Chapitre 5

Polynômes

5.1 L'ensemble des polynômes à une indéterminée

5.1.1 Définitions

Définition 5.1.1 *On appelle* **polynôme à une indéterminée et coefficients dans** $\mathbb{K}$ *ou plus simplement polynôme, toute expression algébrique de la forme*

$$a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0,$$

avec $a_i \in \mathbb{K}$ *pour tout* $i \in \{0, \cdots, p\}$.

- *Les scalaires* a_i *sont appelés* **coefficients** *du polynôme.*
- *S'il existe, le plus grand indice* i *tel que* $a_i \neq 0$ *s'appelle* **degré de** P *et est noté* $\deg P$.
- *Si tous les coefficients* a_i *sont nuls,* P *est appelé* **polynôme nul** *et est noté* 0. *Par convention,* $\deg 0 = -\infty$.
- *Un polynôme de la forme* $P = a_0$ *avec* $a_0 \in \mathbb{K}$ *est appelé* **polynôme constant**. *Si* $a_0 \neq 0$, *son degré est* 0.

L'ensemble des polynôme à une indéterminée et coefficients dans $\mathbb{K}$ *est noté* $\mathbb{K}[X]$.

Exemples :

- $X^3 - \pi X + 3/2$ est un polynôme de degré 3.
- Si $n \in \mathbb{N}^*$, $X^n - 1$ est un polynôme de degré n
- 1 est un polynôme de degré 0.

Remarque 5.1.2 *Nous serons amenés par la suite à additionner des degrés de polynômes. Comme l'application* deg *est à valeurs dans* $\mathbb{N} \cup \{-\infty\}$, *il faut étendre la définition de l'addition. On adopte la convention suivante pour* $n \in \mathbb{N} \cup \{-\infty\}$ *:*

$$-\infty + n = -\infty.$$

Définition 5.1.3 *Les polynômes ne comportant qu'un seul terme non nul (i.e du type* $P = a_p X^p$*) sont appelés* **monômes**.

Remarque : Tout polynôme est donc une somme finie de monômes.

Définition 5.1.4 *Soit* $P = a_p X^p + \cdots + a_0$ *avec* $a_p \neq 0$ *un polynôme. On appelle* **terme dominant** *de* P *le monôme* $a_p X^p$. *Si le coefficient* a_p *du terme dominant est* 1, *on dit que* P *est un* **polynôme unitaire**.

Remarque 5.1.5 *On adopte la convention que l'on ne change pas un polynôme* P *en lui ajoutant un ou plusieurs monômes à coefficients nuls. Par exemple, on ne fera pas la distinction entre*

$$X^4 - X + 1 \quad et \quad 0X^5 + X^4 + 0X^2 - X + 1.$$

5.1.2 Opérations sur $\mathbb{K}[X]$

Nous allons munir $\mathbb{K}[X]$ de deux lois internes "+" et "$*$", et d'une loi externe "$\cdot$".

a) Addition de deux polynômes :

Définition 5.1.6 *Soit $P = a_nX^n + \cdots + a_0$ et $Q = b_nX^n + \cdots + b_0$ avec $n \in \mathbb{N}$. On définit alors le polynôme $P + Q$ par*

$$P + Q \overset{\text{déf}}{=} (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$

Remarque : Dans la définition ci-dessus, il n'est pas restrictif de faire commencer les expressions des polynômes P et Q par un monôme de même degré n (voir la remarque 5.1.5 ci-dessus)

Proposition 5.1.7 *Soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P + Q) \leq \max(\deg P, \deg Q).$$

De plus, si $\deg P \neq \deg Q$ alors $\deg(P + Q) = \max(\deg P, \deg Q)$.

Preuve : Notons $p = \deg P$ et $q = \deg Q$.
- Si $p > q$, le coefficient du terme dominant de $P + Q$ est a_p donc $\deg(P + Q) = \deg P$.
- Si $p < q$, le coefficient du terme dominant de $P + Q$ est b_q donc $\deg(P + Q) = \deg Q$.
- Si $p = q$, le monôme de plus haut degré dans l'expression de $P + Q$ est $(a_p + b_p)X^p$. Donc $\deg(P + Q) \leq p$. Si $b_p = -a_p$, ce monôme est nul et l'on a donc $\deg(P + Q) < p$.

■

b) Multiplication de deux polynômes :

Considérons deux monômes $P = a_pX^p$ et $Q = b_qX^q$. Si l'on interprète ces deux monômes comme des fonctions de la variable réelle ou complexe X, il est naturel de définir le produit de P par Q comme étant le monôme $P * Q \overset{\text{déf}}{=} a_pb_qX^{p+q}$.

Plus généralement, on définit le produit de deux polynômes de la façon suivante :

Définition 5.1.8 *Étant donnés deux polynômes $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$, on définit le polynôme $P * Q$ par $P * Q = c_rX^r + \cdots + c_0$ avec $r = p + q$ et, pour $k \in \{0, \cdots, r\}$,*

$$c_k = \sum_{i+j=k} a_ib_j = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{j=0}^{k} a_{k-j}b_j.$$

Remarque : Si P ou Q est nul, on a donc $P * Q = 0$.

La proposition suivante est une conséquence immédiate de la définition de "$*$" :

Proposition 5.1.9 *Soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P * Q) = \deg P + \deg Q.$$

c) Multiplication d'un polynôme par un scalaire :

Définition 5.1.10 *Soit $P = a_pX^p + \cdots + a_0$ un polynôme de $\mathbb{K}[X]$, et $\lambda \in \mathbb{K}$. On définit alors le polynôme $\lambda \cdot P$ par*

$$\lambda \cdot P \overset{\text{déf}}{=} \sum_{i=0}^{p} \lambda a_iX^i.$$

Le lecteur prouvera sans difficulté le résultat suivant :

Proposition 5.1.11 *Soit P un polynôme et λ un scalaire <u>non nul</u>. Alors $\deg(\lambda \cdot P) = \deg P$.*

5.1.3 Propriétés algébriques de $\mathbb{K}[X]$

Proposition 5.1.12 *$(\mathbb{K}[X], +, *)$ est un anneau commutatif.*

Preuve : Montrons déjà que $(\mathbb{K}[X], +)$ est un groupe commutatif.
- Le polynôme nul est clairement l'élément neutre pour l'addition.
- Si $P = a_pX^p + \cdots + a_0$, le polynôme $-P \stackrel{\text{déf}}{=} -a_pX^p + \cdots - a_1X - a_0$ vérifie $P + (-P) = 0$.
- L'associativité et la commutativité résultent de celles de l'addition sur $\mathbb{K}$.

Reste à étudier les propriétés de la multiplication "$*$".
- De la définition de la multiplication sur $\mathbb{K}[X]$, on déduit facilement que le polynôme $P = 1$ est l'élément neutre pour "$*$".
- Commutativité : considérons $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$. Notons $r = p + q$, $P * Q = c_rX^r + \cdots + c_0$ et $Q * P = d_rX^r + \cdots + d_0$. Alors on a

$$\forall k \in \{0, \cdots, r\},\ c_k = \sum_{i+j=k} a_ib_j = \sum_{j+i=k} b_ja_i = d_k$$

  Donc $P * Q = Q * P$.
- Associativité : Soit $P = a_pX^p + \cdots + a_0$, $Q = b_qX^q + \cdots + b_0$ et $R = c_rX^r + \cdots + c_0$. Soit $U \stackrel{\text{déf}}{=} (P * Q) * R$ et $V \stackrel{\text{déf}}{=} P * (Q * R)$. Notons d_ℓ les coefficients de U, et e_m ceux de V. Enfin, notons f_s les coefficients de $P * Q$, et g_t ceux de $Q * R$. Alors on a

$$\begin{array}{rcl} d_\ell &=& \sum_{s+k=\ell} f_sc_k \\ &=& \sum_{s+k=\ell} \left(\sum_{i+j=s} a_ib_j\right) c_k \\ &=& \sum_{i+j+k=\ell} a_ib_jc_k. \end{array} \quad \left| \quad \begin{array}{rcl} e_\ell &=& \sum_{i+t=\ell} a_ig_t \\ &=& \sum_{i+t=\ell} a_i \left(\sum_{j+k=t} b_jc_k\right) \\ &=& \sum_{i+j+k=\ell} a_ib_jc_k. \end{array} \right.$$

  Donc $d_\ell = e_\ell$, d'où $U = V$.
- Distributivité de la multiplication sur l'addition : Définissons P, Q, R comme ci-dessus et posons $U \stackrel{\text{déf}}{=} (P + Q) * R$ et $V \stackrel{\text{déf}}{=} P * R + Q * R$. Notons encore d_ℓ les coefficients de U, et e_m ceux de V. Alors on a

$$d_\ell = \sum_{i+j=\ell} (a_i + b_i)c_j = \sum_{i+j=\ell} (a_ic_j + b_ic_j) = \sum_{i+j=\ell} a_ic_j + \sum_{i+j=\ell} b_ic_j = e_\ell.$$

  Donc $U = V$.

■

À titre d'exercice, le lecteur pourra établir la

Proposition 5.1.13 *L'anneau $(\mathbb{K}[X], +, *)$ vérifie les propriétés supplémentaires suivantes pour tout $(\lambda, \mu) \in \mathbb{K}2$ et $(P, Q) \in \mathbb{K}[X]^2$:*

1. $(\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P$,
2. $\lambda \cdot (P + Q) = \lambda \cdot P + \lambda \cdot Q$,
3. $\lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$,
4. $1 \cdot P = P$,
5. $\lambda \cdot (P * Q) = (\lambda \cdot P) * Q = P * (\lambda \cdot Q)$.

On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une **algèbre**.

Ainsi, multiplier un polynôme P par un scalaire λ est équivalent à le multiplier par le polynôme constant $\lambda \cdot 1$. On peut donc sans danger noter la multiplication interne $*$ et la multiplication externe $\cdot$ par le même symbole.

Enfin, $(\mathbb{K}[X], +, *, \cdot)$ jouit de la propriété suivante qui est primordiale :

Proposition 5.1.14 *Soit (P, Q) un couple de polynômes tel que $P * Q = 0$. Alors $P = 0$ ou $Q = 0$. On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une* **algèbre intègre**.

Preuve : Soit donc (P, Q) tel que $P * Q = 0$. Alors on a $\deg P + \deg Q = \deg(P * Q) = -\infty$. Donc $\deg P$ ou $\deg Q$ vaut $-\infty$, ce qui est exactement la propriété demandée. ■

Notations : Dorénavant, on omettra les symboles "$*$" et "$\cdot$". Ainsi PQ désignera $P * Q$, et λP désignera $\lambda \cdot P$.

5.2 Division des polynômes

Définition 5.2.1 *On dit que le polynôme A est* **divisible** *par le polynôme B s'il existe un polynôme Q tel que $A = BQ$. Dans ce cas, on note $B \mid A$ (voir remarque [1]) et l'on dit que A est* **multiple** *de B (ou que B est* **diviseur** *de A). Le polynôme Q est parfois noté $\frac{A}{B}$ ou A/B.*

Remarques :

1. Le polynôme nul est divisible par tous les polynômes. En revanche seul le polynôme nul est divisible par le polynôme nul.
2. Dans le cas où A et B sont tous les deux non nuls, $B|A$ entraîne $\deg B \leq \deg A$.

Proposition 5.2.2 *Soit A et B, deux polynômes non nuls. Si $A \mid B$ et $B \mid A$ alors A et B sont proportionnels, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$. On dit que A et B sont* **associés**.

Preuve : D'après la remarque ci-dessus, on a à la fois $\deg A \leq \deg B$ et $\deg B \leq \deg A$. Donc A et B sont de même degré. Comme $B \mid A$, on en déduit que $A = BQ$ avec $\deg Q = 0$. Autrement dit Q est un polynôme constant (et non nul car A n'est pas nul). ■

Remarque 5.2.3 *Deux polynômes unitaires associés sont forcément égaux.*

Exercice : Prouver la remarque ci-dessus.

Proposition 5.2.4 *Soit B un polynôme non nul, et A un multiple de B de même degré que B. Alors A et B sont associés.*

Preuve : Elle reprend la dernière partie de celle de la proposition 5.2.2. ■

Théorème 5.2.5 (Division euclidienne) *Soit A et B deux polynômes avec B non nul. Alors il existe un unique couple (Q, R) de polynômes tel que*

$$A = BQ + R \quad et \quad \deg R < \deg B.$$

Le polynôme Q est appelé **quotient** *de la division de A par B, R est le* **reste**, *B, le diviseur, et A, le* **dividende**.

Preuve : On va d'abord prouver l'unicité du couple (Q, R), puis son existence.

Unicité : Supposons que $A = BQ + R = BQ' + R'$ avec $\deg R < \deg B$ et $\deg R' < \deg B$. Alors on a $R - R' = B(Q' - Q)$. Donc $\deg(R - R') = \deg B + \deg(Q' - Q)$.

Si $Q \neq Q'$, alors on en déduit que $\deg(R - R') \geq \deg B$.

Donc d'après la proposition 5.1.7, $\max(\deg R, \deg R') \geq \deg B$, ce qui contredit la définition de R ou de R'. Donc $Q = Q'$, puis $R = R'$.

[1] Lire "B divise A" et non pas le contraire !

Existence : Fixons un polynôme $B = b_m X^m + \cdots + b_0$ de degré $m \geq 1$ (le cas B constant non nul étant évident). L'existence du couple (Q, R) vérifiant les propriétés voulues se montre par récurrence sur le degré de A. Pour $n \in \mathbb{N}$, on note $(\mathcal{P}_n)$ l'hypothèse de récurrence suivante :

$$(\mathcal{P}_n)\ \ (\forall A \in \mathbb{K}[X], \deg A \leq n) \Rightarrow (\exists Q \in \mathbb{K}[X], \exists R \in \mathbb{K}[X] \mid A = BQ + R \text{ et } \deg R < \deg B)\,.$$

Il est clair que $(\mathcal{P}_{m-1})$ est vraie. En effet, il suffit de choisir $Q = 0$ et $R = A$.
Soit maintenant $n \geq m$. Supposons $(\mathcal{P}_{n-1})$ vraie et démontrons $(\mathcal{P}_n)$. Le polynôme A est de la forme $A = a_n X^n + \cdots + a_0$ avec $a_n \neq 0$. Comme $n \geq m$ et $b_m \neq 0$, l'expression

$$A' \overset{\text{déf}}{=} A - \frac{a_n}{b_m} X^{n-m} B$$

est bien un polynôme, et son degré est au plus $n-1$. D'après $(\mathcal{P}_{n-1})$, il existe donc deux polynômes Q' et R' tels que $A' = Q'B + R'$ et $\deg R' < \deg B$. On en déduit que

$$A = \underbrace{\left(\frac{a_n}{b_m} X^{n-m} + Q'\right)}_{\overset{\text{déf}}{=} Q} B \ + \ \underbrace{R'}_{\overset{\text{déf}}{=} R}\ ,$$

ce qui démontre $(\mathcal{P}_n)$. ∎

La démonstration ci-dessus suggère un procédé de construction itératif permettant de calculer Q et R. En effet, au cours de la récurrence, on a vu comment ramener la division d'un polynôme de degré n à celle d'un polynôme de degré moins élevé (au plus $n-1$). En pratique, on peut donc calculer le couple (Q, R) en "posant" la division comme dans $\mathbb{N}$, les puissances de X jouant le rôle des puissances de 10.

Illustrons nos propos par un exemple.

Exemple : Division de $4X^5 - 7X^3 + 8X^2 - 1$ par $X^3 - 4X^2 + 2X + 3$.

$$\begin{array}{rrrrrrr|l}
4X^5 + & 0X^4 - & 7X3 + & 8X^2 + & 0X - & 1 & & X^3 - 4X^2 + 2X + 3 \\
\cline{8-8}
 & 16X^4 - & 15X^3 - & 4X^2 + & 0X - & 1 & & \\
 & & 49X^3 - & 36X^2 - & 48X - & 1 & & 4X^2 + 16X + 49 = Q \\
 & & R = & 160X^2 - & 146X - & 148 & &
\end{array}$$

Donc $4X^5 - 7X^3 + 8X^2 - 1 = (X^3 - 4X^2 + 2X + 3)(4X^2 + 16X + 49) + 160X^2 - 146X - 148$.

Définition 5.2.6 *On rappelle qu'un sous-ensemble I de $\mathbb{K}[X]$ est un* **idéal** *de $(\mathbb{K}[X], +, *)$ si*

1. *I est un sous-groupe de $(\mathbb{K}[X], +)$,*
2. *I est stable par multiplication par n'importe quel polynôme de $\mathbb{K}[X]$.*

Exemple : Pour $B \in \mathbb{K}[X]$, on note $B\mathbb{K}[X]$ l'ensemble des multiples de B. Il est facile de vérifier que $B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. En particulier, le singleton $\{0\}$ est un idéal.

Nous laissons au lecteur le soin de montrer la proposition suivante :

Proposition 5.2.7 *Soit A et B deux polynômes. Alors $A \mid B$ si et seulement si $B\mathbb{K}[X] \subset A\mathbb{K}[X]$.*

Théorème 5.2.8 *Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. Alors il existe un unique polynôme P unitaire tel que $I = P\mathbb{K}[X]$. Le polynôme P est appelé* **générateur unitaire** *de I.*

On dit que $(\mathbb{K}[X], +, *)$ est un **idéal principal** *.*

Preuve : Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. On note

$$E = \{\deg A \mid A \in I \backslash \{0\}\}.$$

L'ensemble E est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément. On en déduit que I admet un polynôme P non nul et de degré minimal. Comme pour tout $\lambda \in \mathbb{K}$, le polynôme λP appartient aussi à I, on peut toujours choisir P unitaire. La stabilité de I par multiplication par les éléments de $\mathbb{K}[X]$ assure que $P\mathbb{K}[X] \subset I$.

Reste à montrer que $I \subset P\mathbb{K}[X]$. Soit donc $A \in I$. Écrivons la division euclidienne de A par P :

$$A = PQ + R \quad \text{avec} \quad \deg R < \deg P.$$

Comme A et PQ appartiennent à I, on a aussi $R \in I$. Mais par ailleurs $\deg R < \deg P$. Vu la définition de P, on conclut que $R = 0$. ■

5.3 PGCD et PPCM

La division euclidienne va nous permettre de définir les notions de PGCD et de PPCM dans l'ensemble des polynômes.

5.3.1 PGCD

Proposition 5.3.1 *Soit A et B deux polynômes non tous les deux nuls. L'ensemble*

$$A\mathbb{K}[X] + B\mathbb{K}[X] \overset{\text{déf}}{=} \left\{AP + BQ \mid P \in \mathbb{K}[X],\ Q \in \mathbb{K}[X]\right\}$$

est un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. Son générateur unitaire[2] *D est appelé* **Plus Grand Commun Diviseur** *(ou plus simplement PGCD) de A et de B, et est noté* $\mathrm{PGCD}(A, B)$.

Preuve : Notons $J \overset{\text{déf}}{=} A\mathbb{K}[X] + B\mathbb{K}[X]$. Remarquons que J n'est pas réduit à $\{0\}$ car contient A et B, et que l'un de ces deux polynômes n'est pas nul par hypothèse. Reste à montrer que J est un idéal.

1. Montrons que J est un sous-groupe de $(\mathbb{K}[X], +)$:
   - Il est évident que $0 \in J$.
   - Soit C et C' deux polynômes de J. Alors il existe quatre polynômes P, P', Q et Q' tels que $C = AP + BQ$ et $C' = AP' + BQ'$. Donc
   $$C + C' = A(P+P') + B(Q+Q') \in J.$$
   - Enfin, si $C = AP + BQ$, il est clair que $-C = A(-P) + B(-Q)$, donc $-C \in J$.
2. Stabilité de J par produit :
   Soit $C = AP + BQ$ un élément de J, et R un polynôme quelconque. Alors $RC = A(PR) + B(QR)$ donc $RC \in J$.

On conclut que J est un idéal non réduit à $\{0\}$. Le théorème 5.2.8 assure l'existence d'un unique polynôme unitaire D tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$. ■

Remarque : On convient que $\mathrm{PGCD}(0, 0) = 0$. Pour tout couple de polynômes (A, B), on a donc $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathrm{PGCD}(A, B)\,\mathbb{K}[X]$.

La proposition suivante justifie l'appellation "PGCD" donnée au générateur unitaire de $A\mathbb{K}[X] + B\mathbb{K}[X]$.

[2] Dans certains ouvrages, le caractère unitaire n'est pas imposé au PGCD.

Proposition 5.3.2 *Soit (A, B) un couple de polynômes distinct de $(0, 0)$. Alors* $\mathrm{PGCD}\,(A, B)$ *est l'unique polynôme unitaire vérifiant*

$$\mathrm{PGCD}\,(A,B) \mid A, \quad \mathrm{PGCD}\,(A,B) \mid B \quad et \quad (P \mid A \text{ et } P \mid B) \Rightarrow P \mid \mathrm{PGCD}\,(A,B). \tag{5.1}$$

Preuve : Notons $D = \mathrm{PGCD}\,(A, B)$ et montrons que D vérifie (5.1).

Par définition, $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. Comme A et B appartiennent tous les deux à l'ensemble de droite, A et B sont bien des multiples de D. Enfin, si P divise A et B alors, d'après la proposition 5.2.7, $A\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc P divise D.

Pour montrer l'unicité, considérons un polynôme D' unitaire vérifiant (5.1). On a donc en particulier $D \mid D'$. Mais bien sûr $D' \mid D$ donc D et D' sont associés (cf prop. 5.2.2). Comme D et D' sont unitaires, on a $D = D'$. ■

Proposition 5.3.3 *Si A et B ne sont pas simultanément nuls et si C est unitaire alors on a*

$$\mathrm{PGCD}\,(AC, BC) = C\,\mathrm{PGCD}\,(A, B).$$

Preuve : Notons $D = \mathrm{PGCD}\,(A, B)$ et $\Delta = \mathrm{PGCD}\,(AC, BC)$. Il suffit alors de remarquer que

$$\Delta\mathbb{K}[X] = AC\mathbb{K}[X] + BC\mathbb{K}[X] = C\,(A\mathbb{K}[X] + B\mathbb{K}[X]) = CD\mathbb{K}[X].$$

■

Définition 5.3.4 *On dit que deux polynômes A et B sont* **premiers entre eux** *si leur PGCD vaut 1.*

Théorème 5.3.5 (de Bezout) *Deux polynômes A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que $AU + BV = 1$.*

Preuve : $\Longrightarrow$ Si $\mathrm{PGCD}\,(A, B) = 1$ alors par définition du PGCD, on a $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Donc $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$, ce qui signifie qu'il existe U et V tels que $AU + BV = 1$.

$\Longleftarrow$ Si $AU + BV = 1$ alors $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Le générateur unitaire de $A\mathbb{K}[X] + B\mathbb{K}[X]$ est donc un diviseur de 1, donc 1 lui-même. On a donc bien $1 = \mathrm{PGCD}\,(A, B)$. ■

Proposition 5.3.6 *Pour que le polynôme unitaire D soit le PGCD de A et de B, il faut et il suffit que*

$$D \mid A, \quad D \mid B \quad et \quad \mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = 1. \tag{5.2}$$

Preuve : Si $D = \mathrm{PGCD}\,(A, B)$, on a bien sûr $D \mid A$ et $D \mid B$. Notons $P = \frac{A}{D}$ et $Q = \frac{B}{D}$. D'après la proposition 5.3.3, on a

$$D = \mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(DP, DQ) = D\,\mathrm{PGCD}\,(P, Q).$$

Comme D n'est pas nul, on conclut que $\mathrm{PGCD}\,(P, Q) = 1$.

Réciproquement, supposons que (5.2) soit satisfaite. Alors, la proposition 5.3.3 entraîne

$$\mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(D\frac{A}{D}, D\frac{B}{D}) = D\mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = D.$$

■

Théorème 5.3.7 (de Bezout généralisé) *Supposons que D unitaire divise A et B avec A et B non tous les deux nuls. Alors on a*

$$D = \mathrm{PGCD}\,(A, B) \iff \exists U \in \mathbb{K}[X],\ \exists V \in \mathbb{K}[X],\ AU + BV = D.$$

Preuve : En appliquant la proposition 5.3.6, on a

$$D = \mathrm{PGCD}\,(A, B) \iff 1 = \mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}).$$

Or d'après le théorème de Bezout, on a

$$\mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = 1 \iff \exists U \in \mathbb{K}[X],\ \exists V \in \mathbb{K}[X],\ \frac{A}{D}U + \frac{B}{D}V = 1,$$

ce qui achève la preuve du théorème. ■

Théorème 5.3.8 (de Gauss) *Si P divise AB et est premier avec A alors P divise B.*

Preuve : Soit B' le polynôme unitaire associé à B. On a

$$\mathrm{PGCD}\,(PB, AB) = B'\,\mathrm{PGCD}\,(P, A) = B'.$$

Par hypothèse, P divise AB, et il est clair que P divise aussi PB. Donc P divise B' et, partant, B. ■

Proposition 5.3.9 *Un polynôme P est premier avec un produit AB si et seulement si P est premier avec A et avec B.*

Preuve : $\Rightarrow$ Supposons P premier avec AB. Soit P' divisant P et A. Alors P' divise aussi AB. Donc $P' \mid \mathrm{PGCD}\,(AB, P)$, i.e $P'|1$. On en déduit que P' est un polynôme constant. Donc P est premier avec A. On établit de même que P est premier avec B.

$\Leftarrow$ On prouve la réciproque par contraposition. Supposons que P ne soit pas premier avec AB. Alors il existe P' divisant P et AB, et tel que $\deg P' \geq 1$. Si P est premier avec A alors P' également. D'après le théorème de Gauss, P' divise donc B. On a donc montré que P' divise à la fois P et B. Comme $\deg P' \geq 1$, cela signifie que P et B ne sont pas premiers entre eux. ■

Remarque 5.3.10 *Une récurrence élémentaire permet de montrer plus généralement qu'un polynôme P est premier avec un produit de polynôme $A_1 \cdots A_k$ si et seulement si il est premier avec chacun des facteurs A_i. Les détails sont laissés en* **exercice**.

5.3.2 L'algorithme d'Euclide

L'*algorithme d'Euclide* est un moyen systématique permettant de calculer le PGCD de deux polynômes. L'outil de base est la *division euclidienne*. L'algorithme repose sur le lemme suivant :

Lemme 5.3.11 *Soit B un polynôme non nul, et A un polynôme quelconque. Notons Q et R le quotient et le reste de la division euclidienne de A par B. Alors on a*

$$\mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(B, R).$$

Preuve : Soit D divisant A et B. Comme $R = A - BQ$, le polynôme D divise aussi R. Donc D divise $\text{PGCD}(B, R)$. En choisissant $D = \text{PGCD}(A, B)$, on conclut que $\text{PGCD}(A, B) \mid \text{PGCD}(B, R)$.

Soit maintenant D un polynôme divisant B et R. Comme $A = BQ + R$, on a aussi $D \mid A$. Donc $D \mid \text{PGCD}(A, B)$. On a donc finalement $\text{PGCD}(B, R) \mid \text{PGCD}(A, B)$.

Les deux polynômes $\text{PGCD}(B, R)$ et $\text{PGCD}(A, B)$ sont unitaires et associés. Ils sont donc égaux. ■

Ce lemme indique clairement la stratégie à suivre pour calculer $\text{PGCD}(A, B)$. Quitte à permuter A et B, on peut toujours supposer que $\deg A \geq \deg B$. On procède alors comme suit :

- Si $B = 0$, il n'y a rien à faire : $\text{PGCD}(A, B)$ est égal au polynôme unitaire associé à A.
- Si B n'est pas nul, on effectue la division euclidienne de A par B, ce qui donne deux polynômes Q_0 et R_1 tels que $A = BQ_0 + R_1$ et $\deg R_1 < \deg B$.

Le lemme 5.3.11 montre que $\text{PGCD}(A, B) = \text{PGCD}(B, R_1)$. On reprend le calcul ci-dessus en remplaçant A par B, et B par R_1. En itérant le procédé, on construit deux suites R_1, R_2, $\cdots$ et Q_0, Q_1, $\cdots$ telles que :

$$\begin{array}{llll} A & = BQ_0 + R_1 & \text{avec} & \deg R_1 < \deg B, \\ B & = R_1Q_1 + R_2 & \text{avec} & \deg R_2 < \deg R_1, \\ R_1 & = R_2Q_2 + R_3 & \text{avec} & \deg R_3 < \deg R_2, \\ \cdots & \cdots & \cdots & \cdots \\ R_{k-1} & = R_kQ_k + R_{k+1} & \text{avec} & \deg R_{k+1} < \deg R_k, \\ \cdots & \cdots & \cdots & \cdots \\ R_{n-1} & = R_nQ_n + 0. & & \end{array}$$

Le procédé s'arrête nécessairement au bout d'au plus $\deg P$ étapes car chaque itération diminue d'au moins 1 le degré du reste de la division euclidienne. On a donc finalement

$$\boxed{\text{PGCD}(A, B) = \text{PGCD}(B, R_1) = \cdots = \text{PGCD}(R_k, R_{k+1}) = \cdots = \text{PGCD}(R_n, 0) = R_n.}$$

Exemple : Calculer $\text{PGCD}(X^4 - 1, X^3 - 1)$.

Posons la division euclidienne de $X^4 - 1$ par $X^3 - 1$.

$$\begin{array}{r|l} X^4 + \ 0X^3 + \ 0X^2 + \ 0X - \ 1 & X^3 + \ 0X^2 + \ 0X - \ 1 \\ \hline X - \ 1 & \quad X \end{array}$$

Donc $\text{PGCD}(X^4 - 1, X^3 - 1) = \text{PGCD}(X^3 - 1, X - 1)$.

On remarque ensuite que $X^3 - 1$ est divisible par $X - 1$ donc finalement

$$\boxed{\text{PGCD}(X^4 - 1, X^3 - 1) = \text{PGCD}(X^3 - 1, X - 1) = \text{PGCD}(X - 1, 0) = X - 1.}$$

5.3.3 PPCM

Nous laissons au lecteur le soin de prouver le résultat suivant :

Proposition 5.3.12 *Considérons deux polynômes non nuls A et B. Alors l'ensemble $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal non réduit à $\{0\}$. Son générateur unitaire*[3] *est appelé* **Plus Petit Commun Multiple** *(ou plus simplement* **PPCM***) de A et B. On le note* $\text{PPCM}(A, B)$.

Remarque : Si A ou B est nul, on a $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \{0\}$. On adopte alors la convention que $\text{PPCM}(A, B) = 0$. Ainsi, on aura toujours $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \text{PPCM}(A, B)\,\mathbb{K}[X]$.

[3]Dans certains ouvrages, on n'impose pas au PPCM d'être unitaire

En s'inspirant de la preuve de la proposition 5.1, on obtient le résultat suivant qui explique l'appellation "Plus Petit Commun Multiple" donnée au générateur unitaire de $A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

Proposition 5.3.13 *Soit A et B deux polynômes non nuls. Le PPCM de A et de B est l'unique polynôme unitaire vérifiant la propriété suivante :*

$$A \mid \mathrm{PPCM}\,(A,B), \quad B \mid \mathrm{PPCM}\,(A,B) \quad \textit{et} \quad (A \mid M \textit{ et } B \mid M) \Rightarrow \mathrm{PPCM}\,(A,B) \mid M.$$

À certains égards, le PPCM et le PGCD ont des propriétés très similaires. On a par exemple :

Proposition 5.3.14 *Soit C un polynôme unitaire et A, B deux polynômes. Alors on a*

$$\mathrm{PPCM}\,(AC,BC) = C\,\mathrm{PPCM}\,(A,B).$$

Preuve : Il suffit de remarquer que

$$AC\mathbb{K}[X] \cap BC\mathbb{K}[X] = C\left(A\mathbb{K}[X] \cap B\mathbb{K}[X]\right).$$

■

Proposition 5.3.15 *Soit A et B deux polynômes non nuls. Pour que M unitaire soit le PPCM de A et de B, il faut et il suffit que*

$$A \mid M, \quad B \mid M \quad \textit{et} \quad \mathrm{PGCD}\left(\frac{M}{A}, \frac{M}{B}\right) = 1.$$

Preuve : $\Rightarrow$ Notons M le PPCM de A et de B. Alors $M\mathbb{K}[X]$ est inclus dans $A\mathbb{K}[X]$ et dans $B\mathbb{K}[X]$. Donc M divise bien A et B. Soit D unitaire divisant M/A et M/B. Alors $AD|M$ et $BD|M$. Donc $\mathrm{PPCM}\,(AD,BD)|M$. Mais d'après la proposition 5.3.14, $\mathrm{PPCM}\,(AD,BD) = D\,\mathrm{PPCM}\,(A,B) = DM$. Donc $D = 1$.

$\Leftarrow$ Soit M un multiple commun unitaire de A et de B vérifiant de plus $\mathrm{PGCD}\,(\frac{M}{A}, \frac{M}{B}) = 1$. D'après le théorème de Bezout, il existe deux polynômes U et V tels que

$$\frac{M}{A}U + \frac{M}{B}V = 1.$$

Multiplions les deux membres de cette égalité par $\mathrm{PPCM}\,(A,B)$. On trouve

$$M\left(U\frac{\mathrm{PPCM}\,(A,B)}{A} + V\frac{\mathrm{PPCM}\,(A,B)}{B}\right) = \mathrm{PPCM}\,(A,B).$$

Donc M divise $\mathrm{PPCM}\,(A,B)$. Comme M est unitaire et est multiple de A et de B, on conclut que $M = \mathrm{PPCM}\,(A,B)$. ■

Proposition 5.3.16 *Soit A et B deux polynômes. Il existe une constante λ non nulle telle que*

$$\lambda AB = \mathrm{PGCD}\,(A,B)\,\mathrm{PPCM}\,(A,B).$$

- *Si de plus A et B sont unitaires, alors $\lambda = 1$.*
- *Si A et B sont premiers entre eux alors AB et $\mathrm{PPCM}\,(A,B)$ sont associés.*

Preuve : Écartons le cas évident où l'un des deux polynômes A et B est nul. On peut alors appliquer la proposition 5.3.15. On en déduit que

$$\mathrm{PGCD}\left(\frac{\mathrm{PPCM}\,(A,B)}{A}, \frac{\mathrm{PPCM}\,(A,B)}{B}\right) = 1. \tag{5.3}$$

Notons λ l'inverse du coefficient du terme dominant de AB. Alors λAB est unitaire, et la proposition 5.3.14 combinée avec (5.3) montre que

$$\mathrm{PGCD}\left(\lambda AB\left(\frac{\mathrm{PPCM}\,(A,B)}{A}\right), \lambda AB\left(\frac{\mathrm{PPCM}\,(A,B)}{B}\right)\right) = \lambda AB.$$

En appliquant la proposition 5.3.3, on constate que le membre de gauche de cette égalité vaut $\mathrm{PPCM}\,(A,B)\,\mathrm{PGCD}\,(A,B)$. ■

5.3.4 Polynômes irréductibles

Au cours des sections qui précèdent, le lecteur a pu constater que l'ensemble $\mathbb{K}[X]$ avait beaucoup de similarités avec l'ensemble $\mathbb{Z}$ des entiers relatifs : les deux ensembles sont des anneaux principaux intègres sur lesquels on peut définir la division euclidienne, le PGCD et le PPCM. Dans cette section, nous allons introduire une classe de polynômes qui jouent dans $\mathbb{K}[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$: les polynômes irréductibles.

Définition 5.3.17 *On dit qu'un polynôme P est* **irréductible** *si ses seuls diviseurs sont les constantes et les polynômes qui lui sont associés.*

Remarques :

1. À la différence des nombres premiers, les polynômes irréductibles ont une infinité de diviseurs. Mais on notera que ces diviseurs sont triviaux !
2. Tout polynôme de degré 1 est irréductible. En effet, soit P de degré 1, et Q un diviseur de P. Alors $\deg Q \in \{0, 1\}$. Si $\deg Q = 0$ alors Q est une constante, si $\deg Q = 1$ alors $\deg Q = \deg P$ donc P et Q sont associés.

La proposition suivante constitue une "loi du tout ou rien" pour la division par les polynômes irréductibles.

Proposition 5.3.18 *Soit A un polynôme et P un polynôme irréductible ne divisant pas A. Alors P est premier avec A.*

Preuve : Soit B un diviseur commun de A et de P. Comme P est irréductible, B doit être constant, ou associé à P. Le deuxième cas est exclus car on a supposé que P ne divisait pas A. Donc B est constant. On a donc bien $\mathrm{PGCD}\,(A, P) = 1$. ∎

De même que tout entier possède une décomposition en facteurs premiers, tout polynôme a une décomposition en facteurs irréductibles.

Théorème 5.3.19 (Décomposition en facteurs irréductibles) *Soit P un polynôme non constant. Alors il existe un entier $k \geq 1$, k entiers $\alpha_1, \cdots, \alpha_k$ non nuls, k polynômes irréductibles unitaires $P_1, \cdots, P_k$ deux à deux distincts, et $\lambda \in \mathbb{K}\backslash\{0\}$ tels que*

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i}.$$

Cette décomposition, appelée décomposition en facteurs irréductibles, est unique à ordre des facteurs près.

Preuve : On prouve d'abord l'existence puis l'unicité à ordre des facteurs près.

Existence : Elle se fait par récurrence sur le degré de P.

- Si $\deg P = 1$ alors P est irréductible. On pose $k = 1$, $\alpha_1 = 1$ et l'on prend pour P_1 le polynôme unitaire associé à P. Il est de degré 1 donc irréductible.
- Supposons maintenant que le théorème de décomposition soit valable pour tout polynôme de degré compris entre 1 et n. Soit P de degré $n+1$ et $P' \overset{\text{déf}}{=} P/\lambda$ avec λ coefficient du terme dominant de P. Le polynôme P' est unitaire et de degré $n+1$. S'il est irréductible, $P = \lambda P'$ constitue une décomposition de P en facteurs premiers. Sinon, il existe un polynôme A unitaire de degré compris entre 1 et n et divisant P'. On a donc $P' = AB$ avec A et B unitaires et de degré compris entre 1 et

n. D'après l'hypothèse de récurrence, A et B admettent chacun une décomposition en facteurs premiers :

$$A = \prod_{i=1}^{k} A_i^{\alpha_i} \quad \text{et} \quad B = \prod_{i=1}^{\ell} B_i^{\beta_i}.$$

Donc

$$P = \lambda \left(\prod_{i=1}^{k} A_i^{\alpha_i} \right) \left(\prod_{i=1}^{\ell} B_i^{\beta_i} \right).$$

Il ne reste plus qu'à renuméroter les facteurs de la décomposition pour obtenir le résultat voulu.

Unicité : Supposons que P admette *deux* décompositions en facteurs irréductibles :

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i} = \mu \prod_{i=1}^{\ell} Q_i^{\beta_i}.$$

Comme tous les facteurs irréductibles sont unitaires, λ et μ sont égaux au coefficient du terme dominant de P. Donc $\lambda = \mu$. De ce fait, on a

$$\prod_{i=1}^{k} P_i^{\alpha_i} = \prod_{i=1}^{\ell} Q_i^{\beta_i}. \tag{5.4}$$

Par ailleurs, P_1 divise la somme de droite. De la remarque 5.3.10, on déduit que P_1 n'est pas premier avec au moins un des Q_j : il existe j_1 tel que Q_{j_1} et P_1 ne soient pas premiers entre eux. Comme par ailleurs Q_{j_1} et P_1 sont irréductibles et unitaires, cela signifie que $P_1 = Q_{j_1}$. En vertu du caractère intègre de $\mathbb{K}[X]$, on peut donc simplifier l'expression (5.4) par P_1. On itère ce procédé et en $\alpha_1 + \cdots + \alpha_k$ étapes, on parvient à une expression du type $1 = \prod_{j=1}^{\ell} Q_j^{\beta'_j}$ avec $\beta'_j = \beta_j - \alpha_j$. Cela permet de conclure que tous les β'_j sont nuls. Donc les deux décompositions sont identiques à ordre près des facteurs.

■

5.4 Fonctions polynômes

5.4.1 Définition des fonctions polynômes

Jusqu'à présent, nous avons traité les polynômes comme des objets algébriques "abstraits". Ce point de vue permet de manipuler de façon unifiée des objets mathématiques très différents dès lors qu'ils peuvent être interprétés comme des polynômes. Dans cette section, nous allons nous borner à remplacer la variable muette X par des nombres réels ou complexes. Mais vous verrez en deuxième année que l'on peut fort bien remplacer X par une matrice...

Définition 5.4.1 *Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$, et $t \in \mathbb{K}$. On définit alors l'élément $P(t)$ de $\mathbb{K}$ par*

$$P(t) = a_n t^n + \cdots + a_1 t + a_0.$$

On dit que $P(t)$ est obtenu par substitution de t à X.

Proposition 5.4.2 *Soit $t \in \mathbb{K}$ un scalaire fixé. Alors on a pour tous polynômes P et Q, et pour tout scalaire λ :*

1. $P(t)+Q(t)=(P+Q)(t)$,
2. $P(t)Q(t)=(PQ)(t)$,
3. $\lambda P(t)=(\lambda P)(t)$,
4. $1(t)=1$.

Preuve : Vérifions la deuxième relation. Les autres sont immédiates.

Rappelons que si $P=a_pX^p+\cdots+a_1X+a_0$ et $Q=b_qX^q+\cdots+b_1X+b_0$ alors

$$PQ=\sum_{j=0}^{p+q}\Big(\sum_{k+\ell=j}a_kb_\ell\Big)X^j. \tag{5.5}$$

Donc

$$\begin{aligned}(PQ)(t) &= \textstyle\sum_{j=0}^{p+q}\left(\sum_{k+\ell=j}a_kb_\ell\right)t^j,\\ &= \textstyle\sum_{j=0}^{p+q}\left(\sum_{k+\ell=j}(a_kt^k)(b_\ell t^\ell)\right),\\ &= \left(\sum_{k=0}^{p}a_kt^k\right)\left(\sum_{\ell=0}^{q}b_\ell t^\ell\right)=P(t)Q(t).\end{aligned}$$

■

Définition 5.4.3 *Soit $P\in\mathbb{K}[X]$. L'application*

$$\widetilde{P}\ :\ \left\{\begin{array}{ccc}\mathbb{K} & \longrightarrow & \mathbb{K}\\ t & \longmapsto & P(t)\end{array}\right.$$

est appelée fonction polynôme définie par P sur $\mathbb{K}$.

Remarque : Dans la suite du cours, on ne fera plus la distinction entre le polynôme P qui est un objet algébrique et la fonction polynôme $\widetilde{P}$ qui lui est associée[4].

5.4.2 Racines

Définition 5.4.4 *Soit $a\in\mathbb{K}$ et $P\in\mathbb{K}[X]$. On dit que a est* **racine** *ou* **zéro** *de P si $P(a)=0$.*

Proposition 5.4.5 *Soit $a\in\mathbb{K}$ et $P\in\mathbb{K}[X]$. Pour que a soit une racine de P, il faut et il suffit que $X-a$ divise P.*

Preuve : $\Rightarrow$ Supposons que $P(a)=0$. La division euclidienne de P par $X-a$ donne

$$P=Q(X-a)+R\quad\text{avec}\quad\deg R\leq 0.$$

En substituant a à X dans la relation ci-dessus, on trouve $R(a)=0$. Comme la fonction polynôme R est constante, on conclut que $R=0$.

$\Leftarrow$ Si $X-a\mid P$ alors il existe Q tel que $P=Q(X-a)$, ce qui donne en particulier $P(a)=Q(a)(a-a)=0$. ■

Définition 5.4.6 *Soit $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$ et $k\in\mathbb{N}^*$. On dit que a est racine de P de multiplicité k si $(X-a)^k\mid P$.*

- *Si $k=1$, on parle de racine simple,*
- *Si $k=2$, on dit que a est racine double,*
- *Si $k=3$, on dit que a est racine triple, etc.*

[4]La proposition 5.4.2 nous autorise à faire cet abus de notation.

Proposition 5.4.7 *Soit P un polynôme non nul admettant les racines $a_1, \cdots, a_k$ avec multiplicité $\alpha_1, \cdots, \alpha_k$. Alors $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P.*

Preuve :

- On sait déjà que $(X-a_1)^{\alpha_1}$ divise P.
- Supposons que $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$ divise P (avec $j \leq k$). Comme les a_i sont deux à deux distincts, les polynômes $(X-a_i)^{\alpha_i}$ sont premiers entre eux deux à deux. La remarque 5.3.10 permet donc d'affirmer que $(X-a_j)^{\alpha_j}$ est premier avec $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$. Comme P est multiple de $(X-a_j)^{\alpha_j}$ par hypothèse, et de $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$, P est également multiple du PPCM de ces deux polynômes qui, d'après la proposition 5.3.16, vaut $\prod_{i=1}^{j}(X-a_i)^{\alpha_i}$.

Nous venons donc de montrer par récurrence sur j que $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P. ■

Remarque 5.4.8 *En particulier, si $P \neq 0$, toutes les racines de P sont de multiplicité inférieure ou égale à $\deg P$.*

Exercice : Justifier la remarque 5.4.8.

Proposition 5.4.9 *Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines comptées avec leur ordre de multiplicité : $\{a_1, \cdots, a_k\}$ est l'ensemble des racines de P, et α_i est la multiplicité de a_i, alors on a $\alpha_1 + \cdots + \alpha_k \leq n$.*

Preuve : D'après la proposition 5.4.8, on a $\prod_{i=1}^{k}(X-a_i)^{\alpha_i} \mid P$. Donc

$$\sum_{i=1}^{k} \deg(X-a_i)^{\alpha_i} \leq \deg P.$$

Le membre de gauche vaut $\sum_{i=1}^{k}\alpha_i$, d'où le résultat. ■

Remarque 5.4.10 *Le seul polynôme ayant une infinité de racines est le polynôme nul.*

5.4.3 Polynômes dérivés

Définition 5.4.11 *Soit $P = a_kX^k + \cdots + a_1X + a_0$ un polynôme de $\mathbb{K}[X]$. On appelle* **polynôme dérivé** *noté P' le polynôme suivant :*

$$P' = ka_kX^{k-1} + \cdots + a_1 = \sum_{j=1}^{k} ja_jX^{j-1}.$$

Proposition 5.4.12 *Soit P et Q deux polynômes, et $\lambda \in \mathbb{K}$.*

1. *Si $\deg P > 0$ alors $\deg P' = \deg P - 1$,*
2. *Si P est constant alors $P' = 0$,*
3. *$(P+Q)' = P' + Q'$,*
4. *$(\lambda P)' = \lambda P'$,*
5. *$(PQ)' = P'Q + PQ'$.*

Preuve : Les quatre premiers points sont évidents. Prouvons le cinquième.

Soit $P = a_pX^p + \cdots + a_1X + a_0$ et $Q = b_qX^q + \cdots + b_1X + b_0$. En appliquant la définition du polynôme dérivé à la relation (5.5), on trouve

$$(PQ)' = \sum_{j=1}^{p+q} j\Big(\sum_{k+\ell=j} a_kb_\ell\Big)X^{j-1}.$$

Des calculs élémentaires montrent donc que

$$\begin{aligned}(PQ)' &= \sum_{j=1}^{p+q}\sum_{k+\ell=j}\Big(ka_kX^{k-1}b_\ell X^\ell + a_kX^k\ell b_\ell X^{\ell-1}\Big),\\ &= \sum_{j=1}^{p+q}\Big(\sum_{k+\ell=j} ka_kX^{k-1}\,b_\ell X^\ell\Big) + \sum_{j=1}^{p+q}\Big(\sum_{k+\ell=j} a_kX^k\,\ell b_\ell X^{\ell-1}\Big),\\ &= \Big(\sum_{k=1}^{p} ka_kX^{k-1}\Big)\Big(\sum_{\ell=0}^{q} b_\ell X^\ell\Big) + \Big(\sum_{k=0}^{p} a_kX^k\Big)\Big(\sum_{\ell=1}^{q}\ell b_\ell X^{\ell-1}\Big),\\ &= P'Q + PQ'.\end{aligned}$$

■

Proposition 5.4.13 *Soit P un polynôme non nul, et a une racine de P. Alors a est une racine simple si et seulement si $P'(a) \neq 0$.*

Preuve : Nous allons prouver la négation de l'équivalence : i.e a est une racine double de P si et seulement si $P(a) = P'(a) = 0$.

Supposons donc que a est une racine double de P. Alors $(X-a)2 \mid P$. Donc P s'écrit $P = Q(X-a)2$ pour un certain polynôme Q. Il est donc immédiat que $P(a) = 0$. En dérivant, on trouve $P' = Q'(X-a)2 + 2(X-a)Q$, donc $P'(a) = 0$.

Réciproquement, supposons que $P(a) = P'(a) = 0$. La division euclidienne de P par $(X-a)2$ s'écrit $P = Q(X-a)2 + R$ avec $\deg R \leq 1$. Comme $P(a) = 0$, on a $R(a) = 0$. En dérivant la relation $P = Q(X-a)2 + R$, on obtient $R'(a) = 0$. Comme R' est un polynôme constant, on a $R' = 0$, puis, comme $R(a) = 0$, R est nul aussi. ■

5.5 Polynômes scindés

5.5.1 Le théorème fondamental de l'algèbre

Définition 5.5.1 *On dit qu'un polynôme non constant est scindé si la somme des ordres de multiplicité de ses racines est égal à son degré.*

Remarque : Autrement dit, P *de degré* n est scindé si et seulement si il existe un n-uplet $(\lambda_1, \cdots, \lambda_n)$ de $\mathbb{K}^n$ tel que P soit associé à $(X-\lambda_1)\cdots(X-\lambda_n)$.

Proposition 5.5.2 *Soit P un polynôme scindé <u>unitaire</u> d'expression $X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Notons λ_i ses racines comptées avec leur ordre de multiplicité. Alors on a les relations suivantes entre les racines et les coefficients :*

$$a_0 = (-1)^n\prod_{i=1}^{n}\lambda_i \quad \textit{et} \quad a_{n-1} = -\sum_{i=1}^{n}\lambda_i.$$

Preuve : On développe l'expression $(X-\lambda_1)\cdots(X-\lambda_n)$ et on identifie les termes du développement avec ceux de l'expression $X^n + a_{n-1}X^{n-1} + \cdots + a_0$. ■

Remarque : Dans le cas où $P = X^2 + a_1X + a_0$ a pour racines λ_1 et λ_2, on retrouve les relations

$$a_0 = \lambda_1\lambda_2 \quad \text{et} \quad a_1 = -(\lambda_1 + \lambda_2).$$

Le très important résultat suivant est connu sous le nom de **théorème fondamental de l'algèbre** ou **théorème de d'Alembert-Gauss**. Il en existe de nombreuses preuves, mais toutes dépassent le cadre du programme.

Théorème 5.5.3 *Tout polynôme <u>de $\mathbb{C}[X]$</u> est scindé*[5].

[5] On dit que $\mathbb{C}$ est un **corps algébriquement clos.**

Remarque : On a vu que toutes les équations de degré 2 avaient deux solutions (éventuellement confondues) dans $\mathbb{C}$. Le théorème fondamental exprime que toute équation de degré n admet n solutions (éventuellement confondues) dans $\mathbb{C}$. Dans le cas $n = 3$ ou 4, il existe des formules (assez compliquées) donnant les solutions en fonction des coefficients. Pour une équation de degré supérieur ou égal à 5, il a été prouvé par un jeune mathématicien du XIX ème siècle, E. Galois, que de telles formules n'existent pas !

5.5.2 Polynômes irréductibles de $\mathbb{C}[X]$

Théorème 5.5.4 *Un polynôme P est irréductible dans $\mathbb{C}$ si et seulement si* $\deg P = 1$.

Preuve : On a déjà vu que tout polynôme de degré 1 était irréductible (que ce soit dans $\mathbb{C}$ ou dans $\mathbb{R}$).

Pour montrer la réciproque, donnons-nous un polynôme P de degré au moins 2. Le théorème fondamental de l'algèbre nous dit que P admet au moins une racine λ_1. Donc P est divisible par $X - \lambda_1$. Clairement $X - \lambda_1$ n'est pas constant et n'est pas associé à P car de degré strictement inférieur à 2. Donc P n'est pas irréductible. ■

En appliquant le théorème général de décomposition irréductible, on en déduit :

Corollaire 5.5.5 *Tout polynôme P non nul de $\mathbb{C}[X]$ admet une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \prod_{i=1}^{k} (X - \lambda_i)^{\alpha_i},$$

où $\{\lambda_1, \cdots, \lambda_k\}$ est l'ensemble des racines de P, α_i est la multiplicité de λ_i, et λ est le coefficient du terme dominant de P.

5.5.3 Polynômes irréductibles de $\mathbb{R}[X]$

Dans $\mathbb{R}[X]$, la situation est un peu plus compliquée. On sait d'ores et déjà que tous les polynômes irréductibles ne sont pas de degré 1. Par exemple, $X^2 + 1$ ne saurait être irréductible dans $\mathbb{R}[X]$ car n'a pas de racine réelle (la fonction polynôme associée est minorée par 1, donc ne s'annule jamais).

On peut cependant dresser une liste de tous les polynômes irréductibles de $\mathbb{R}[X]$:

Théorème 5.5.6 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

- *Les polynômes de degré 1,*
- *Les polynômes de degré 2 à discriminant strictement négatif : $P = aX^2 + bX + c$ avec $a \neq 0$ et $\Delta \stackrel{\text{déf}}{=} b^2 - 4ac < 0$.*

La preuve de ce théorème repose sur le lemme suivant :

Lemme 5.5.7 *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Notons $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$ le polynôme conjugué. Alors λ est racine de P de multiplicité α si et seulement si $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité α.*

Preuve : Soit λ une racine de P de multiplicité α. Alors il existe un polynôme Q tel que $P = Q(X - \lambda)^\alpha$. En prenant le conjugué de cette expression, on obtient $\overline{P} = \overline{Q}(X - \overline{\lambda})^\alpha$. Donc $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité $\overline{\alpha} \geq \alpha$.

En échangeant les rôles de P et $\overline{P}$, λ et $\overline{\lambda}$, α et $\overline{\alpha}$, on obtient $\overline{\alpha} \leq \alpha$, d'où le résultat. ■

Preuve du théorème 5.5.6 :

On sait déjà que les polynômes de degré 1 sont irréductibles. Soit maintenant $P = aX^2 + bX + c$ à discriminant strictement négatif. La fonction $t \mapsto P(t)$ associée ne s'annule pas sur $\mathbb{R}$ (elle est du signe de a), et donc aucun polynôme de degré 1 ne saurait diviser P. Par ailleurs, on a vu que toute équation de degré 2 à coefficients réels et discriminant positif ou nul admettait au moins une solution réelle. Donc les polynômes de degré 2 à discriminant positif ne sont pas irréductibles dans $\mathbb{R}[X]$.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme de degré au moins 3. Supposons que P n'ait pas de racine réelle (sinon P n'est pas irréductible dans $\mathbb{R}[X]$). D'après le lemme 5.5.7, les racines complexes non réelles de P sont deux à deux conjuguées (avec ordres de multiplicité égaux deux à deux). Le corollaire 5.5.5 assure donc l'existence de nombres complexes (non réels) $\mu_1, \cdots, \mu_p$, d'entiers $\alpha_1, \cdots, \alpha_p$, et d'un réel α, tels que

$$P = \alpha \prod_{i=1}^{p} \Big[(X - \mu_i)^{\alpha_i} (X - \bar{\mu}_i)^{\alpha_i} \Big].$$

Mais un calcul facile montre que

$$(X - \mu_i)^{\alpha_i} (X - \bar{\mu}_i)^{\alpha_i} = (X^2 - 2\mathcal{R}e\,\mu_i\, X + |\mu_i|^2)^{\alpha_i}$$

Donc P est divisible par le polynôme *réel* $X^2 - 2\mathcal{R}e\,\mu_i\, X + |\mu_i|^2$ (de degré 2) et n'est donc pas irréductible. ■

En reprenant la preuve ci-dessus, on déduit facilement le résultat suivant.

Corollaire 5.5.8 *Tout polynôme à coefficients réels admet dans $\mathbb{R}[X]$ une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \Big(\prod_{i=1}^{k} (X - \lambda_i)^{\alpha_i} \Big) \Big(\prod_{j=1}^{\ell} (X^2 - 2\mathcal{R}e\,\mu_j\, X + |\mu_j|^2)^{\beta_j} \Big),$$

où λ est le coefficient du terme dominant de P, $\{\lambda_1, \cdots, \lambda_k\}$ est l'ensemble des racines réelles de P, α_i, multiplicité de λ_i, et $\{\mu_1, \cdots, \mu_\ell\}$ est l'ensemble des racines complexes et non réelles de P et β_j, la multiplicité de μ_j.

Critère d'Eisenstein

Francinou-Gianella-Nicolas, *Oraux X-ENS Algèbre 1*, page 172

Exercice :

1. (a) On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est *primitif* si le *pgcd* de ses coefficients est égal à 1. Montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est primitif.

   (b) Pour $A \in \mathbb{Z}[X]$ non nul, on appelle *contenu de* A, et on note $c(A)$ le *pgcd* des coefficients de A. Soient A et B deux polynômes non nuls de $\mathbb{Z}[X]$. Montrer que $c(AB) = c(A)c(B)$.

2. Soit $A = a_n X^n + \dots a_1 X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que

   (i) p ne divise pas a_0
   (ii) p divise $a_0, a_1, \dots, a_{n-1}$
   (iii) p^2 ne divise pas a_0

   Montrer que A est irréductible dans $\mathbb{Q}[X]$.

1. (a) Soient $A = \sum_{k=0}^{n} a_k X^k$, $B = \sum_{k=0}^{m} b_k X^k$ des polynômes à coefficients entiers et $C = \sum_{k=0}^{m+n} c_k X^k = AB$. Supposons A et B primitifs et montrons en raisonnant par l'absurde, que C est primitif. Si ce n'est pas le cas, il existe un nombre premier p divisant tous les c_k. Pour $P \in \mathbb{Z}[X]$, notons $\overline{P}$ le projeté de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$: si $P = \sum_{k\in\mathbb{N}} s_k X^k$, $\overline{P} = \sum_{k\in\mathbb{N}} \overline{s_k} X^k$, où $\overline{s_k}$ est la classe de s_k modulo p. Comme p divise tous les c_k, on a $\overline{C} = 0$ et donc $\overline{AB} = \overline{AB} = \overline{C} = 0$. Mais $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc on a $\overline{A} = 0$ ou $\overline{B} = 0$. Autrement dit, p divise tous les coefficients de A ou tous les coefficients de B. Ceci est exclu.
   On conclut que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est encore primitif.

   (b) On peut écrire $AB = c(A)c(B)\dfrac{A}{c(A)}\dfrac{B}{c(B)}$. Alors les polynômes $\dfrac{A}{c(A)}$ et $\dfrac{B}{c(B)}$ sont primitifs, donc leur produit aussi d'après la question précédente, et le contenu de AB est $c(A)c(B)$.

2. Montrons que si A n'est pas irréductible dans $\mathbb{Q}[X]$, alors il peut s'écrire $A = BC$ avec B et C dans $\mathbb{Z}[X]$ de degrés strictement inférieurs à celui de A.
   Soient $\alpha = c(A)$ et $A' = A/\alpha \in \mathbb{Z}[X]$; A' est primitif. A étant composé, par hypothès, A' l'est aussi et on peut écrire $A' = B'C'$, avec B' et C' dans $\mathbb{Q}[X]$ de degrés strictement inférieurs à celui de A. Notons β (resp. γ) le produit des dénominateurs des coefficients de B' (resp. C'). Alors les polynômes $B = \beta B'$ et $C = \gamma C'$ sont dans $\mathbb{Z}[X]$ et $\beta\gamma A' = BC$. En passant aux contenus, on obtient $\beta\gamma = \beta\gamma c(A') = c(B)c(C)$. Par conséquent, on a

   $$A = \alpha(B/\beta)(C/\gamma) = \alpha(B/c(B))(C/c(C)) = (\alpha B/c(B))(C/c(C))$$

   et $\alpha B/c(B)$ et $C/c(C)$ sont à coefficients entiers de degré strictement inférieur à celui de A.
   Passons à la démonstration proprement dire du critère d'Eisenstein. Raisonnons par l'absurde et supposons A non irréductible. D'après ce qui précède, il existe B et C dans $\mathbb{Z}[X]$, de degrés strictement inférieurs à n, tels que $A = BC$. Ecrivons $B = b_k X^k + \dots + b_1 X + b_0$ et $C = c_l X^l + \dots + c_1 X + c_0$, avec $k = \deg B$ et $l = \deg C$. Comme dans la question précédente, on projette l'égalité $A = BC$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Il vient $\overline{a_n} X^n = \overline{BC}$. Les polynômes $\overline{B}$ et $\overline{C}$ sont de degrés respectifs k et l car $b_k c_l = a_n$ n'étant pas divisible par p, $\overline{b_k} \neq 0$ et $\overline{c_l} \neq 0$. Par unicité de la décomposition en irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$, $\overline{B} = \overline{b_k} X^k$ et $\overline{C} = \overline{c_l} X^l$. On a alors $\overline{b_0} = \overline{c_0} = 0$, c'est-à-dire $p|b_0$ et $p|c_0$. Mais alors p^2 divise $a_0 = b_0 c_0$ ce qui contredit (iii).

Exemple : $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout entier $n \geq 1$ (prendre $p = 2$), ce qui prouve qu'il y a dans $\mathbb{Q}[X]$ des irréductibles de tout degré.