idéal engendré par les polynômes x et y.]

§ 3 Les idéaux de $\mathbb{K}[x]$

III.3.1. Générateurs des idéaux de $\mathbb{K}[x]$.— Soit $\mathbb{K}$ un corps. D'après la section précédente, tout idéal I de $\mathbb{K}[x]$ est engendré par un élément. Dans ce cas, la construction de la preuve du théorème III.1 s'exprime de la façon suivante. L'idéal nul est engendré par le polynôme nul. Soit I un idéal non nul de $\mathbb{K}[x]$; notons g un polynôme non nul de I de degré minimal. Pour tout polynôme f de I, d'après le théorème de la division euclidienne, théorème I.2, il existe des polynômes q et r de $\mathbb{K}[x]$ tels que

$$f = qg + r,$$

avec $\deg(r) < \deg(g)$. Si r est non nul, alors $r = f - qg \in I$, ce qui contredit le choix de g, car $\deg(r) < \deg(g)$. Par conséquent, on a $r = 0$ et $f = qg$. Ainsi $I \subseteq \langle g \rangle$. Comme $g \in I$, on a l'égalité :

$$I = \langle g \rangle .$$

Le polynôme g ainsi obtenu est unique à un facteur près. C'est une conséquence du fait que si $\langle g_1 \rangle = \langle g_2 \rangle$, alors g_1 divise g_2 et g_2 divise g_1, donc il existe un scalaire λ tel que $g_1 = \lambda g_2$. On peut dire que le polynôme g obtenu dans cette preuve est le « *meilleur* » polynôme générateur pour l'idéal I.

III.3.2. Problème du calcul d'un générateur.— Étant donné un idéal I de $\mathbb{K}[x]$, comment calculer un polynôme g tel que $I = \langle g \rangle$? Dans un premier temps, nous allons aborder ce problème dans le cas d'un idéal engendré par deux polynômes, dont l'un au moins n'est pas nul :

$$I = \langle f_1, f_2 \rangle .$$

Par exemple, comment trouver un générateur pour l'idéal $I = \langle f_1, f_2 \rangle$ avec $f_1 = x^4 - 1$ et $f_2 = x^6 - 1$?

III.3.3. Plus grand commun diviseur.— Rappelons que le *plus grand commun diviseur* de f_1 et f_2, noté $\operatorname{pgcd}(f_1, f_2)$, est le polynôme g vérifiant les trois assertions suivantes

i) g divise f_1 et g divise f_2,

ii) si un polynôme h de $\mathbb{K}[x]$ divise f_1 et f_2, alors h divise g,

iii) $\operatorname{lc}(g) = 1$.

On a

III.3 Proposition. — Soient f_1 et f_2 deux polynômes de $\mathbb{K}[x]$, dont l'un au moins est non nul. Alors, le pgcd de f_1 et f_2 existe et on a

$$\langle f_1, f_2 \rangle = \langle \operatorname{pgcd}(f_1, f_2) \rangle .$$

Preuve. D'après la section III.3.1, il existe un polynôme g de $\mathbb{K}[x]$ tel que

$$\langle f_1, f_2 \rangle = \langle g \rangle .$$

Le polynôme g étant unique à un facteur près, on peut supposer que $\operatorname{lc}(g) = 1$. Montrons que $g = \operatorname{pgcd}(f_1, f_2)$. Comme $f_1, f_2 \in \langle g \rangle$, alors g divise à la fois f_1 et f_2. Supposons qu'un polynôme h divise à la fois f_1 et f_2. Comme g est dans l'idéal $\langle f_1, f_2 \rangle$, il existe une décomposition de g en

$$g = h_1 f_1 + h_2 f_2,$$

où h_1 et h_2 sont deux polynômes de $\mathbb{K}[x]$. Par suite, h divise g. □

Remarque III.4. — La preuve de la proposition précédente permet également de montrer l'existence et l'unicité du pgcd de deux polynômes.

Le problème de trouver un unique générateur de l'idéal $\langle f_1, f_2 \rangle$ se réduit ainsi à celui du calcul du pgcd de f_1 et f_2.

Exercice 60. — Soient f et g deux polynômes de $\mathbb{K}[x]$. Montrer qu'il existe des polynômes u et v de $\mathbb{K}[x]$, tels que

$$uf + vg = \operatorname{pgcd}(f, g).$$

III.3.4. Algorithme de la division euclidienne.— L'*algorithme d'Euclide* permet de calculer le pgcd en utilisant l'algorithme de division vu dans le premier chapitre. Il est basé sur le résultat suivant :

III.5 Proposition. — Soient f_1 et f_2 deux polynômes de $\mathbb{K}[x]$, dont l'un au moins est non nul. Alors,

$$\operatorname{pgcd}(f_1, f_2) = \operatorname{pgcd}(f_1 - q f_2, f_2),$$

pour tout polynôme q de $\mathbb{K}[x]$.

Preuve. Soit q un polynôme non nul. On a $f_1 = f_1 - q f_2 + q f_2$, par suite

$$\langle f_1, f_2 \rangle = \langle f_1 - q f_2, f_2 \rangle .$$

D'après la proposition III.3, on a

$$\langle \operatorname{pgcd}(f_1, f_2) \rangle = \langle f_1, f_2 \rangle = \langle f_1 - q f_2, f_2 \rangle = \langle \operatorname{pgcd}(f_1 - q f_2, f_2) \rangle .$$

Par suite, $\operatorname{pgcd}(f_1, f_2)$ et $\operatorname{pgcd}(f_1 - q f_2, f_2)$ sont égaux à une constante multiplicative près. Le pgcd de deux polynômes étant de coefficient dominant égal à 1, on en déduit l'égalité recherchée $\operatorname{pgcd}(f_1, f_2) = \operatorname{pgcd}(f_1 - q f_2, f_2)$. □

ENTRÉE : $f_1, f_2 \in \mathbb{K}[x]$, non tous les deux nuls,

SORTIE : $f = \text{pgcd}(f_1, f_2)$.

INITIALISATION : $f := f_1$; $g := f_2$

TANT QUE : $g \neq 0$ **FAIRE**

$f \xrightarrow{g} r$, où r est le reste de la division de f par g,

$f := g$,

$g := r$,

$f := \frac{1}{\text{lc}(f)} f$.

L'algorithme d'Euclide.

Exercice 61. — Montrer que l'algorithme d'Euclide termine.

III.3.5. Exemple.— Illustrons l'algorithme d'Euclide sur le calcul du pgcd des polynômes $f_1 = x^3 + x^2 - 5x + 3$ et $f_2 = x^2 + x - 2$ de $\mathbb{Q}[x]$.

INITIALISATION : $f := x^3 + x^2 - 5x + 3$, $g := x^2 + x - 2$.
Début de la boucle **TANT QUE :**
Première itération de la boucle **TANT QUE :**
$x^3 + x^2 - 5x + 3 \xrightarrow{g} -3x + 3$,
$f := x^2 + x - 2$,
$g := -3x + 3$,
Deuxième itération de la boucle **TANT QUE :**
$x^2 + x - 2 \xrightarrow{g} 0$,
$f := -3x + 3$,
$g := 0$,
Arrêt de la boucle **TANT QUE :**
$f := \frac{1}{\text{lc}(f)} f = \frac{1}{-3}(-3x + 3) = x - 1$.

Par suite, $\text{pgcd}(f_1, f_2) = x - 1$.

III.3.6. Exemple.— Pour calculer le pgcd des polynômes $f_1 = x^4 - 1$ et $f_2 = x^6 - 1$:

$$\begin{aligned} x^4 - 1 &= 0(x^6 - 1) + x^4 - 1, \\ x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1 \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0. \end{aligned}$$

Ainsi

$$\text{pgcd}(f_1, f_2) = \text{pgcd}(x^6 - 1, x^4 - 1) = \text{pgcd}(x^4 - 1, x^2 - 1) = \text{pgcd}(x^2 - 1, 0) = x^2 - 1.$$

En conséquence,

$$\langle f_1, f_2 \rangle = \langle x^2 - 1 \rangle .$$

III.3.7. Cas d'un idéal engendré par plus de deux polynômes.— Considérons un idéal $I = \langle f_1, \ldots, f_s \rangle$ de $\mathbb{K}[x]$ engendré par des polynômes non tous nuls. Rappelons que le *plus grand commun diviseur* des polynômes $f_1, \ldots, f_s$, noté $\text{pgcd}(f_1, \ldots, f_s)$, est le polynôme g vérifiant les trois assertions suivantes

i) g divise f_i, pour tout $i \in [\![1, s]\!]$

ii) si un polynôme h de $\mathbb{K}[x]$ divise f_i, pour tout $i \in [\![1, s]\!]$, alors h divise g,

iii) $\text{lc}(g) = 1$.

On a

III.6 Proposition. — Soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x]$, non tous nuls. Alors,

i) $\langle f_1, \ldots, f_s \rangle = \langle \text{pgcd}(f_1, \ldots, f_s) \rangle$,

ii) pour $s \geq 3$, alors $\text{pgcd}(f_1, \ldots, f_s) = \text{pgcd}(f_1, \text{pgcd}(f_2, \ldots, f_s))$.

Preuve. Montrons l'assertion **i)**. L'anneau $\mathbb{K}[x]$ étant principal, il existe un polynôme g de $\mathbb{K}[x]$ tel que

$$\langle f_1, \ldots, f_s \rangle = \langle g \rangle .$$

Le polynôme g étant unique à une constante près, on peut supposer que $\text{lc}(g) = 1$. Montrons que $g = \text{pgcd}(f_1, \ldots, f_s)$. Comme $f_1, \ldots, f_s \in \langle g \rangle$, alors g divise tous les polynômes $f_1, \ldots, f_s$. Supposons qu'un polynôme h divise tous les polynômes $f_1, \ldots, f_s$. Comme g est dans l'idéal $\langle f_1, \ldots, f_s \rangle$, il existe une décomposition de g en

$$g = h_1 f_1 + h_2 f_2 + \ldots + h_s f_s,$$

où $h_1, h_2, \ldots, h_s$ sont des polynômes de $\mathbb{K}[x]$. Par suite, h divise g.

Montrons l'assertion **ii)**. Posons $h = \text{pgcd}(f_2, \ldots, f_s)$. D'après **i)**, on a $\langle f_2, \ldots, f_s \rangle = \langle h \rangle$. Ainsi

$$\langle f_1, \ldots, f_s \rangle = \langle f_1, h \rangle .$$

Toujours d'après **i)**,

$$\text{pgcd}(f_1, \ldots, f_s) = \text{pgcd}(f_1, h) = \text{pgcd}(f_1, \text{pgcd}(f_2, \ldots, f_s)).$$

□

III.3.8. Exemple.— Calculons le générateur de l'idéal

$$I = \left\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \right\rangle \subset \mathbb{K}[x].$$

On a

$$\begin{aligned} \text{pgcd}(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \text{pgcd}(x^3 - 3x + 2, \text{pgcd}(x^4 - 1, x^6 - 1)) \\ &= \text{pgcd}(x^3 - 3x + 2, x^2 - 1) = x - 1. \end{aligned}$$

Ainsi

$$I = \langle x - 1 \rangle .$$

III.3.9. Problèmes.— Nous pouvons répondre dans le cas d'une indéterminée aux problèmes posés dans le chapitre précédent.

a) Problème de la description d'un idéal :

- tout idéal I de $\mathbb{K}[x]$ possède un unique générateur,
- il existe un « *meilleur* » générateur, c'est le pgcd des polynômes qui engendrent I.

b) Problème de l'appartenance à un idéal :

étant donné un idéal $I = \langle f_1, \dots, f_s \rangle$ et un polynôme f de $\mathbb{K}[x]$, pour déterminer si $f \in I$, on calcule $g = \text{pgcd}(f_1, \dots, f_s)$, puis on divise f par g. Le reste de cette division est nul si, et seulement si, $f \in I$, i.e.,

$$f \xrightarrow{g} 0 \quad \text{si, et seulement si,} \quad f \in I = \langle g \rangle .$$

c) Problème de la résolution d'équations polynomiales :

étant donnés des polynômes $f_1, \dots, f_s$ de $\mathbb{K}[x]$, les solutions dans $\mathbb{K}$ du système d'équations polynomiales

$$\begin{cases} f_1(x) = 0 \\ \quad \vdots \\ f_s(x) = 0 \end{cases}$$

sont les solutions de l'équation

$$g(x) = 0,$$

où $g = \text{pgcd}(f_1, \dots, f_s)$.

III.3.10. Exemple.— Comment déterminer si le polynôme $f = x^3 + 4x^2 + 3x - 7$ appartient à l'idéal

$$I = \left\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \right\rangle .$$

On a montré que $I = \langle x - 1 \rangle$. On a calcule la division de f par $x - 1$:

$$x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1.$$

Ainsi, la réduction de f par $x - 1$ est 1 :

$$x^3 + 4x^2 + 3x - 7 \xrightarrow{x-1} 1$$

On en déduit que f n'appartient pas à l'idéal I.

Exercice 62. — Déterminer si le polynôme f est contenu dans l'idéal I de $\mathbb{K}[x]$.

1. $f = x^2 - 3x + 2$, $I = \langle x - 2 \rangle$,
2. $f = x^5 - 4x + 1$, $I = \left\langle x^3 - x^2 + x \right\rangle$,
3. $f = x^2 - 4x + 4$, $I = \left\langle x^4 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8 \right\rangle$,
4. $f = x^3 - 1$, $I = \left\langle x^9 - 1, x^5 + x^3 - x^2 - 1 \right\rangle$.

Exercice 63. — Étant donnés des polynômes $f_1, \dots, f_s$ de $\mathbb{K}[x]$, existe-t-il un algorithme pour décider si l'ensemble algébrique affine $\mathbf{V}(f_1, \dots, f_s)$ est non vide ? Dans le cas où $\mathbb{K} = \mathbb{C}$ la réponse est affirmative.

1. Soit f est un polynôme non nul de $\mathbb{C}[x]$, montrer que $\mathbf{V}(f)$ est vide si, et seulement si, f est constant.
2. Soit $f_1, \dots, f_s$ des polynômes de $\mathbb{C}[x]$. Montrer que $\mathbf{V}(f_1, \dots, f_s)$ est vide si, et seulement si, $\text{pgcd}(f_1, \dots, f_s) = 1$.
3. Décrire une méthode algorithmique pour déterminer si $\mathbf{V}(f_1, \dots, f_s)$ est non vide.
4. Que peut-on dire dans le cas où $\mathbb{K} = \mathbb{R}$?

III.3.11. En conclusion.— Nous avons vu que la notion de réduction via l'algorithme de division est un point clef dans la résolution des problèmes mentionnés en III.3.9. Nous n'avons pas mis en évidence l'importance d'ordonner les termes dans le cas d'une seule indéterminée, car il existe un ordre naturel dans ce cas, celui donné par le degré des termes. Dans la réduction

$$f \xrightarrow{g} f - \frac{\text{lt}(f)}{\text{lt}(g)} g,$$

le reste $f - \frac{\text{lt}(f)}{\text{lt}(g)} g$ est de degré strictement inférieur au degré de f. C'est la raison pour laquelle l'algorithme termine ; c'est une conséquence du fait que

$$n < m \quad \text{si, et seulement si} \quad x^n \text{ divise } x^m.$$

La fin de ce chapitre est consacré au problème de cette réduction dans le cas de plusieurs indéterminées.

§ 4 Les ordres monomiaux

Nous noterons $\mathscr{M}(x_1, \dots, x_n)$, ou $\mathscr{M}$ s'il n'y a pas de confusion, l'ensemble des monômes en les indéterminées $x_1, \dots, x_n$:

$$\mathscr{M}(x_1, \dots, x_n) = \{x^\alpha \mid \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}.$$

III.4.1. Ordre monomial.— Un *ordre monomial* sur $\mathscr{M}$ est une relation $\preccurlyeq$ vérifiant les assertions suivantes

i) $\preccurlyeq$ est un ordre total sur $\mathscr{M}$,
ii) si $x^\alpha \preccurlyeq x^\beta$, alors $x^\alpha x^\gamma \preccurlyeq x^\beta x^\gamma$, pour tous x^α, x^β et x^γ dans $\mathscr{M}$,
iii) $1 \preccurlyeq x^\alpha$, pour tout $x^\alpha \in \mathscr{M}$.

III.4.2. Ordre lexicographique.— Étant donné un *ordre alphabétique*

$$x_n < \ \dots \ < x_2 < x_1$$

i.e., un ordre sur l'ensemble des indéterminées, on définit l'*ordre lexicographique* $\preccurlyeq_{\text{lex}}$ sur $\mathscr{M}$ en posant, pour tous n-uplets d'entiers naturels $\alpha = (\alpha_1, \dots, \alpha_n)$ et $\beta = (\beta_1, \dots, \beta_n)$,

$$x^\alpha \preccurlyeq_{\text{lex}} x^\beta$$

si, et seulement si, les premières coordonnées α_i et β_i, en partant de la gauche dans α et β, qui sont différentes satisfont à $\alpha_i < \beta_i$.

III.4.3. Exemple.— Supposons que l'on ait deux indéterminées avec l'ordre alphabétique $y < x$, on a

$$1 = y^0 \preccurlyeq_{\text{lex}} y \preccurlyeq_{\text{lex}} y^2 \preccurlyeq_{\text{lex}} y^3 \preccurlyeq_{\text{lex}} \dots \preccurlyeq_{\text{lex}} x \preccurlyeq_{\text{lex}} yx \preccurlyeq_{\text{lex}} y^2x \preccurlyeq_{\text{lex}} \dots \preccurlyeq_{\text{lex}} x^2 \preccurlyeq_{\text{lex}} yx^2 \preccurlyeq_{\text{lex}} \dots$$

III.4.4. Remarque.— L'ordre lexicographique dépend de l'ordre alphabétique sur les indéterminées. Tout ordre alphabétique sur les indéterminées $x_1, \dots, x_n$ définit un ordre lexicographique sur $\mathscr{M}(x_1, \dots, x_n)$.

Exercice 64. — Montrer qu'il existe $n!$ ordres lexicographiques possibles sur cet ensemble de monômes.

Notons que $x^\alpha \preccurlyeq_{\text{lex}} x^\beta$ si, et seulement si, le premier entier non nul dans le n-uplet

$$\beta - \alpha = (\beta_1 - \alpha_1, \dots, \beta_n - \alpha_n) \in \mathbb{Z}^n$$

est positif. Par exemple, si $z < y < x$, on a

a) $y^2z^4 \preccurlyeq_{\text{lex}} xy^2$, car $\beta - \alpha = (1, 0, -4)$,

b) $x^3y^2z^1 \preccurlyeq_{\text{lex}} x^3y^2z^4$, car $\beta - \alpha = (0, 0, 3)$.

c) $y^3z^4 \preccurlyeq_{\text{lex}} x$, car $\beta - \alpha = (1, -3, -4)$.

III.7 Proposition. — L'ordre lexicographique $\preccurlyeq_{\text{lex}}$ est un ordre monomial.

Exercice 65. — Montrer la proposition III.7.

III.4.5. Propriétés des ordres monomiaux.—

III.8 Proposition. — Soit $\preccurlyeq$ un ordre monomial sur $\mathscr{M}$. Soient x^α et x^β deux monômes de $\mathscr{M}$, tels que x^α divise x^β, alors $x^\alpha \preccurlyeq x^\beta$.

Preuve. Si le monôme x^α divise le monôme x^β, il existe alors un monôme x^γ dans $\mathscr{M}$, tel que $x^\beta = x^\alpha x^\gamma$. L'ordre $\preccurlyeq$ étant monomial, on a $1 \preccurlyeq x^\gamma$, d'où $x^\alpha \preccurlyeq x^\alpha x^\gamma = x^\beta$. □

Exercice 66. — Montrer qu'il n'y a qu'un seul ordre monomial sur $\mathscr{M}(x_1)$.

Tout bon ordre est un ordre total, remarque I.6.5. La réciproque est fausse en général, cependant pour les ordres monomiaux, on a

III.9 Proposition. — Tout ordre monomial sur $\mathscr{M}$ est un bon ordre.

En particulier, toute suite décroissante de monômes

$$\dots \preccurlyeq x^{\alpha_{i_k}} \preccurlyeq \dots \preccurlyeq x^{\alpha_{i_2}} \preccurlyeq x^{\alpha_{i_1}}$$

termine.

Exercice 67. — 1. Soit $\preccurlyeq$ un ordre monomial sur $\mathscr{M}(x_1, \dots, x_{n+1})$, montrer que $\preccurlyeq$ induit un ordre monomial sur $\mathscr{M}(x_1, \dots, x_n)$.

2. Soient x^α et x^β deux mônomes de $\mathscr{M}(x_1, \dots, x_n)$, et k, l deux entiers naturels tels que

$$x^\alpha x_{n+1}^k \preccurlyeq x^\beta x_{n+1}^l.$$

Montrer que

$$x^\alpha \preccurlyeq x^\beta \text{ ou } k \leq l.$$

3. Montrer la proposition III.9. (Indication : on fera une récurrence sur le nombre d'indéterminée.)

III.4.6. Définitions.— Fixons un ordre monomial $\preccurlyeq$ sur $\mathscr{M}(x_1, \dots, x_n)$. Tout polynôme non nul f de $\mathbb{K}[x_1, \dots, x_n]$ peut s'écrire sous la forme

$$f = a_1x^{\alpha_{i_1}} + a_2x^{\alpha_{i_2}} + \dots + a_rx^{\alpha_{i_r}},$$

où les a_k sont des scalaires non nul, les $x^{\alpha_{i_k}}$ des monômes de $\mathscr{M}(x_1, \dots, x_n)$ deux à deux distincts et

$$x^{\alpha_{i_r}} \preccurlyeq \dots \preccurlyeq x^{\alpha_{i_2}} \preccurlyeq x^{\alpha_{i_1}}.$$

Le n-uplet α_{i_1} est appelé le *multidegré* de f, on le note $\text{multideg}(f)$:

$$\text{multideg}(f) = \alpha \text{ tel que } x^\alpha \text{ est le plus grand monôme apparaissant dans } f.$$

On dit alors

i) que a_1 est le *coefficient de plus haut degré* de f (*leading coefficient*) de f, noté $\text{lc}(f)$,

ii) que $a_1x^{\alpha_{i_1}}$ est le *terme de plus haut degré* f (*leading term*), noté $\text{lt}(f)$,

iii) que $x^{\alpha_{i_1}}$ est le *monôme de plus haut degré de* f (*leading monomial*), noté $\text{lm}(f)$.

Si g est un second polynôme non nul de $\mathbb{K}[x_1, \dots, x_n]$, on dit que f est de multidegré plus petit que g si le monôme de plus haut degré de f est plus petit que celui de g :

$$\text{multideg}(f) \leq \text{multideg}(g) \text{ si } \text{lm}(f) \preccurlyeq \text{lm}(g).$$

On pose, par ailleurs $\text{lc}(0) = \text{lt}(0) = \text{lm}(0) = 0$.

III.4.7. Remarque.— Un ordre monomial étant un bon ordre, on peut faire des raisonnements par récurrence sur le multidegré.

III.4.8. Exemple.— Considérons l'ordre alphabétique $z < y < x$ et soit f le polynôme

$$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2,$$

on a,

$$\text{multideg}(f) = (3,0,0),\ \text{lc}(f) = -5,\ \text{lm}(f) = x^3,\ \text{lt}(f) = -5x^3.$$

Exercice 68. — On fixe un ordre monomial sur $\mathscr{M}(x_1, \dots, x_n)$.

1. Montrer que pour tous polynôme f et monôme m de $\mathbb{K}[x_1, \dots, x_n]$, on a

$$\text{lt}(mf) = m\text{lt}(f).$$

2. Soient f et g des polynômes de $\mathbb{K}[x_1,\dots,x_n]$, a-t-on toujours $\mathrm{lt}(fg)=\mathrm{lt}(f)\,\mathrm{lt}(g)$?
3. Soient $f_1,\dots,f_s,g_1,\dots,g_s$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$. A-t-on

$$\mathrm{lm}(f_1g_1+\dots+f_sg_s)=\mathrm{lm}(f_i)\mathrm{lm}(g_i),$$

pour un $i\in[\![1,s]\!]$?

III.10 Proposition.— On fixe un ordre monomial sur $\mathscr{M}(x_1,\dots,x_n)$. Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Le multidegré vérifie les propriétés suivantes :

i) $\mathrm{multideg}(fg)=\mathrm{multideg}(f)+\mathrm{multideg}(g)$;

ii) si $f+g$ est non nul, alors $\mathrm{multideg}(f+g)\leq\max(\mathrm{multideg}(f),\mathrm{multideg}(g))$ et si, de plus $\mathrm{multideg}(f)\neq\mathrm{multideg}(g)$, on a l'égalité.

Exercice 69.— Montrer la Proposition III.10.

Exercice 70.— On fixe un ordre monomial sur $\mathscr{M}(x_1,\dots,x_n)$. Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. On admettra qu'il existe un unique polynôme d (le pgcd de f et g, noté $\mathrm{pgcd}(f,g)$) dans $\mathbb{K}[x_1,\dots,x_n]$ [1] vérifiant

i) d divise f et d divise g,

ii) si un polynôme h de $\mathbb{K}[x_1,\dots,x_n]$ divise f et g, alors h divise d,

iii) $\mathrm{lc}(d)=1$.

1. Vérifier que $<f,g>\subseteq<\mathrm{pgcd}(f,g)>$.
2. Montrer que l'idéal $<f,g>$ est principal si et seulement si $<f,g>=<\mathrm{pgcd}(f,g)>$.
3. Montrer que $\mathrm{pgcd}(f,g)$ a un multidegré maximal parmi les diviseurs communs de f et g.
4. Vérifier que tout polynôme non nul de $<f,g>$ a un multidegré supérieur ou égal à celui de $\mathrm{pgcd}(f,g)$.
5. Montrer que si l'idéal $<f,g>$ contient un polynôme de même multidegré que celui de $\mathrm{pgcd}(f,g)$, alors $<f,g>=<\mathrm{pgcd}(f,g)>$.
6. On considère $K[x,y]$ et un ordre monomial sur $\mathscr{M}(x,y)$ tel que $y\preccurlyeq x$. Montrer que y a un multidegré minimal parmi les polynômes non nuls de l'idéal $<x,y>$.
7. Vérifier que 1 est le pgcd de x et y.

III.4.9. Ordre lexicographique gradué.— Étant donné un ordre alphabétique $x_n<\dots<x_2<x_1$, on définit l'*ordre lexicographique gradué* $\preccurlyeq_{\mathrm{grlex}}$ sur $\mathscr{M}$ de la façon suivante : pour $\alpha=(\alpha_1,\dots,\alpha_n)$ et $\beta=(\beta_1,\dots,\beta_n)$, on pose

$$x^\alpha\preccurlyeq_{\mathrm{grlex}}x^\beta$$

si, et seulement si,

$$\left(\sum_{i=1}^n\alpha_i<\sum_{i=1}^n\beta_i\right)\quad\text{ou}\quad\left(\sum_{i=1}^n\alpha_i=\sum_{i=1}^n\beta_i\quad\text{et}\quad x^\alpha\preccurlyeq_{\mathrm{lex}}x^\beta\right).$$

1. Ce résultat suit du fait que, de même que pour une seule indéterminée, l'anneau $\mathbb{K}[x_1,\dots,x_n]$ est un anneau factoriel, c'est-à-dire que tout polynôme se factorise de manière unique en produit de facteurs irréductibles.

Par exemple, avec $y<x$, on a

$$1\preccurlyeq_{\mathrm{grlex}}y\preccurlyeq_{\mathrm{grlex}}x\preccurlyeq_{\mathrm{grlex}}y^2\preccurlyeq_{\mathrm{grlex}}xy\preccurlyeq_{\mathrm{grlex}}x^2\preccurlyeq_{\mathrm{grlex}}y^3$$

Exercice 71.— Montrer que $\preccurlyeq_{\mathrm{grlex}}$ est un ordre monomial.

Exercice 72.— On considère les ordres $\preccurlyeq_{\mathrm{lex}}$ et $\preccurlyeq_{\mathrm{grlex}}$ sur $\mathscr{M}(x,y,z)$ à partir de l'ordre alphabétique $x>y>z$.

Classer par ordre lexicographique croissant, puis par ordre lexicographique gradué croissant les monômes suivants :

$$x^2y^3z^4,\quad x^3z,\quad x^2y^4,\quad y^7z^2,\quad xyz^2.$$

Exercice 73.— Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Montrer que $\deg(fg)=\deg(f)+\deg(g)$ où deg désigne le degré total.

§ 5 Algorithme de division en plusieurs indéterminées

L'objectif de cette partie est de définir un algorithme de division pour les polynômes à plusieurs indéterminées qui généralise l'algorithme de division pour les polynômes à une indéterminée.

Dans $\mathbb{K}[x]$, la division d'un polynôme f par g donne une décomposition de f sous la forme

$$f=qg+r,$$

avec $\deg(r)<\deg(g)$, théorème I.2. Dans le cas général, l'objectif est de divisiser un polynôme f de $\mathbb{K}[x_1,\dots,x_n]$ par un ensemble de polynômes $f_1,\dots,f_s\in\mathbb{K}[x_1,\dots,x_n]$. Nous allons voir que cela consiste à écrire le polynôme f sous la forme

$$f=u_1f_1+\dots+u_sf_s+r,$$

où les *quotients* sont les polynômes $u_1,\dots,u_s\in\mathbb{K}[x_1,\dots,x_n]$ et le *reste* est le polynôme $r\in\mathbb{K}[x_1,\dots,x_n]$.

Le principe de l'algorithme de division d'un polynôme f à plusieurs indéterminées par un ensemble de polynômes $f_1,\dots,f_s$ est le même que dans le cas à une seule indéterminée :

1. fixer un ordre sur les termes,
2. remplacer le terme dominant de f en multipliant un des f_i par un terme approprié et soustraire le résultat à f ; ce terme est alors un terme du quotient u_i,
3. procèder ainsi avec tous les polynômes $f_1,\dots,f_s$.

III.5.1. Premier exemple.— Posons $f=xy^2+1$, $f_1=xy+1$ et $f_2=y+1$. On fixe l'ordre alphabétique $y<x$ et l'ordre lexicographique associé sur les termes. Le terme dominant $\mathrm{lt}(f)=xy^2$ est divisible par les termes dominants $\mathrm{lt}(f_1)=xy$ et $\mathrm{lt}(f_2)=y$:

$$\begin{array}{rl|l} xy^2 & +1 & xy+1 \\ \cline{3-3} xy^2 & +y & y \\ \cline{1-2} 1 & -y & \end{array}$$

$$\begin{array}{rl|l} 1 & -y & y+1 \\ \hline -y & -1 & -1 \\ \hline & 2 & \end{array}$$

Comme $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas 2, ce reste est irréductible. On a obtenu les réductions [2]

$$xy^2+1 \xrightarrow{f_1} 1-y \xrightarrow{f_2} 2.$$

On écrit

$$xy^2 \xrightarrow{f_1,f_2} 2.$$

Le polynôme f s'écrit alors sous la forme

$$xy^2+1 = y(xy+1)+(-1)(y+1)+2.$$

Nous aurions commencé par la division par f_2 :

$$\begin{array}{rl|l} xy^2 & +1 & y+1 \\ \hline xy^2 & +xy & xy \\ \hline -xy & +1 & \end{array}$$

$$\begin{array}{rl|l} -xy & +1 & y+1 \\ \hline -xy & -1 & -1 \\ \hline 2 & & \end{array}$$

Comme $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas 2, ce reste est irréductible. On a obtenu les réductions

$$xy^2+1 \xrightarrow{f_2} -xy+1 \xrightarrow{f_1} 2,$$

soit

$$xy^2 \xrightarrow{f_2,f_1} 2.$$

Le polynôme f s'écrit alors sous la forme

$$xy^2+1 = (-1)(xy+1)+(xy)(y+1)+2.$$

On notera que les restes de ces deux divisions sont égaux, mais les quotients différents. Après la première réduction par f_2, on peut encore appliquer la réduction par f_2, car $\mathrm{lt}(f_2)$ divise $-xy$:

$$\begin{array}{rl|l} xy^2 & +1 & y+1 \\ \hline xy^2 & +xy & xy \\ \hline -xy & +1 & \end{array}$$

$$\begin{array}{rl|l} -xy & +1 & y+1 \\ \hline -xy & -x & -x \\ \hline x & +1 & \end{array}$$

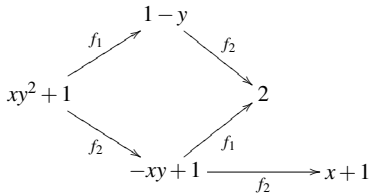
Le polynôme $x+1$ est le dernier reste, car les termes x et 1 ne sont pas divisibles par les

2. voir partie suivante 6

termes dominants de f_1 et f_2. Dans ce cas, la décomposition est

$$xy^2+1 = (0)(xy+1)+(xy-x)(y+1)+(x+1).$$

La situation est la suivante :



III.5.2. Deuxième exemple.— Soient $f = x^2y+xy^2+y^2$, $f_1 = xy-1$ et $f_2 = y^2-1$. Comme dans les exemples précédents, on considère l'ordre lexicographique, avec l'ordre alphabétique $y < x$. On effectue la division de f par f_1 puis par f_2

$$\begin{array}{rl|l} x^2y & +xy^2 & +y^2 \quad xy-1 \\ \hline x^2y & -x & x \\ \hline x & +xy^2 & +y^2 \end{array} \qquad x^2y+xy^2+y^2 \xrightarrow{f_1} x+xy^2+y^2$$

$$\begin{array}{rl|l} xy^2 & +x & +y^2 \quad xy-1 \\ \hline xy^2 & -y & y \\ \hline x & +y & +y^2 \end{array} \qquad xy^2+x+y^2 \xrightarrow{f_1} x+y+y^2$$

Les termes dominants $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$ ne divisent pas le terme dominant $\mathrm{lt}\left(x+y^2+y\right) = x$. Cependant, $x+y^2+y$ n'est pas le reste, car $\mathrm{lt}(f_2)$ divise y^2. On extrait alors le terme x du reste et on poursuit la division :

$$\begin{array}{rl|l} y^2 & +y & y^2-1 \\ \hline y^2 & -1 & 1 \\ \hline y & +1 & \end{array} \qquad x+y^2+y \xrightarrow{f_2} x+y+1$$

Après cette division, le reste est $x+y+1$. Les termes dominants de f_1 et f_2 ne divisent aucun terme de $x+y+1$, qui est ainsi le dernier reste. On a

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

et

$$x^2y+xy^2+y^2 \xrightarrow{f_1,f_2} x+y+1.$$

Ces exemples illustrent le théorème suivant et le second exemple éclaire le fonctionnement de l'algorithme de division associé.

III.11 Théorème.— Soit $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Étant donné un ordre monomial $\preccurlyeq$ sur $\mathscr{M}(x_1, \ldots, x_n)$, tout polynôme non nul f de $\mathbb{K}[x_1, \ldots, x_n]$ s'écrit sous la forme

$$f = u_1 f_1 + \ldots + u_s f_s + r,$$

où $u_1, \ldots, u_s, r$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, tels que $r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$. On a de plus, pour tout quotient $u_i \neq 0$,

$$\mathrm{multideg}(u_i f_i) \leq \mathrm{multideg}(f).$$

Preuve. On fait un raisonnement par récurrence sur le multidegré. Soit f un polynôme non nul et supposons que le résultat est vérifié pour tout polynôme non nul de multidegré strictement inférieur à celui de f. Alors,

– ou bien il existe i, tel que $\mathrm{lt}(f_i)$ divise $\mathrm{lt}(f)$. Dans ce cas on choisit un tel j et on effectue la division de f par f_j et on obtient

$$f = \frac{\mathrm{lt}(f)}{\mathrm{lt}(f_j)} f_j + g$$

avec g nul ou $\mathrm{multideg}(g) < \mathrm{multideg}(f)$. Si g est nul, le résultat est vérifié car

$$\mathrm{multideg}\left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_j)} f_j\right) = \mathrm{multideg}(f).$$

Sinon, par hypothèse de récurrence,

$$g = u'_1 f_1 + \ldots + u'_j f_j + \ldots + u'_s f_s + r$$

où $u'_1, \ldots, u'_s, r$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, tels que
– $r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$;
– $\mathrm{multideg}(u'_i f_i) \leq \mathrm{multideg}(g) < \mathrm{multideg}(f)$ pour tout $u'_i \neq 0$.
On obtient

$$f = u'_1 f_1 + \ldots + \left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_i)} + u'_i\right) f_i + \ldots + u'_s f_s + r$$

avec les propriétés souhaitées car

$$\mathrm{multideg}\left(\left(\frac{\mathrm{lt}(f)}{\mathrm{lt}(f_i)} + u'_i\right) f_i\right) = \mathrm{multideg}(f);$$

– ou bien le terme dominant $\mathrm{lt}(f)$ de f n'est divisible pas aucun des $\mathrm{lt}(f_i)$. Dans ce cas, si $f = \mathrm{lt}(f)$ c'est terminé, sinon on applique l'hypothèse de récurrence à $g = f - \mathrm{lt}(f)$. Alors

$$g = u_1 f_1 + \ldots + u_i f_i + \ldots + u_s f_s + r'$$

avec les bonnes propriétés et donc

$$f = u_1 f_1 + \ldots + u_i f_i + \ldots + u_s f_s + (\mathrm{lt}(f) + r')$$

avec les propriétés souhaitées.

□

Notons que dans les exemples précédents, les quotients u_i et le reste r ne sont pas uniques. Ils dépendent du choix de la suite des divisions effectuées.

III.5.3. Algorithme de division dans $\mathbb{K}[x_1, \ldots, x_n]$.— La preuve du théorème III.11 correspond à l'algorithme de division suivant

ENTRÉE : $f_1, \ldots, f_s, f \in \mathbb{K}[x_1, \ldots, x_n]$,
SORTIE : $u_1, \ldots, u_s, r \in \mathbb{K}[x_1, \ldots, x_n]$ tels que
$r = 0$ ou r est une somme de termes non divisibles par $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$.
INITIALISATION : $u_1 := 0, \ldots u_s := 0, \quad r := 0, \quad p := f$;
TANT QUE : $p \neq 0$ **FAIRE**
  $i := 1$
  $div := faux$
  TANT QUE : $(i \leq s$ **ET** $div = faux)$ **FAIRE**
    SI ($\mathrm{lt}(f_i)$ divise $\mathrm{lt}(p)$) **ALORS**
      $u_i := u_i + \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$
      $p := p - \dfrac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$
      $div := vrai$
    SINON $i := i + 1$
  SI $div = faux$ **ALORS**
    $r := r + \mathrm{lt}(p)$
    $p := p - \mathrm{lt}(p)$

Algorithme de la division des polynômes à plusieurs indéterminées.

Cet algorithme est constitué de deux parties principales :
– une *étape de division*, si $\mathrm{lt}(f_i)$ divise $\mathrm{lt}(p)$ pour un i, l'algorithme procède à la division comme dans le cas d'une seule indéterminée avec le premier i vérifiant cette condition,
– une *étape de reste*, si $\mathrm{lt}(f_i)$ ne divise $\mathrm{lt}(p)$ pour aucun i, l'algorithme rajoute $\mathrm{lt}(p)$ au reste.
Le polynôme r obtenu par cet algorithme est appelé le *reste* de la division de f par $f_1, \ldots, f_s$, on note

$$f \xrightarrow{f_1, \ldots, f_s} r.$$

III.5.4. Remarque sur la non unicité du reste.— Contrairement à la division dans le cas d'une seule indéterminée, le reste n'est pas unique, il dépend de l'ordre des polynômes $f_1, \ldots, f_s$

dans l'algorithme de division. En effet, reprenons le deuxième exemple avec $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ et $f_2 = y^2 - 1$, avec l'ordre lexicographique associé à l'ordre alphabétique $y < x$. On a effectué la division de f par f_1 puis par f_2

$$f \xrightarrow{f_1} x + xy^2 + y^2 \xrightarrow{f_1} x + y + y^2 \xrightarrow{f_2} x + y + 1$$

soit

$$f \xrightarrow{f_1,f_2} x + y + 1.$$

Changeons l'ordre des diviseurs en prenant pour premier diviseur f_2 :

$$\begin{array}{l|l} x^2y + xy^2 + y^2 & y^2 - 1 \\ \hline xy^2 - x & x \\ \hline x^2y + y^2 + x & \end{array}$$

$$\begin{array}{l|l} x^2y + y^2 + x & y^2 - 1 \\ \hline y^2 - 1 & 1 \\ \hline x^2y + x + 1 & \end{array}$$

On divise alors le reste obtenu par f_1 :

$$\begin{array}{l|l} x^2y + x + 1 & xy - 1 \\ \hline x^2y - x & x \\ \hline 2x + 1 & \end{array}$$

On a ainsi

$$x^2y + xy^2 + y^2 = (x)(xy - 1) + (x + 1)(y^2 - 1) + 2x + 1.$$

Soit

$$f \xrightarrow{f_2} x^2y + y^2 + x \xrightarrow{f_2} x^2y + x + 1 \xrightarrow{f_1} 2x + 1$$

et donc

$$f \xrightarrow{f_2,f_1} 2x + 1.$$

Le reste obtenu par ce chemin de réduction n'est pas le même. Cet exemple illustre que l'ordre des polynômes $f_1, \ldots, f_s$ dans l'algorithme de division a une influence sur le reste r et les polynômes $u_1, \ldots, u_s$. Ce point est une obstruction à la résolution du problème de l'appartenance à un idéal. En effet, si après la division de f par $f_1, \ldots, f_s$, on obtient un reste nul, i.e.,

$$f = u_1 f_1 + \ldots + u_s f_s,$$

alors $f \in I = \langle f_1, \ldots, f_s \rangle$. On a

$$\text{si } f \xrightarrow{f_1,\ldots,f_s} 0, \quad \text{alors } f \in I.$$

Cependant, la réciproque n'est pas vraie comme le montre l'exemple suivant.

III.5.5. Exemple.— Soient $f = xy^2 - x$ et I l'idéal de $\mathbb{K}[x,y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$. On a

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y),$$

soit

$$f \xrightarrow{f_1,f_2} -x - y.$$

Mais si on considère l'ordre f_2, f_1, on a

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0,$$

ainsi

$$f \xrightarrow{f_2,f_1} 0,$$

par suite $f \in I$. C'est ainsi que l'on peut avoir $f \in I$ sans que f se réduise à 0 par un ensemble de polynômes qui engendrent I. L'algorithme de division que nous venons de construire présente sur ce point une difficulté. Pour remédier à cela, l'objectif est de construire un « *bon* » ensemble de générateurs pour l'idéal I. C'est-à-dire un ensemble de générateurs G de l'idéal I, pour lequel le reste de la division par G est unique, peu importe l'ordre utilisé sur les diviseurs $g_1, g_2, \ldots, g_t$ avec $G = \{g_1, \ldots, g_t\}$, et que l'on ait ainsi

$$f \in I \quad \text{si, et seulement si,} \quad f \xrightarrow{g_1,\ldots,g_t} 0.$$

L'existence d'un ensemble de générateur satisfaisant cette propriété fera l'objet du prochain chapitre et un algorithme de construction d'un tel ensemble du chapitre suivant .

Exercice 74.— Soit $f = x^7y^2 + x^3y^2 - y + 1$ un polynôme de $\mathbb{K}[x,y]$ et soient $f_1 = xy^2 - x$ et $f_2 = x - y^3$.

1. Calculer le reste de la division de f par f_1, f_2 en utilisant l'ordre lexicographique et l'ordre lexicographique gradué.
2. Même question avec les diviseurs dans l'ordre f_2, f_1.

Exercice 75.— Soient $f = xy^2z^2 + xy - yz$, $f_1 = x - y^2$, $f_2 = y - z^3$, $f_3 = z^2 - 1$. En utilisant l'ordre lexicographique,

1. calculer le reste de la division de f par f_1, f_2, f_3,
2. calculer le reste de la division de f par f_3, f_2, f_1.

Exercice 76.— On étudie la division du polynôme $f = x^3 - x^2y - x^2z + x$ par les polynômes $f_1 = x^2y - z$ et $f_2 = xy - 1$.

1. En utilisant l'ordre lexicographique gradué, calculer le reste de la division de f par f_1, f_2, puis par f_2, f_1.
2. Les deux restes sont différents, à quel moment dans le processus de division cette différence apparaît ?
3. Posons $r = r_1 - r_2$. A-t-on $r \in \langle f_1, f_2 \rangle$? Si oui, donner une décomposition $r = u_1 + u_2 f_2$, sinon expliquer pourquoi ?
4. Calculer le reste de la division de r par f_1, f_2. Ce résultat était-il prévisible ?
5. Trouver un autre polynôme $g \in \langle f_1, f_2 \rangle$, tel que le reste de la division de g par f_1, f_2 est non nul.
6. L'algorithme de la division donne-t-il une solution pour le problème de l'appartenance à l'idéal $\langle f_1, f_2 \rangle$?

Exercice 77. — 1. En utilisant l'ordre lexicographique gradué, donner un élément g de l'idéal

$$\langle f_1, f_2\rangle = \langle 2xy^2 - x, 3x^2y - y - 1\rangle \subset \mathbb{R}[x,y]$$

dont le reste de la division par f_1, f_2 est non nul.

2. Même question avec l'idéal

$$\langle f_1, f_2, f_3\rangle = \langle x^4y^2 - z, x^3y^2 - z, x^3y^3 - 1, x^2y^4 - 2z\rangle \subset \mathbb{R}[x,y,z].$$

§ 6 Division et réduction

III.6.1. Exemple.— Soit $f_1 = x^3 - 2xy \in \mathbb{Q}[x,y]$ muni de l'ordre lexicographique associé à $y < x$.

On peut interpréter la division d'un polynôme de $\mathbb{Q}[x,y]$ par f_1 comme une *réduction* par f_1. La division de x^3 par f_1 est de reste $2xy$ et en terme de réduction on a

$$x^3 \xrightarrow{f_1} 2xy.$$

Pour calculer le reste de la division de $x^4 + 3x^3y$ par f_1, on remplace Dans l'expression $x^4 + 3x^3y$, les occurrences du terme x^3 par le terme $2xy$:

$$x^4 + 3x^3y \xrightarrow{f_1} x(2xy) + 3x^3y \xrightarrow{f_1} x(2xy) + 3(2xy)y = 2x^2y + 6xy^2.$$

Le polynôme $2x^2y + 6xy^2$ ne possède pas de terme divisible par x^3 et correspond ainsi au reste recherché.

III.6.2. Réduction.— Soient f, g, h trois polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, avec g non nul. On dit que f se *réduit en une étape* en h modulo g et on note

$$f \xrightarrow{g} h,$$

si $\mathrm{lt}(g)$ divise un terme non nul X de f et que

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

En particulier, un ordre monomial fixé, on a, pour tout polynôme f,

$$\mathrm{lt}(f) \xrightarrow{f} \mathrm{lt}(f) - f.$$

Par exemple, si $f = x^3y^2 - x^2y^3 + x$, avec l'ordre lexicographique gradué et $y < x$, on a

$$x^3y^2 \xrightarrow{f} x^2y^3 - x.$$

III.6.3. Exemple.— Considérons les polynômes $f = 6x^3y - x + y^4 + 4y^3 - 1$ et $g = 2xy + y^3$ de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique induit par $y < x$. On a $\mathrm{lt}(g) = 2xy$ qui divise $6x^3y$, d'où la réduction

$$f \xrightarrow{g} -3x^2y^3 - x + y^4 + 4y^3 - 1.$$

Si l'on considère l'ordre lexicographique gradué avec $y < x$, alors $\mathrm{lt}(g) = y^3$ et on a la réduction

$$f \xrightarrow{g} 6x^3y + y^4 - 8xy - x - 1.$$

Noter que, dans ce cas, la réduction ne porte ni sur le terme dominant de f qui vaut $6x^3y$, ni sur le terme de plus haut degré divisible par y^3. En général, on fera en premier la réduction sur le terme de plus haut degré divisible par $\mathrm{lt}(g) = y^3$, soit

$$f \xrightarrow{g} 6x^3y - 2xy^2 + 4y^3 - x - 1.$$

III.6.4. Définition.— Soient f, h des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ et $F = \{f_1, \ldots, f_s\}$ une famille de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$. On dit que f se *réduit* en h modulo F et on note

$$f \xrightarrow{F} h,$$

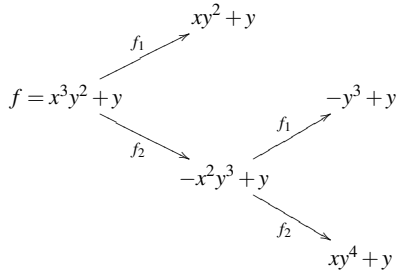
s'il existe une suite de réductions en une étape

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \ldots\ h_{i_{k-1}} \xrightarrow{f_{i_k}} h,$$

où $f_{i_j} \in F$ et $h_j \in \mathbb{K}[x_1, \ldots, x_n]$.

III.6.5. Exemple.— Soient $f_1 = x^2y - y$ et $f_2 = x^2 + xy$ des polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique associé à $y < x$. On a donc en particulier $x^2y \xrightarrow{f_1} y$ et $x^2 \xrightarrow{f_2} xy$.

Soit $F = \{f_1, f_2\}$ et $f = x^3y^2 + y$. Alors,



soit

$$x^3y^2 + y \xrightarrow{F} xy^2 + y,$$
$$x^3y^2 + y \xrightarrow{F} -y^3 + y \text{ et}$$
$$x^3y^2 + y \xrightarrow{F} xy^4 + y,$$

ce qui correspond aux 3 réductions sous *formes normales* de f modulo F.

III.6.6. Formes normales.— Un polynôme r est dit en *forme normale* par rapport à un ensemble $F = \{f_1, \ldots, f_s\}$ de polynômes non nuls, si $r = 0$ ou si aucun des termes de r n'est divisible par $\mathrm{lt}(f_i)$, pour $i \in [\![1, s]\!]$. On dit aussi que le polynôme r ne peut pas être réduit modulo F.

III.6.7. Remarque.— Dans le cas de l'algorithme de division présenté dans la partie précédente, on choisit un ordre pour les polynômes $f_1, \ldots, f_s$. Une réduction sous forme normale d'un

polynôme modulo F correspond également à une division par les polynômes de F, mais sans fixer d'ordre sur le choix des diviseurs successifs. Par exemple, la réduction $x^3y^2+y \xrightarrow{F} -y^3+y$ en III.6.5 ne correspond ni à la division par f_1, f_2 $\left(x^3y^2+y \xrightarrow{f_1,f_2} xy^2+y\right)$, ni à la division par f_2, f_1 $\left(x^3y^2+y \xrightarrow{f_2,f_1} xy^4+y\right)$.

Pour un polynôme non nul f de $\mathbb{K}[x_1,\ldots,x_n]$, si $f \xrightarrow{F} r$, où r est en forme normale relativement à F, alors il existe des quotients $u_1,\ldots,u_s$ dans $\mathbb{K}[x_1,\ldots,x_n]$ tels que

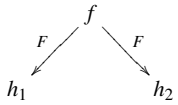
$$f = u_1f_1 + \ldots + u_sf_s + r$$

est une décomposition de f satisfaisant les propriétés du théorème III.11 : multideg$(u_if_i) \leq$ multideg(f) pour tout $u_i \neq 0$. En particulier, si $f \xrightarrow{F} 0$ alors $f \in \langle f_1,\ldots,f_s\rangle$.

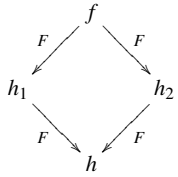
Réciproquement, par l'algorithme de division par $f_1,\ldots,f_s$, il existe toujours un polynôme r en forme normale par rapport à F tel que $f \xrightarrow{F} r$.

Exercice 78. — Reprendre l'exemple III.6.5 avec l'ordre lexicographique associé à $y > x$ et déterminer pour cet ordre les réductions de f modulo F sous forme normale.

III.6.8. Confluence.— Soit $F = \{f_1,\ldots,f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. On dit qu'une paire de réductions sur un même polynôme f modulo F

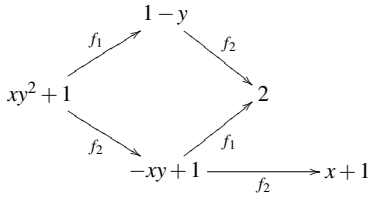


est *confluente* s'il existe un couple de réductions vers un même polynôme

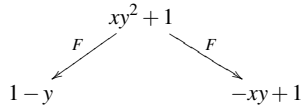


La relation de réduction $\xrightarrow{F}$ est dite *confluente* si toute paire l'est.
On verra que cette dernière propriété caractérise le fait d'être une *bonne* base.

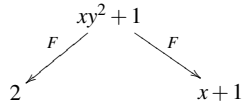
III.6.9. Exemple.— Reprenons le premier exemple III.5.1. Soient $f = xy^2+1$, $f_1 = xy+1$ et $f_2 = y+1$ trois polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique induit par $y < x$ et posons $F = \{f_1, f_2\}$. On a



La paire de réductions



est confluente, par contre la paire de réductions



ne l'est pas. La relation de réduction $\xrightarrow{F}$ n'est donc pas confluente.

Exercice 79. — Soit $F = \{f_1,\ldots,f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1,\ldots,x_n]$. Montrer que relation de réduction $\xrightarrow{F}$ est confluente si, et seulement si, tout polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$ a une unique réduction sous forme normale modulo F.

Exercice 80. — Soient $f_1 = x^2y - yz$, $f_2 = xy^2 - z^2$ et $f_3 = xz - y^2$ des polynômes de $\mathbb{R}[x,y,z]$, avec l'ordre lexicographique associé à $z < y < x$. Montrer que pour $F = \{f_1, f_2, f_3\}$, la relation de réduction $\xrightarrow{F}$ n'est pas confluente.