CHAPITRE I

Anneaux de polynômes

I.1. Expressions algébriques

On appelle *polynôme* une *expression algébrique* du type

$$f = 3x^5 - 4x^2 + x + \pi.$$

Il y a des *coefficients*, réels ou complexes, et la lettre x qui intervient avec divers exposants. On appelle *monôme* un polynôme avec un seul terme (par exemple $2x^3$).

On peut écrire un polynôme suivant les puissances décroissantes (comme ci-dessus) ou suivant les puissances croissantes, on écrirait ici

$$f = \pi + x - 4x^2 + 3x^5.$$

On pourrait aussi écrire

$$f = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

avec $a_0 = \pi, a_1 = 1, a_2 =_4, a_3 = a_4 = 0, a_5 = 3$. Par commodité il est admis de ne pas écrire les termes dont le coefficient est nul (ainsi, pour un monôme, on se contente d'écrire un seul terme). On peut aussi imaginer qu'il y a des termes nuls à la suite de ceux que l'on a écrit (ici, $a_6 = 0$), et même une infinité de termes (ici, $a_7 = a_8 = \ldots = 0$).

Écriture normalisée. On peut "normaliser" l'écriture des polynômes et définir f comme une suite (a_n) de coefficients (réels ou complexes), nulle à partir d'un certain rang (il existe N tel que, $\forall n > N, a_n = 0$). On écrit alors $f = (a_n)$.

Un polynôme est entièrement déterminé par la suite de ses coefficients. Dire que deux polynômes $f = (a_n)$ et $g = (b_n)$ sont égaux, c'est donc dire que $a_n = b_n$ pour tout n.

Alternativement on pourrait aussi écrire

$$f = a_0x^0 + a_1x^1 + \ldots + a_nx^n + \ldots$$

mais, contrairement à l'usage, la lettre x et les signes $+$ sont superflus.

Somme et produit. On peut aisément définir la somme et le produit de deux polynômes en écriture normalisée :

- *La somme* de $f = (a_n)$ et $g = (b_n)$ est le polynôme $f + g$ de coefficients s_n définis par

$$s_n = a_n + b_n.$$

- *Le produit* de $f = (a_n)$ et $g = (b_n)$ est le polynôme fg de coefficients p_n définis par

$$p_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_0 b_n = \sum_{i+j=n} a_i b_j.$$

On peut vérifier que somme et produit sont *commutatifs* :

$$f + g = g + f \quad \text{et} \quad fg = gf,$$

qu'ils sont *associatifs* :

$$(f + g) + h = f = (g + h) \quad \text{et} \quad (fg)h = f(gh),$$

et enfin que le produit est *distributif* par rapport à la somme :

$$f(g + h) = fg + fh.$$

Il y a un polynôme nul, noté 0, dont tous les coefficients sont nuls, tel que

$$0 + f = f + 0 = f, \quad \text{et} \quad 0f = f0 = 0.$$

Il y a un polynôme unité, noté 1, défini par la suite de coefficients $(1, 0, \ldots, 0, \ldots)$, tel que

$$1f = f1 = f.$$

Enfin on note $-f$ le polynôme obtenu en changeant les signes de tous les coefficients de f de sorte qu'on a

$$f + (-f) = 0.$$

On retrouve ainsi toutes les règles usuelles de calcul sur les nombres et en particulier les identités remarquables, comme la fameuse égalité

$$(f + g)^2 = f^2 + 2fg + g^2.$$

On dit que les polynômes forment un *anneau*. On note $\mathbb{R}[X]$ l'anneau des polynômes réels (à coefficients réels) et $\mathbb{C}[X]$ l'anneau des polynômes complexes (à coefficients complexes).

Remarque I.1.1. Il est facile de vérifier que la somme des monômes $a_0, a_1 x, \ldots, a_n x^n$ n'est autre que le polynôme $a_0 + a_1 x + \ldots + a_n x^n$, il suffit en effet de faire la somme terme à terme des suites correspondantes, soit :

$$\begin{array}{cccccc} & (a_0, & 0, & 0, & \ldots) \\ + & (0, & a_1, & 0, & \ldots) \\ + & (0, & 0, & a_2, & \ldots) \\ + & \ldots & \ldots & \ldots & \ldots \\ \hline = & (a_0, & a_1, & a_2, & \ldots) \end{array}$$

Ceci justifie l'emploi du signe + dans la notation usuelle des polynômes.

I.2. Degré

DÉFINITION I.2.1. Soit $f = (a_n)$ un polynôme non nul. On appelle *degré de* f, on note $\deg(f)$, le plus grand entier n tel que $a_n \neq 0$.

On note que le polynôme nul n'a pas de degré (il n'y a pas d'entier n pour lequel $a_n \neq 0$). On conviendra de poser $\deg(0) = -\infty$.

PROPOSITION I.2.2. *Soient f et g deux polynômes. On a*

- $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$,
- $\deg(fg) = \deg(f) + \deg(g)$.

On observe qu'on peut étendre ce résultat et admettre des polynômes nuls si on convient que, pour tout entier n, on a

$-\infty \leq n$, $\quad -\infty \leq -\infty$,
$-\infty + n = -\infty$, $\quad -\infty + (-\infty) = -\infty$.

Quelques précisions de vocabulaire :

DÉFINITIONS I.2.3.

- Le coefficient a_0 de f s'appelle le *terme constant* de f.
- Si f est non nul, son coefficient de plus haut degré s'appelle le *coefficient directeur* de f.
- Un polynôme non nul de coefficient directeur égal à 1 s'appelle un *polynôme unitaire*.
- Un polynôme dont tous les termes non constants sont nuls (donc tel que $a_n = 0$ pour $n \geq 1$) s'appelle un *polynôme constant*, on dit aussi que c'est *une constante*

Les constantes non nulles sont donc les polynômes de degré 0. Le polynôme nul (encore appelé *constante nulle*) est le seul polynôme de degré $-\infty$.

LEMME I.2.4. *Le produit de deux polynômes non nuls est non nul.*

Notamment le degré du produit [proposition I.2.2] est supérieur ou égal à celui de chacun des facteurs. On tire la *règle de simplification* :

PROPOSITION I.2.5. *Si on a l'égalité $fh = gh$ avec $h \neq 0$, alors $f = g$.*

Démonstration. Le produit $(f-g)h$ est nul, donc l'un des facteurs est nul. Ce n'est pas le facteur h, c'est donc le facteur $f - g$. □

I.3. Division euclidienne

THÉORÈME I.3.1. *Soient f et g deux polynômes réels (resp. complexes), avec $g \neq 0$. Alors il existe un unique polynôme réel (resp. complexe) q et un unique polynôme réel (resp. complexe) r tels que*

$$f = gq + r \quad \text{et} \quad \deg(r) < \deg(g).$$

Notons que q et r peuvent être nuls ; si $r = 0$, l'inégalité $\deg(r) < \deg(g)$ est alors satisfaite grâce à la convention $\deg(0) = -\infty$. Avant de montrer ce résultat, fixons le vocabulaire.

DÉFINITION I.3.2. Lorsqu'on écrit $f = gq + r$, on dit qu'on effectue la division *euclidienne* ou *suivant les puissances décroissantes* de f par g. On dit que f est le *dividende*, g le *diviseur*, q le *quotient* et r le *reste* de cette division.

Démonstration. Si $\deg(f) < \deg(g)$, il suffit de prendre $q = 0$ et $r = f$. On a bien alors $f = gq + r = 0 + f$ avec $\deg(r) = \deg(f) < \deg(g)$. Sinon on procède par un algorithme qui permet d'abaisser le degré de f :

Première étape. On suppose qu'on a $\deg(f) = n \geq \deg(g) = m$ (de "vrais" degré puisque g est non nul). Il existe alors un monôme q_1 tel que gq_1 et f sont de même degré et de même coefficient directeur. En effet, si

$$f = a_n x^n + a_{n-1}x^{n-1} + \dots \quad \text{et} \quad g = b_m x^m + b_{m-1}x^{m-1} + \dots$$

il suffit de prendre $q_1 = (a_n/b_m)x^{n-m}$ (en particulier, $q_1 = a_n/b_m$ si $n = m$). On peut donc écrire

$$f = gq_1 + r_1 \quad \text{avec} \quad \deg(r_1) < \deg(f).$$

Si $\deg(r_1) < \deg(g)$, on a terminé. Sinon, on recommence.

Étapes suivantes. On écrit tour à tour

$$\begin{aligned} f &= gq_1 + r_1 \quad \text{avec} \quad \deg(r_1) < \deg(f), \\ r_1 &= gq_2 + r_2 \quad \text{avec} \quad \deg(r_2) < \deg(r_1). \\ r_2 &= gq_3 + r_3 \quad \text{avec} \quad \deg(r_2) < \deg(r_3) \end{aligned}$$

Ainsi de suite. On s'arrête lorsqu'on obtient un reste r_n (éventuellement nul) tel que $\deg(r_n) < \deg(g)$. Comme la suite des degrés des restes est strictement décroissante, ceci ne manque pas d'arriver! Si, par exemple, on s'arrête à r_3, on a donc

$$f = gq_1 + r_1 = gq_1 + gq_2 + r_2 = gq_1 + gq_2 + gq_3 + r_3 = g(q_1 + q_2 + q_3) + r_3.$$

Le quotient q est alors la somme des quotient partiels, soit $q = q_1 + q_2 + q_3$ et le reste r le dernier reste, soit $r = r_3$. Noter que les quotients partiels sont des monômes et que q se trouve ainsi naturellement écrit suivant les puissances décroissantes!

Unicité. Supposons données deux solutions

$$f = gq + r \text{ avec } \deg(r) < \deg(g) \quad \text{et} \quad f = gq^\star + r^\star \text{ avec } \deg(r^\star) < \deg(g).$$

On a alors $f = gq + r = gq^\star + r^\star$ et donc

$$g(q - q^\star) = r^\star - r.$$

Le degré du premier terme est

$$\deg(g(q - q^\star)) = \deg(g) + \deg(q - q^\star)$$

et pour le second terme on a

$$\deg(r^\star - r) \leq \max\{\deg(r^\star), \deg(r)\} < \deg(g).$$

On aurait une contradiction, sauf si les deux termes sont nuls (donc de degré égal à $-\infty$), soit $q = q^\star \quad \text{et} \quad r = r^\star$. □

I.4. Divisibilité

DÉFINITION I.4.1. Si $f = qg$ on dit que g *divise* f ou que g est un *diviseur* de f ou encore que f est un *multiple* de g. On note (g) l'ensemble des polynômes multiples de g.

Pour $g \neq 0$, dire que f est multiple de g signifie donc que le reste de la division de f par g est nul (la division *tombe juste*).

Faisons quelques remarques sur les ensembles de multiples :

- Parmi les multiples de g il y a toujours g lui-même (on peut écrire $g = 1g$). Autrement dit $g \in (g)$.
- Pour tout $g, 0$ est multiple de g (on peut écrire $0 = 0g$). Autrement dit $0 \in (g)$.
- Le seul multiple de 0 est 0 lui-même (pour tout $q, q0 = 0$). Autrement dit $(0) = \{0\}$.
- Tout polynôme f est multiple de 1 ($f = f1$). Autrement dit (1) est l'ensemble de tous les polynômes ($\mathbb{R}[X]$ si on considère les polynômes réels, $\mathbb{C}[X]$ si on considère les polynômes complexes).
- Plus généralement, si a est une constante non nulle, alors tout f est multiple de a ($f = (a^{-1}f)a$).

Combinaisons. On étend la notion de multiple comme suit.

DÉFINITION I.4.2. Soit $\{g_1, g_2, \ldots, g_n\}$ une famille finie de polynômes. On dit qu'un polynôme f est une *combinaison* de cette famille si on peut écrire

$$f = q_1 g_1 + q_2 g_2 + \ldots + q_n g_n.$$

On note $(g_1, g_2, \ldots, g_n)$ l'ensemble de ces combinaisons.

L'ensemble (g) des multiples de g est donc l'ensemble des combinaisons de la famille formée du seul polynôme g (ceci justifie l'emploi de la même notation).

PROPOSITION I.4.3. *Soit $\{g_1, g_2, \ldots, g_n\}$ une famille de polynômes. Alors*

- *La somme de deux (ou plusieurs) combinaisons de cette famille est encore une combinaison.*
- *Tout multiple d'une combinaison est encore une combinaison.*

Démonstration. Considérons deux combinaisons

$$f = q_1 g_1 + q_2 g_2 + \ldots + q_n g_n \quad \text{et} \quad f^\star = q_1^\star g_1 + q_2^\star g_2 + \ldots + q_n^\star g_n.$$

— Faisant la somme, on obtient la combinaison

$$f + f^\star = (q_1 + q_1^\star) g_1 + (q_2 + q_2^\star) g_2 + \ldots + (q_n + q_n^\star) g_n.$$

— Le multiple qf de f est la combinaison

$$qf = (qq_1) g_1 + (qq_2) g_2 + \ldots + (qq_n) g_n.$$

□

COROLLAIRE I.4.4. *Soit $\{g_1, g_2, \ldots, g_n\}$ une famille de polynômes. Alors une combinaison de deux (ou plusieurs) combinaisons de cette famille est encore une combinaison (de cette famille).*

Polynômes associés. On discute ici de la possibilité pour f et g de se diviser l'un l'autre ou encore d'être multiple l'un de l'autre. Comme un multiple d'un multiple est encore un multiple, cela veut dire que f et g ont le même ensemble de multiples.

DÉFINITION I.4.5. On dit que deux polynômes f et g sont *associés* s'ils se divisent l'un l'autre, soit $(f) = (g)$.

Si g divise f, soit $f = qg$, alors $\deg(g) \leq \deg(f)$ (sauf si f est nul). Si f et g se divisent l'un l'autre, ils ont donc même degré et le facteur q est une constante (en fait, si l'un est nul, alors l'autre aussi, et n'importe quel facteur convient) :

PROPOSITION I.4.6. *Deux polynômes f et g sont associés si et seulement si il existe une constante $a \neq 0$ telle que $f = ag$ et $g = a^{-1}f$.*

I.5. Pgcd

Une constante non nulle divise tout polynôme. Deux polynômes f et g admettent donc toujours des diviseurs communs. Si f et g sont non nuls, les degrés de ces diviseurs sont majorés (par les degrés de f et de g).

DÉFINITION I.5.1. Soient f et g deux polynômes (non nuls). On dit que d est un *plus grand commun diviseur* (ou *Pgcd*) de f et de g, on note $d = \mathrm{Pgcd}(f, g)$, si d est de degré maximal parmi les diviseurs de f et de g.

Algorithme d'Euclide. Soient f et g deux polynômes (non nuls). On pose $r_0 = g$. On divise f par g (donc par r_0) écrivant
$f = q_1 r_0 + r_1$ avec $\deg(r_1) < \deg(r_0)$.
Si r_1 n'est pas nul, on divise ensuite r_0 par r_1,
$r_0 = q_2 r_1 + r_2$ avec $\deg(r_2) < \deg(r_1)$.
Si r_2 n'est pas nul, on divise ensuite r_1 par r_2,
$r_1 = q_3 r_2 + r_3$ avec $\deg(r_3) < \deg(r_2)$,
ainsi de suite, tant que le reste n'est pas nul (et que la division est possible). Mais comme les restes sont de degrés strictement décroissants, il advient nécessairement qu'un reste soit nul.

PROPOSITION I.5.2. *Appliquant l'algorithme d'Euclide, le dernier reste non nul est un diviseur de f et de g multiple de tous les autres diviseurs communs, donc un Pgcd de f et de g.*

Avant de faire la démonstration faisons quelques remarques.

- Parmi plusieurs polynômes, si l'un est de degré maximal, il n'est pas nécessairement multiple de tous les autres. Il est donc remarquable qu'un Pgcd soit multiple de tous les autres diviseurs communs.

- Si le premier reste est nul, alors g divise f et $g = r_0$ est un Pgcd de f et de g.
- On peut échanger les rôles de f et de g. On a cependant intérêt à diviser le "plus grand" (de plus grand degré) par le "plus petit".

Démonstration. Sans perte de généralité, supposons que r_3 soit le dernier reste non nul.
— On montre que f et g sont multiple de r_3 ("en remontant") : d'abord, le reste de la division de r_2 par r_3 est nul, donc r_2 est multiple de r_3. Puis
$r_1 = q_3 r_2 + r_3$,
donc r_1 (combinaison des multiples r_2 et r_3) est multiple de r_3,
$r_0 = q_2 r_1 + r_2$,
donc $g = r_0$ (combinaison des multiples r_1 et r_2) est multiple de r_3,
$f = q_1 r_0 + r_1$,
donc f (combinaison des multiples r_0 et r_1) est multiple de r_3.

— Si d est un autre diviseur commun, on montre ("en descendant") que r_3 est multiple de d : $r_1 = f - q_1 r_0$,
donc r_1 (combinaison des multiples f et r_0) est multiple de d,
$r_2 = r_0 - q_2 r_1$,
donc r_2 (combinaison des multiples r_0 et r_1) est multiple de d,
$r_3 = r_1 - q_3 r_2$,
donc r_3 (combinaison des multiples r_1 et r_2) est multiple de d. □

Corollaire I.5.3. *Tous les Pgcd de f et de g sont associés entre eux.*

Démonstration. Si d et $d^\star$ sont associés, ils ont même degré et même ensemble de multiples. Si d est de degré maximal parmi les diviseurs communs de f et de g, il en est alors de même pour $d^\star$. Réciproquement, si d est le Pgcd fourni par l'algorithme d'Euclide et $d^\star$ un autre Pgcd, alors d est un multiple de $d^\star$ et le facteur multiplicatif est une constante puisqu'ils ont même degré. Ainsi, tous les Pgcd sont associés à d donc aussi entre eux. □

Relation de Bézout.

Proposition I.5.4. *Un polynôme d est un Pgcd de f et de g si et seulement il divise f et g et est combinaison de f et de g : $d = pf + qg$.*

Démonstration. Le Pgcd de l'algorithme d'Euclide [proposition I.5.2] est une combinaison de f et de g. En effet
$r_1 = f - q_1 r_0$,
est combinaison de f et de $r_0 = g$,
$r_2 = r_0 - q_2 r_1$,
est combinaison de r_0 et de r_1. Or une combinaison de combinaisons est une combinaison [corollaire I.4.4], donc r_2 est combinaison de f et de g.
$r_3 = r_1 - q_3 r_2$,
est combinaison de r_1 et de r_2, donc, pour la même raison, combinaison de

f et de g. Un autre Pgcd est associé à ce dernier, donc multiple par une constante (non nulle) et donc encore combinaison de f et de g.

Réciproquement, si $d = pf + qg$ est un diviseur commun, alors c'est un Pgcd. En effet, si $d^\star$ est un autre diviseur commun, alors d (combinaison de f et g, multiples de $d^\star$) est un multiple de $d^\star$. □

Polynômes étrangers.

Définition I.5.5. On dit que deux polynômes (non nuls) f et g sont *étrangers* s'ils n'admettent que les constantes (non nulles) pour diviseurs communs.

Autrement dit, les polynôme de degré 0 sont de degré maximal parmi les diviseurs communs et, en particulier, 1 est un Pgcd de f et de g. On a alors une forme particulière de la relation de Bézout :

Corollaire I.5.6. *Les polynômes f et g sont étrangers si et seulement si il existe p et q tels que $pf + qg = 1$.*

Démonstration. Cela résulte de la proposition I.5.4. Pour vérifier que 1 est un Pgcd, il suffit en effet de vérifier que c'est une combinaison de f et de g puisque c'est toujours un diviseur commun. □

I.6. Ppcm

Deux polynômes f et g admettent toujours des multiples communs, par exemple 0 ou le produit fg. Si on s'intéresse aux multiples non nuls, leur degré est supérieur à celui de f et de g.

Définition I.6.1. Soient f et g deux polynômes (non nuls). On dit que m est un *plus petit commun multiple* (ou *Ppcm*) de f et de g, on note $m = \mathrm{Ppcm}(f, g)$, si m est de degré minimal parmi les multiples non nuls de f et de g.

Proposition I.6.2. *Un Ppcm divise tous les autres communs multiples de f et de g.*

Démonstration. Soit m un Ppcm et $m^\star$ un autre commun multiple. Effectuant la division euclidienne de $m^\star$ par m, soit $m^\star = mq + r$, on a $r = m^\star - mq$. Ainsi le reste r est une combinaison de multiples de f et de g donc lui aussi un commun multiple. Il faut qu'il soit nul, donc que m divise $m^\star$, pour respecter le caractère minimal de m. □

Corollaire I.6.3. *Tous les Ppcm de f et de g sont associés entre eux.*

Relation entre Pgcd et Ppcm. Si m est un Ppcm, il divise le produit fg qui est un autre commun multiple, on peut donc écrire $fg = dm$. Étudiant cette relation, on va montrer comment calculer un Ppcm à l'aide d'un Pgcd.

PROPOSITION I.6.4. *Soient f, g, m, d des polynômes (non nuls) tels que $fg = md$. Alors*

(1) *d divise f si et seulement si m est un multiple de g.*
(2) *d divise g si et seulement si m est un multiple de f.*
(3) *d est un diviseur commun de f et de g si et seulement si m est un multiple commun de f et de g.*
(4) *$d = \mathrm{Pgcd}(f, g)$ si et seulement si $m = \mathrm{Ppcm}(f, g)$.*

Démonstration. 1) Si d divise f on peut écrire $f = pd$, donc (remplaçant f par pd dans la relation $fg = dm$) on a $pdg = dm$. On peut simplifier par d qui est non nul [proposition I.2.5]. Donc $m = pg$ est multiple de g. Inversement, si $m = pg$, alors $fg = dpg$ et $f = dp$.
2) Il suffit d'échanger les rôles de f et de g.
3) Si d divise f **et** g, il en résulte que m est multiple de g **et** de f.
4) La somme $\deg(d) + \deg(m)$ est constante (égale à $\deg(f) + \deg(g)$). Ainsi d est de degré maximal si et seulement si m est de degré minimal. □

On sait calculer un Pgcd (par l'algorithme d'Euclide). Si d est un Pgcd, c'est un diviseur commun et on a alors

$$f = pd \quad \text{et} \quad g = qd.$$

Avec ces notations, on obtient une expression pour un Ppcm :

COROLLAIRE I.6.5. *Le polynôme $m = dpq$ est un Ppcm de f et de g.*

Démonstration. On a en effet $md = dpqd = (pd)(qd) = fg$. □