Chapitre 4

Polynômes

Sommaire

4.1 Vocabulaire des anneaux 1
4.2 L'algèbre des polynômes 2
4.3 Arithmétique des polynômes 7
4.4 Racines 12
4.5 Le théorème fondamental de l'algèbre 14

Intuitivement, un polynôme est une expression de la forme $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$. On part d'un élément indéterminé X, on en écrit des puissances et on multiplie ces puissances par des coefficients a_i choisis dans un ensemble donné (les nombres réels, par exemple). On cherche ensuite à comprendre comment on calcule avec de telles expressions : additionner, multiplier, diviser, composer, etc.

Il est important de comprendre qu'un polynôme n'est pas la même chose qu'une fonction qui serait définie par une formule polynomiale : $f(x) = 3x^2 + 2x + 5$ définit une fonction (de $\mathbb{R}$ dans $\mathbb{R}$ par exemple), alors que $3X^2 + 2X + 5$ désigne un polynôme, donc une formule que l'on peut évaluer dès que l'on choisit une valeur pour X. Une différence tient au fait qu'un polynôme donné (comme $3X^2+2X+5$ à coefficients dans $\mathbb{R}$) peut être appliqué à toutes sortes d'objets au-delà de l'ensemble des coefficients (par exemple à des suites, à des matrices...) tant qu'il est possible d'interpréter les opérations nécessaires.

4.1 Vocabulaire des anneaux

On va voir que sur beaucoup de points les polynômes se manipulent comme les entiers, en particulier on peut y parler de divisibilité et adapter des résultats de l'arithmétique des entiers. Pour faire cela formellement, on utilisera occasionnellement le cadre plus abstrait de la théorie des anneaux.

Un anneau est un ensemble muni de trois opérations d'addition, soustraction et multiplication qui vérifient les propriétés usuelles d'associativité, commutativité (pour l'addition) et distributivité de la multiplication sur l'addition.

4.1 **Définition (anneau).** Un *anneau* est la donné d'un ensemble A, de deux opérations binaires $+$ (addition) et $\cdot$ (multiplication) de $A \times A$ dans A et de deux éléments 0 et 1 de

A qui satisfont les propriétés suivantes :

associativité :	$x+(y+z)=(x+y)+z$	$x(yz)=(xy)z$	pour tous $x,y,z\in A$
commutativité :	$x+y=y+x$		pour tous $x,y,z\in A$
neutralité :	$0+x=0$	$1\cdot x=x\cdot 1=x$	pour tout $x\in A$
distributivité :	$(x+y)z=xz+yz$	$x(y+z)=xy+xz$	pour tous $x,y,z\in A$
	$0\cdot x=0$	$x\cdot 0=0$	pour tout $x\in A$

et tels que tout élément x a un opposé $-x$ tel que $x+(-x)=(-x)+x=0$. L'opération de soustraction est déduite de l'addition et de l'opposé : on pose $x-y:=x+(-y)$.

Un *anneau commutatif* est un anneau dans lequel la propriété de commutativité est satisfaite aussi par la multiplication.

4.2 *Exemple.* L'ensemble $\mathbb{Z}$ des entiers relatifs, avec les opérations usuelles, est un anneau commutatif. Les autres ensembles de nombres usuels $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ en sont aussi.

4.3 *Exemple.* L'ensemble $\mathcal{C}(\mathbb{R})$ des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$, avec les opérations d'addition et de multiplication définies point par point, est un anneau commutatif. L'élément neutre de l'addition y est la fonction nulle et celui de la multiplication est la fonction constante égale à 1.

4.4 *Exemple.* L'ensemble $\mathbb{N}$ des entiers naturels n'est *pas* un anneau. En effet, il satisfait toutes les propriétés sauf l'existence d'opposés : un entier naturel non nul n'a pas d'opposé dans $\mathbb{N}$ pour l'addition.

4.5 En arithmétique (des entiers ou des polynômes), on utilise presque toujours des anneaux commutatifs. Les anneaux non commutatifs existent aussi, les premiers exemples se trouvent en algèbre linéaire avec l'ensemble des endomorphismes d'un espace vectoriel, ou encore l'ensemble des matrices carrées d'un taille donnée.

4.6 Dans la définition, on demande qu'il existe des éléments neutres 0 (pour l'addition) et 1 (pour la multiplication) de sorte que 0 soit absorbant. On ne demande pas que ces deux éléments soient distincts, mais il y a un seul anneau dans lequel $1=0$ et il ne contient pas d'autre élément que 0, en effet pour tout élément x d'un tel anneau on a $x=1\cdot x=0\cdot x=0$.

4.7 **Définition.** Un *corps* est un anneau dans lequel tout élément non nul admet un inverse pour la multiplication.

4.8 *Exemple.* Les ensemble de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

4.9 *Exemple.* L'ensemble des entiers naturels $\mathbb{Z}$ n'est pas un corps puisque seuls -1 et 1 sont inversibles pour la multiplication.

4.2 L'algèbre des polynômes

Formellement, on définit donc un polynôme par la suite de ses coefficients et on définit les opérations usuelles sur les coefficients. Dans tout le chapitre, $\mathbb{K}$ désigne un corps dans lequel on prend les coefficients (ce sera $\mathbb{R}$ ou $\mathbb{C}$ en général, parfois $\mathbb{Q}$).

4.10 **Définition.** L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est l'ensemble des suites à valeurs dans $\mathbb{K}$ nulles à partir d'un certain rang. Pour $P = (a_n) \in \mathbb{K}[X]$, la valeur a_n est appelée *coefficient* de degré n de P. L'ensemble $\mathbb{K}[X]$ est muni des opérations suivantes, où $P = (a_n)$ et $Q = (b_n)$ sont deux éléments de $\mathbb{K}[X]$:

addition $P + Q$ désigne la suite $(a_n + b_n)$,

multiplication PQ désigne la suite (c_n) où pour chaque n on a $c_n = \sum_{i=0}^{n} a_i b_{n-i} = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n$.

Pour tout $\lambda \in \mathbb{K}$, on désigne aussi par λ le polynôme dont le coefficient de degré 0 est λ et dont tous les autres coefficients sont nuls (la suite $\lambda, 0, 0 \ldots$) ; les polynômes de cette forme sont appelés *polynômes constants*. On note X le polynôme dont le coefficient de degré 1 est 1 et donc tous les autres coefficients sont nuls (la suite $0, 1, 0, 0 \ldots$) ; ce polynôme est appelé *l'indéterminée*.

4.11 *Exemple.* Le polynôme P habituellement noté $3X^2 + 2X + 5$ est formellement la suite (a_n) telle que $a_0 = 5$, $a_1 = 2$, $a_2 = 3$ et $a_n = 0$ pour tout $n \geq 3$, c'est-à-dire la suite $5, 2, 3, 0, 0, 0 \ldots$ Le polynôme Q habituellement noté $X^3 - 2X$ est la suite (b_n) dont les premiers termes sont $0, -2, 0, 1, 0, 0 \ldots$

Le polynôme $P + Q$ est donc la suite obtenue en additionnant les termes indice par indice, donc $5, 0, 3, 1, 0, 0 \ldots$, noté habituellement $X^3 + 3X^2 + 5$, ce qui correspond au résultat obtenu en calculant $(3X^2 + 2X + 5) + (X^3 - 2X)$ avec les règles usuelles.

Le polyôme produit PQ, selon la définition, correspond à la suite (c_n) telle que

$$\begin{aligned}
c_0 &= 5 \times 0 = 0 \\
c_1 &= 5 \times (-2) + 2 \times 0 = -10 \\
c_2 &= 5 \times 0 + 2 \times (-2) + 3 \times 0 = -4 \\
c_3 &= 5 \times 1 + 2 \times 0 + 3 \times (-2) + 0 \times 0 = -1 \\
c_4 &= 5 \times 0 + 2 \times 1 + 3 \times 0 + 0 \times (-2) + 0 \times 0 = 2 \\
c_5 &= 5 \times 0 + 2 \times 0 + 3 \times 1 + 0 \times 0 + 0 \times (-2) + 0 \times 0 = 3
\end{aligned}$$

et les coefficients suivants sont tous nuls, donc PQ est ce que l'on note habituellement $3X^5 + 2X^4 - X^3 - 4X^2 - 10X$. On peut vérifier qu'en calculant $(3X^2 + 2X + 5)(X^3 - 2X)$ avec les règles usuelles, on obtient le même résultat.

4.12 La multiplication par un polynôme constant a une expression plus simple et plus intuitive que la multiplication générale : pour $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$ avec $P = (a_n)$, on a tout simplement $\lambda P = (\lambda a_n)$, donc chaque coefficient est multiplié par la constante λ.

4.13 L'opération de puissance P^n se déduit de la multiplication : on pose $P^0 = 1$ pour tout P et $P^n = P \cdot P \cdots P$, produit de n fois le polynôme P. On peut alors observer que X^n désigne le polynôme dont le coefficient de degré n est 1 et les autres sont 0, et par conséquent on a

$$P(X) = \sum_{n=0}^{\infty} a_n X^n \qquad \text{si} \quad P = (a_n)$$

ce qui permet de retrouver l'écriture intuitive d'un polynôme et justifie que a_n est bien le coefficient de degré n, donc le coefficient de X^n dans P. De cette écriture on peut aussi

déduire qu'il est possible d'identifier deux polynômes coefficients par coefficients :

$$\text{Si } \sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} b_n X^n \text{ alors } a_n = b_n \text{ pour tout } n.$$

Notons que ces sommes sont écrites comme si elles étaient infinies mais elle sont en fait finies puisqu'il n'y a qu'un nombre fini de coefficients non nuls.

4.14 À partir de cette écriture, on retrouve les règles habituelles de calcul des sommes et des produits qui justifient les définitions initiales :

$$\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$
$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_i b_j X^{i+j} = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) X^n$$

4.15 **Définition.** Un *monôme* est un polynôme qui a exactement un coefficient non nul.

4.16 *Exemple.* Les constantes non nulles sont des monôme, l'indéterminée X est un monôme, plus généralement les monômes sont tous les polynôme de la forme aX^n pour un certain a non nul.

4.17 **Proposition.** *L'ensemble* $\mathbb{K}[X]$ *est un* algèbre commutative *sur* $\mathbb{K}$*, c'est-à-dire que*
- $\mathbb{K}[X]$ *muni de l'addition et de la multiplication des polynômes est un anneau commutatif, avec* 0 *pour neutre de l'addition et* 1 *pour neutre de la multiplication ;*
- $\mathbb{K}[X]$ *muni de l'addition et de l'opération* $(\lambda, P) \mapsto \lambda P$ *(de* $\mathbb{K} \times \mathbb{K}[X]$ *dans* $\mathbb{K}[X]$*) est un espace vectoriel sur* $\mathbb{K}$ *;*
- *la multiplication est linéaire en ses deux variables :* $P(Q + \lambda R) = PQ + \lambda PR$*,* $(P + \lambda Q)R = PR + \lambda QR$*.*

4.18 **Définition (composition).** Soient P et Q deux polynômes, posons $P = \sum_{n=0}^{\infty} a_n X^n$. La composée de P et Q est le polynôme $\sum_{n=0}^{\infty} a_n Q^n$, noté $P \circ Q$.

4.19 *Exemple.* Reprenons les polynômes $P = 3X^2 + 2X + 5$ et $Q = X^3 - 2X$ de l'exemple précédent. On a $Q^0 = 1$, $Q^1 = Q$ et $Q^2 = (X^3 - 2X)(X^3 - 2X) = X^6 - 4X^4 + 4X^2$ donc $P \circ Q = 3Q^2 + 2Q^1 + 5Q^0 = 3(X^6 - 4X^4 + 4X^2) + 2(X^3 - 2X) + 5$ donc finalement $P \circ Q = 3X^6 - 12X^4 + 2X^3 + 12X^2 - 4X + 5$.

4.20 La composition $P \circ Q$ consiste donc à remplacer l'indéterminée X dans P par un polynôme Q et calculer le résultat avec les opérations d'addition et de multiplication des polynômes. En particulier, $P \circ X$ est toujours la même chose que X, on peut aussi observer que $P \circ 0$ est égal au coefficient de degré 0 de P (la constante).

4.21 **Définition (degré).** Le degré $\deg(P)$ d'un polynôme $P = (a_n)$ est le plus grand n tel que $a_n \neq 0$, ou par convention $-\infty$ si $P = 0$. Un polynôme est *constant* si son degré est $-\infty$ ou 0.

4.22 *Exemple.* Le degré de $3X^2 + 2X + 5$ est 2.

4.23 **Définition (coefficient dominant).** Soit P un polynôme non nul. Le *coefficient dominant* de P est le coefficient de degré $\deg(P)$, c'est-à-dire le coefficient non nul de plus haut degré. Un polynôme P est *unitaire* si son coefficient dominant est 1.

4.24 *Exemple.* Le coefficient dominant de $3X^2 + 2X + 5$ est 3, ce polynôme n'est donc pas unitaire. Le coefficient dominant de $X^3 - X$ est 1 et ce polynôme est unitaire.

4.25 **Proposition.** *Soient P et Q deux polynômes. On a*
- $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$*, avec égalité si* $\deg(P) \neq \deg(Q)$ *;*
- $\deg(PQ) = \deg(P) + \deg(Q)$.
- $\deg(P \circ Q) = \deg(P) \times \deg(Q)$ *si Q n'est pas constant,* $\deg(P \circ Q) \in \{0, -\infty\}$ *si Q est constant.*

Démonstration. Notons $P = \sum_{n=0}^{\infty} a_n X^n$ et $Q = \sum_{n=0}^{\infty} b_n X^n$.

Pour tout $n > \max(\deg(P), \deg(Q))$ on a $a_n = b_n = 0$ par définition du degré, donc $a_n + b_n = 0$, ainsi tous les coefficients de $P + Q$ de degrés strictement supérieurs à $\max(\deg(P), \deg(Q))$ sont nuls, ce qui entraîne $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.

Dans le cas où $\deg(P) \neq \deg(Q)$, en posant $d = \max(\deg(P), \deg(Q))$, on a deux cas exclusifs : soit $d = \deg(P)$ soit $d = \deg(Q)$. Dans le premier cas on a $a_d \neq 0$ et $b_d = 0$ donc $a_d + b_d = a_d \neq 0$ donc $\deg(P+Q) \geq d$ et on a donc bien l'égalité. Le second cas est similaire avec $a_d = 0$ et $b_d \neq 0$.

Pour le produit, considérons un degré n. Par définition on le coefficient de degré n de PQ est $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. On raisonne sur la nullité de $a_i b_{n-i}$ en fonction de i :
- si $i > \deg(P)$ alors $a_i = 0$ et $a_i b_{n_i} = 0$;
- si $i < n - \deg(Q)$ alors $n - i > \deg(Q)$ donc $b_{n-i} = 0$ et $a_i b_{n-i} = 0$;
- si $i = \deg(P)$ et $j = \deg(Q)$ alors $a_i \neq 0$ et $b_{n-i} \neq 0$ donc $a_i b_{n-i} \neq 0$.

Les deux premiers cas prouvent que $c_n = 0$ pour tout $n > \deg(P) + \deg(Q)$ puisque dans ce cas on a $i > \deg(P)$ ou $i < n - \deg(Q)$ pour tout i, par conséquent $\deg(PQ) \leq \deg(P) + \deg(Q)$. Avec le troisième cas on déduit que $c_{\deg(P)+\deg(Q)} \neq 0$ puisque $a_{\deg(P)} b_{\deg(Q)}$ est le seul terme non nul dans la somme pour le cas $n = \deg(P) + \deg(Q)$, par conséquent $\deg(PQ) \geq \deg(P) + \deg(Q)$, on a donc bien l'égalité.

On déduit le cas de la composition des deux cas précédents : pour chaque n on a $\deg(Q^n) = n \deg(Q)$, donc dès que $\deg(Q) \geq 1$ on sait que tous les Q^n sont de degrés distincts, ainsi $\deg(P \circ Q) = \max\{n \deg(Q) \mid a_n \neq 0\} = \deg(P)\deg(Q)$. Dans le cas où Q est constant, tous les Q^n le sont aussi donc $P \circ Q$ aussi, ce qui fait que $\deg(P \circ Q)$ est 0 ou $-\infty$. □

4.26 Dans le cas de la somme l'inégalité est inévitable, parce que certains coefficients de $P + Q$ peuvent s'annuler. Par exemple, si $P = X^3 - X + 1$ et $Q = -X^3 + X^2 + 2$ on a $\deg(P) = \deg(Q) = 3$ or $P + Q = X^2 - X + 3$ donc $\deg(P + Q) = 2$.

4.27 Dans le cas du produit, la formule sur le degré s'applique même en présence de $-\infty$, en effet si $P = 0$ alors $\deg(P) = -\infty$ et pour tout Q on a $PQ = 0$ donc $\deg(PQ) = -\infty = \deg(Q) - \infty$, quel que soit le degré de Q. On peut en déduire des propriétés de la multiplication :
- un produit de polynômes PQ ne peut être nul que si $P = 0$ ou $Q = 0$ (on dit que l'anneau des polynômes est *intègre*),
- pour tout P non nul, si $PA = PB$ alors $A = B$ (en passant par $P(A - B) = 0$, qui ne peut donc être nul que si $A - B = 0$),
- un produit de polynômes PQ ne peut être égal à 1 que si P et Q sont de degré 0, c'est-à-dire constants non nuls, donc les *inversibles* de $\mathbb{K}[X]$ sont exactement les polynômes de degré 0, les polynômes constants non nuls.

4.28 On est parfois amené à considérer des polynômes dont les coefficients sont pris dans un anneau qui n'est pas un corps, par exemple $\mathbb{Z}[X]$ est l'ensemble des polynômes à coefficients entiers. Cet ensemble est lui aussi un anneau, et les opérations sur les polynômes (somme, produit, degré) y sont bien définies aussi, mais certaines propriétés sont perdues (comme la caractérisation des inversibles dans la remarque précédente, ou les résultats d'arithmétique développés dans la suite, qui deviennent plus complexes).

4.29 **Définition (fonction polynomiale).** Soit $P = \sum_{n=0}^{\infty} a_n X^n$ un polynôme un polynôme à coefficients dans $\mathbb{K}$ et soit A une algèbre sur $\mathbb{K}$. On note P_A la fonction de A dans A telle que pour tout $x \in A$ on ait $P_A(x) = \sum_{n=0}^{\infty} a_n x^n$. On appelle *fonction polynomiale* une fonction qui peut s'écrire P_A pour un certain polynôme P.

On rappelle qu'une algèbre sur $\mathbb{K}$ est un ensemble A muni d'opérations d'addition, multiplication interne (pour $x, y \in A$ on a $xy \in A$) et multiplication externe par $\mathbb{K}$ (pour $\lambda \in K$ et $x \in A$ on a $\lambda x \in A$), de sorte que ces opérations vérifient les règles de calcul habituelles. C'est donc à la fois un anneau et un espace vectoriel sur $\mathbb{K}$.

4.30 *Exemple.* Soit le polynôme $P = 3X^2 - 2X + 4$, élément de $\mathbb{R}[X]$. L'ensemble $\mathbb{R}$, avec les opérations usuelles, est une algèbre sur $\mathbb{R}$, on peut donc considérer la fonction $P_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ et c'est la fonction polynomiale définie par la formule $P_{\mathbb{R}}(x) = 3x^2 - 2x + 4$.

L'ensemble $\mathbb{C}$ des nombres complexes est aussi une algèbre sur $\mathbb{R}$ pour les opérations usuelles, donc on peut considérer la fonction $P_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$ définie par la même formule. C'est une fonction différente même si, en quelque sorte, elle étend la précédente.

L'ensemble $\mathcal{M}_2(\mathbb{R})$ des matrices 2×2 à coefficients réels, avec l'addition et le produit de matrices et la multiplication par les scalaires, est une algèbre sur $\mathbb{R}$. On peut donc aussi considérer la fonction $P_{\mathcal{M}_2(\mathbb{R})}$ sur cet ensemble de matrices. Considérons par exemple la matrice $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On peut vérifier que l'on a $M^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, de plus l'élément neutre du produit est la matrice identité $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ donc on a

$$P_{\mathcal{M}_2(\mathbb{R})}(M) = 3M^2 - 2M + 4 = 3\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} - 2\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + 4\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 0 & 5 \end{pmatrix}$$

4.31 Du fait que c'est toujours la même formule qui s'applique quand on calcule P_A dans une algèbre A, on pourra s'autoriser à ne pas préciser l'indice A, à condition qu'il soit clair que l'on est en train de parler de la fonction.

4.32 L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un algèbre sur $\mathbb{K}$, on peut donc considérer la fonction $P_{\mathbb{K}[X]} : \mathbb{K}[X] \to \mathbb{K}[X]$ associée à un polynôme $P \in \mathbb{K}[X]$. On peut vérifier que pour tout $Q \in \mathbb{K}[X]$ on a $P_{\mathbb{K}[X]}(Q) = P \circ Q$, de plus $P_{\mathbb{K}[X]}(X) = P$. Ainsi, en gardant implicite l'indice dans la fonction polynomiale, $P(X)$ désigne exactement la même chose que P et $P(Q)$ désigne la même chose que $P \circ Q$ (et la composition de polynômes correspond se traduit bien par la composition des fonctions polynomiales associées).

4.33 **Exercice.** Montrer que l'évaluation des fonctions polynomiales est compatible avec les opérations sur les polynômes, c'est-à-dire que pour tous polynômes $P, Q \in \mathbb{K}[X]$, toute

algèbre A sur $\mathbb{K}$ et tout élément x de A on a

$$\begin{aligned}(P+Q)_A(x) &= P_A(x) + Q_A(x)\\ (PQ)_A(x) &= P_A(x)\,Q_A(x)\\ (P\circ Q)_A(x) &= P_A(Q_A(x))\end{aligned}$$

4.34 On verra plus loin que si le corps $\mathbb{K}$ des coefficients est infini (c'est bien sûr le cas avec $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$), alors l'égalité des fonctions d'évaluation implique l'égalité des polynômes : si P et Q sont deux polynômes tels que pour tout $x \in \mathbb{K}$ on ait $P_{\mathbb{K}}(x) = Q_{\mathbb{K}}(x)$, alors $P = Q$. On rappelle que l'égalité $P = Q$ signifie, par définition, l'égalité des coefficients degré par degré.

4.3 Arithmétique des polynômes

Les polynômes forment une structure d'anneau, c'est-à-dire qu'on peut les additionner en multiplier en suivant les règles usuelles de calcul. En revanche ils ne forment pas un corps : la plupart des polynômes n'ont pas d'inverse pour la multiplication. En ce sens, la structure de $\mathbb{K}[X]$ est assez similaire à celle de l'ensemble $\mathbb{Z}$ des entiers. On va voir maintenant que la plupart des notions et résultats de l'arithmétique des entiers se transposent bien dans le cas des polynômes.

4.35 **Définition (idéal).** Soit A un anneau commutatif. Un *idéal* de A est un sous-ensemble I de A non vide, stable par addition et soustraction (c'est donc un sous-groupe) et absorbant pour la multiplication (c'est-à-dire que pour tous $x \in A$ et $y \in I$ on a $xy \in I$).

4.36 *Exemple.* L'ensemble des nombres pairs est un idéal de l'anneau $\mathbb{Z}$.

4.37 *Exemple.* Plus généralement, si $a \in A$ est un élément d'un anneau, alors l'ensemble des multiples de a est un idéal que l'on note (a) ou aA. Dans ce cas, a est un *générateur* de l'idéal (a). Un idéal de cette forme est qualifié de *principal*.

4.38 *Exemple.* Dans l'anneau $\mathcal{C}(\mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, l'ensemble Z des fonctions continues qui s'annulent en 0 forme un idéal. En effet il est facile de voir qu'il vérifie les propriétés voulues.

On peut montrer qu'il n'est pas principal. En effet, supposons que $Z = (f)$ pour une certaine fonction f. On peut déjà observer que f doit s'annuler en 0 et uniquement en 0. Considérons alors la fonction $\sqrt[3]{f}$. Cette fonction s'annule en 0, donc $\sqrt[3]{f} \in Z$ et par hypothèse il existe donc une fonction continue $g \in \mathcal{C}(\mathbb{R})$ telle que $\sqrt[3]{f} = fg$. Pour tout $x \neq 0$, on a $f(x) \neq 0$ donc $\sqrt[3]{f(x)} \neq 0$ et donc $g(x) = \sqrt[3]{f(x)}/f(x) = 1/(\sqrt[3]{f(x)}^2)$. Par hypothèse f est continue donc elle tend vers 0 en 0, donc $\sqrt[3]{f}$ aussi, et donc $1/(\sqrt[3]{f(x)}^2)$ diverge quand x tend vers 0, ce qui est contradictoire avec le fait que g est continue.

4.39 **Exercice.** Montrer que dans l'anneau $\mathbb{Z}$, les idéaux sont exactement les sous-ensembles de $\mathbb{Z}$ de la forme $n\mathbb{Z}$, c'est-à-dire $\{nx \mid x \in \mathbb{Z}\}$, pour un n fixé.

4.40 **Définition (anneau quotient).** Soit A un anneau commutatif et soit I un idéal de A. Deux éléments x, y de A sont *congrus modulo* I si $x - y \in I$, ou de façon équivalente si $x+I = y+I$, ce que l'on note aussi $x \equiv y\,[I]$. Les opérations d'addition et de multiplication sont compatibles avec cette équivalence :

— si $x - y \in I$ alors pour tout z on a $(x + z) - (y + z) = x - y \in I$,
— si $x - y \in I$ alors pour tout z on a $xz - yz = (x - y)z \in zI \subseteq I$ (parce que I est absorbant pour le produit).

L'ensemble des classes d'équivalence est l'ensemble $\{x + I \mid x \in A\}$ (qui est donc un ensemble de parties de A), il forme donc un anneau. Cet anneau est appelé *anneau quotient* de A par I et est noté A/I.

4.41 *Exemple.* Dans le cas où $A = \mathbb{Z}$, on retrouve la notion habituelle de congruence en arithmétique : deux entiers a et b sont congrus modulo n au sens usuel si $a-b$ est multiple de n, ce qui revient à dire que $a-b$ est élément de l'idéal $n\mathbb{Z}$. L'ensemble des classes d'équivalence modulo n est l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$, noté $\mathbb{Z}/n\mathbb{Z}$. Dans cet anneau quotient, on calcule avec des additions et des multiplications comme dans $\mathbb{Z}$ (puisque les opérations sont compatibles avec la congruence) et ajoutant en plus la règle que les multiples de n sont tous équivalents à 0.

4.42 **Théorème (division euclidienne).** *L'anneau $\mathbb{K}[X]$ est* euclidien*, c'est-à-dire que la division euclidienne y est bien définie : pour tous $A, B \in \mathbb{K}[X]$ avec $B \neq 0$ il existe un unique couple de polynômes (Q, R) tels que $A = BQ + R$ et $\deg R < \deg B$.*

Démonstration. Considérons l'ensemble (B) de tous les multiples de B dans $\mathbb{K}[X]$. L'ensemble (B) est un idéal de $\mathbb{K}[X]$.

La classe d'équivalence de A modulo (B) est $A + (B)$. Cet ensemble n'est pas vide puisqu'il contient A, l'ensemble des degrés des éléments de $A + (B)$ est donc un sous-ensemble non vide de $\mathbb{N} \cup \{-\infty\}$. Soit R un élément de $A + (B)$ de degré minimal.

On montre que $\deg(R) < \deg(B)$, en procédant par contradiction : supposons que $\deg(R) \geq \deg(B)$. Le terme dominant de R s'écrit $rX^{\deg(R)}$, celui de B s'écrit $bX^{\deg(B)}$. On pose alors $S = (r/b)X^{\deg(R)-\deg(B)}B$. Par construction $R - S$ est de degré strictement inférieur à $\deg(R)$ puisque R et S ont même terme dominant. De plus $S \in (B)$ par construction, or $R \in A + (B)$ donc $R - S \in A + (B)$, on a donc un élément de $A + (B)$ de degré strictement inférieur à celui de R, ce qui contredit la définition de R. Ainsi on a bien $\deg(R) < \deg(B)$.

Par construction $R \in A + (B)$ donc $A - R \in (B)$ c'est-à-dire que $A - R$ est multiple de B, il existe donc un polynôme Q tel que $A - R = BQ$ d'où $A = BQ + R$.

Pour l'unicité, supposons que l'on ait un autre couple (Q', R') tel que $A = BQ' + R'$ et $\deg(R') < \deg(B)$. On a donc $B(Q - Q') + (R - R') = 0$, donc $R - R'$ est multiple de B, donc $\deg(R-R')$ est soit $-\infty$ soit supérieur ou égal à $\deg(B)$. D'autre part $\deg(R-R') \leq \max(\deg(R), \deg(R')) < \deg(B)$. On a donc $\deg(R-R') = \infty$ donc $R-R' = 0$ soit $R = R'$. Par conséquent $B(Q - Q') = 0$ d'où $Q - Q' = 0$ et $Q = Q'$. □

4.43 *Exemple.* Prenons $A = X^4 - X$ et $B = X^2 + 2X + 3$. On peut calculer le quotient et le reste dans la division de A par B comme ceci :

$$\begin{aligned} X^2B &= X^4 + 2X^3 + 3X^2 & A - X^2B &= -2X^3 - 3X^2 - X \\ 2XB &= 2X^3 + 4X^2 + 6X & A - X^2B + 2XB &= X^2 + 5X \\ & & A - X^2 + 2XB - B &= 3X - 3 \end{aligned}$$

on a donc $A = (X^2 - 2X + 1)B + (3X - 3)$. Comme le degré de $3X - 3$ est 1 qui est strictement inférieur à celui de B qui est 2, on a l'écriture attendue. Ainsi le quotient est

$X^2 - 2X + 1$ et le reste est $3X - 3$.

4.44 On peut faire systématiquement ce genre de calcul en posant la division, comme on a appris à le faire pour les nombres entiers depuis l'école primaire. Pour reprendre l'exemple précédent on posera alors comme ceci, avec une colonne par puissance de X :

dividende →	$X^4 \qquad\qquad - X$	$X^2 + 2X + 3$	← diviseur
	$X^4 + 2X^3 + 3X^2$	X^2	
	$\quad - 2X^3 - 3X^2 \ - X$		
	$\quad - 2X^3 - 4X^2 - 6X$	$-2X$	← quotient
	$\qquad\quad X^2 + 5X$		
	$\qquad\quad X^2 + 2X + 3$	1	
reste →	$\qquad\qquad\quad 3X - 3$		

On commence avec comme « reste » le polynôme à diviser (habituellement appelé *dividende*). À chaque étape, on obtient un monôme du quotient en prenant pour degré la différence entre celui du reste et celui diviseur et en prenant pour coefficient le quotient entre le coefficient dominant du reste de celui du diviseur. On reporte le produit de ce monôme avec le diviseur sous le reste (en rangeant par degrés pour faciliter le calcul) puis on calcule la différence pour obtenir le nouveau reste. Le calcul est terminé lorsque le reste a un dégré est inférieur à celui du diviseur. On obtient alors le quotient en faisant la somme des monômes obtenus.

4.45 **Corollaire.** *Tout idéal de $\mathbb{K}[X]$ est principal, c'est-à-dire que pour tout idéal I de $\mathbb{K}[X]$ il existe $B \in \mathbb{K}[X]$, tel que $I = (B)$.*

Démonstration. Par définition, un idéal n'est pas vide. Si $I = \{0\}$ alors $I = (0)$, on suppose donc maintenant que I n'est pas réduit à $\{0\}$. Soit $B \in I$ un polynôme non nul de degré minimal dans I. Pour tout polynôme $A \in I$, par division euclidienne il existe $Q, R \in \mathbb{K}[X]$, tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$. Comme $A, B \in I$ et que I est un idéal, $R = A - BQ$ est aussi dans I. Comme le degré de B est minimal parmi les polynômes non nuls de I, on a $R = 0$. Donc A est un multiple de B. □

4.46 **Exercice.** Montrer que si A et B sont des générateurs du même idéal de $\mathbb{K}[X]$ alors il existe $\lambda \in \mathbb{K}$ tel que $B = \lambda A$. En déduire que tout idéal de $\mathbb{K}[X]$ a un unique générateur qui soit un polynôme unitaire.

4.47 **Exercice.** Montrer que toute intersection d'idéaux d'un anneau donné est un idéal de cet anneau.

4.48 **Définition (PGCD).** Soit $P, Q \in \mathbb{K}[X]$ deux polynômes. Soit (P, Q) l'intersection de tous les idéaux de $\mathbb{K}[X]$ qui contiennent P et Q (comme $\mathbb{K}[X]$ est un idéal qui contient P et Q, (P, Q) existe et est le plus petit idéal contenant P et Q). Un *plus grand commun diviseur* de P et Q est un générateur de l'idéal (P, Q). Le générateur unitaire de cet idéal est noté $P \wedge Q$.

La proposition suivante montre que cette définition correspond bien à la définition utilisée dans les entiers.

4.49 **Proposition.** *Soient P et Q deux polynômes. Alors $P \wedge Q$ est bien un plus grand commun diviseur de P et Q dans le sens suivant :*

— *$P \wedge Q$ divise P et Q,*
— *si D divise P et Q alors D divise $P \wedge Q$.*

Démonstration. Comme $P \wedge Q$ est par définition un générateur d'un idéal contenant P et Q, les polynômes P et Q sont multiples de $P \wedge Q$. Soit D un diviseur commun de P et Q, alors P et Q sont éléments de l'idéal (D) donc $(P,Q) \subseteq (D)$; comme $P \wedge Q$ engendre (P,Q) on a $P \wedge Q \in (P,Q)$ et donc $P \wedge Q \in (D)$, par conséquent D divise $P \wedge Q$. □

4.50 *Exemple.* L'algorithme d'Euclide permet de calculer le PGCD de polynômes de la même façon que pour le PGCD des entiers, simplement en appliquant la division euclidienne des polynômes. Considérons par exemple $P = X^3 - 1$ et $Q = X^2 + X - 2$. On a alors les étapes suivantes (on ne détaille pas le calcul des étapes de division) :

k	A_k	B_k	division euclidienne
0	$X^3 - 1$	$X^2 + X - 2$	$X^3 - 1 = (X-1) \cdot (X^2 + X - 2) + (3X - 3)$
1	$X^2 + X - 2$	$3X - 3$	$X^2 + X - 2 = ((1/3)X + 2/3) \cdot (3X - 3) + 0$
2	$3X - 3$	0	

On obtient donc un PGCD avec le dernier terme non nul obtenu, $3X - 3$, et les deux résultats précédents montrent que tout diviseur commun de $X^3 - 1$ et $X^2 + X - 2$ divise aussi $3X - 3$. On obtient *le* PGCD en divisant ce polynôme par son coefficient dominant pour le rendre unitaire et on obtient $(X^3 - 1) \wedge (X^2 + X - 2) = X - 1$.

4.51 **Théorème (Bézout).** *Pour tous polynômes $P, Q \in \mathbb{K}[X]$ il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = P \wedge Q$.*

Démonstration. Par définition, $P \wedge Q \in (P,Q)$ or l'idéal (P,Q), l'idéal engendré par P et Q, peut s'écrire explicitement sous la forme $(P,Q) = \{UP + VQ \mid U, V \in \mathbb{K}[X]\}$. En effet, cet ensemble est un idéal qui contient P et Q et tout idéal contenant P et Q doit contenir cet ensemble. Ainsi il existe bien $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = P \wedge Q$. □

Cette propriété est exactement la même que le théorème de Bézout pour les entiers. De même, l'algorithme d'Euclide permet de calculer les coefficients dont le théorème prouve l'existence.

4.52 *Exemple.* Pour reprendre l'exemple précédent avec $P = X^3 - 1$ et $Q = X^2 + X - 2$ dont le PGCD est $X - 1$, on déduit les calculs suivants en relisant les étapes de l'algorithme. En effet la divison de P par Q donne $P = (X-1)Q - (3X-3)$ donc $3X - 3 = P - (X-1)Q$ or le PGCD est $(1/3)(3X - 3)$ donc $P \wedge Q = (1/3)P - (X/3 - 1/3)Q$, autrement dit $U = 1/3$ et $V = (1/3)X + 1/3$ conviennent.

4.53 **Définition (polynômes premiers entre eux).** Deux polynômes P et Q sont *premiers entre eux* si leurs seuls diviseurs communs sont des constantes.

4.54 *Exemple.* Les polynômes $X^2 + X + 1$ et $X - 2$ sont premiers entre eux. En effet, les seuls diviseurs de $X - 2$ sont les constantes et les polyômes obtenues en multipliant $X - 2$ par une constante. Or la division euclidienne de $X^2 + X + 1$ par $X - 2$ donne $X^2 + X + 1 = (X + 3)(X - 2) + 7$ donc $X^2 + X + 1$ n'est pas divisible par $X - 2$ et en conséquence les seuls diviseurs communs sont les constantes.

4.55 Comme dans le cas de entiers, selon le théorème de Bézout, P et Q sont premiers entre eux si et seulement s'il existe $U, V \in \mathbb{K}[X]$, tels que $UP + VQ = 1$.

Le lemme suivant est l'analogue du lemme de Gauss des entiers dans le cas de l'anneau $\mathbb{K}[X]$.

4.56 **Proposition.** *Soient P, A, B trois polynômes. Si P divise AB et si P et A sont premiers entre eux alors P divise B.*

Démonstration. Comme P et A sont supposés premiers entre eux, d'après le théorème de Bézout il existe deux polynômes U et V, tels que $UA + VP = 1$. En multipliant par B, on obtient $UAB + VPB = B$. Comme P divise AB, il divise UAB, de plus P divise évidemment VPB, donc P divise B. □

4.57 **Définition (polynôme irréductible).** Un polynôme P est *irréductible* s'il n'est pas constant et si ses diviseurs sont uniquement les λP pour $\lambda \in \mathbb{K}$ et les polynômes constants.

Les polynômes irréductibles sont l'analogue des nombres premiers dans le cas des polynômes : ce sont ceux que l'on ne peut pas décomposer par division.

4.58 *Exemple.* Quel que soit $\mathbb{K}$, les polynômes de la forme $aX + b$ avec $a \neq 0$ sont toujours irréductibles.

4.59 *Exemple.* Il peut y avoir des polynômes irréductibles de degré supérieur à 1. Par exemple, le polynôme $X^2 + 1$, en tant qu'élément de $\mathbb{R}[X]$, est irréductible. Pour le prouver, raisonnons par contradiction : supposons que l'on ait $X^2 + 1 = PQ$ avec P et Q non constants. Alors en raisonnant sur les degrés on voit que P et Q doivent être de degré 1, de plus leur coefficient dominant doit être 1, donc on a $P = X + a$ et $Q = X + b$ pour deux réels a et b. Mais alors on a $X^2 + 1 = (X + a)(X + b) = X^2 + (a + b)X + ab$ d'où on déduit, en identifiant les coefficients, que $a + b = 0$ et $ab = 1$. Or $a + b = 0$ implique $b = -a$ donc $ab = -a^2$, et il n'y a pas de réel a tel que $a^2 = -1$.

4.60 *Exemple.* Le polynôme $X^2 + 1$, en tant qu'élément de $\mathbb{C}[X]$, n'est pas irréductible : on a $X^2 + 1 = (X + i)(X - i)$ puisque $i^2 = -1$. En fait, on peut prouver que dans $\mathbb{C}[X]$ les seuls polynômes irréductibles sont les polynômes de degré 1 (mais c'est un peu difficile).

4.61 *Exemple.* Dans $\mathbb{Q}[X]$, il y a des polynômes irréductibles de degrés quelconques. Par exemple, pour tout n, le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$. La démonstration de ce résultat est l'objet des exercices 28 et 29 de la feuille d'exercices.

4.62 **Théorème.** *Tout polynôme non nul $Q \in \mathbb{K}[X]$ se décompose en un produit fini $Q = \lambda P_1 \cdots P_n$ où $\lambda \in \mathbb{K}$ et où $P_1, \ldots, P_n$ sont des polynômes irréductibles unitaires. De plus cette décomposition est unique à permutation près de la famille $P_1, \ldots, P_n$.*

Démonstration. On commence par démontrer l'existence de la décomposition, par récurrence forte sur le degré de Q. Si Q est irréductible, il n'y a rien à démontrer. Sinon il existe deux polynômes A et B tels que $Q = AB$, $\deg(A) < \deg(Q)$ et $\deg(B) < \deg(Q)$. Par hypothèse de récurrence appliquée à A il existe une décomposition $A = \lambda P_1 \cdots P_m$ et par hypothèse de récurrence appliquée à B il existe une décomposition $B = \mu P'_1 \cdots P'_n$, d'où on déduit $Q = AB = (\lambda\mu) P_1 \cdots P_m P'_1 \cdots P'_n$.

Prouvons maintenant l'unicité de la décomposition. Pour cela on montre que pour toute égalité $\lambda P_1 \cdots P_n = \mu P'_1 \cdots P'_{n'}$ où les P_i et P'_j sont irréductibles, on a $\lambda = \mu$, $n' = n$

et la famille $P'_1, \dots, P'_{n'}$ est une permutation de la famille $P_1, \dots, P_n$. On procède pour cela par récurrence sur n.

Dans le cas initial $n = 0$ l'égalité devient $\lambda = \mu P'_1 \cdots P'_{n'}$, or les P'_i sont irréductibles donc non constants. La seule façon que le produit $\mu P'_1 \cdots P'_{n'}$ soit constant est donc d'avoir $n' = 0$ et par suite $\lambda = \mu$, ce qui est le résultat voulu.

Pour l'étape de récurrence, considérons une égalité $\lambda P_1 \cdots P_{n+1} = \mu P'_1 \cdots P'_{n'}$. Il est clair que P_{n+1} divise le membre gauche de l'égalité, donc il divise aussi le membre droit. Comme ce produit de polynôme n'est pas constant (puisqu'un polynôme irréductible n'est pas constant), on a $n' \geq 1$. En appliquant n' fois la généralisation du lemme de Gauss prouvée plus haut, on déduit qu'il existe un i tel que P_{n+1} divise P'_i. Quitte à permuter la famille $P'_1, \dots, P'_{n'}$, on peut supposer que $i = n'$. Par définition des polynômes irréductibles, si P_{n+1} divise $P'_{n'}$ alors $P'_{n'}$ s'écrit αP_{n+1} pour un certain $\alpha \in \mathbb{K}$ puisque P_{n+1} n'est pas constant. Comme P_{n+1} et $P'_{n'}$ sont supposés unitaires tous les deux, on a $\alpha = 1$ et donc $P_{n+1} = P'_{n'}$. En déduit $\lambda P_1 \cdots P_n = \mu P'_1 \cdots P'_{n'-1}$ et on conclut par hypothèse de récurrence. □

4.63 *Exemple.* Considérons dans $\mathbb{R}[X]$ le polynôme $P = X^4 + 2X^3 - X - 2$. On peut remarquer que $P(1) = 0$ donc on peut en déduire que P est divisible par $X - 1$ (on reviendra sur ce phénomène dans la suite). En effet, en posant la division on obtient $P = (X - 1)(X^3 + 3X^2 + 3X + 2)$. En explorant un peu on constate que le polynôme $X^3 + 3X^2 + 3X + 2$ s'annule -2 et donc qu'il est divisible par $X + 2$ et la division donne $X^3 + 3X^2 + 3X + 2 = (X + 2)(X^2 + X + 1)$. Enfin, le polynôme $X^2 + X + 1$ est irréductible (dans $\mathbb{R}[X]$), il suffit pour s'en convaincre de supposer qu'il peut se factoriser, alors ce serait sous la forme $(X - a)(X - b)$ et il s'annulerait en a et en b, or $X^2 + X + 1$ ne s'annule pas sur $\mathbb{R}$ parce que son discriminant est négatif. La décomposition de P en irréductibles dans $\mathbb{R}[X]$ est donc $P = (X - 1)(X + 2)(X^2 + X + 1)$.

4.64 La présence du coefficient λ rend cet énoncé un peu plus compliqué que celui de la décomposition en facteurs premiers dans le cas des entiers. On peut déduire du théorème que tout polynôme non constant est produit d'une famille finie de polynômes irréductibles, mais cette décomposition n'est plus unique : on passe d'une décomposition à une autre en changeant l'ordre des facteurs et en appliquant éventuellement un coefficient à chaque terme.

4.4 Racines

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

4.66 **Proposition.** *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. La valeur a est racine de P si et seulement si le polynôme $X - a$ divise P.*

Démonstration. Quel que soit P, par division euclidienne, il existe un polynôme Q et une constante b tels que $P = (X - a)Q + b$, puisqu'un polynôme de degré strictement inférieur à 1 est une constante. On observe alors :

- Si a est racine de P alors $P(a) = 0$ donc $(a - a)Q(a) + b = 0$ or $(a - a)Q(a) + b = 0Q(a) + b = 0 + b = b$ donc $b = 0$, par conséquent $X - a$ divise P.
- Si $X - a$ divise P alors $b = 0$ et $P = (X - a)Q$ donc $P(a) = (a - a)Q(a) = 0$. □

4.67 **Corollaire.** *Tout polynôme de $\mathbb{R}[X]$ de degré impair autre que 1 est réductible.*

Démonstration. Soit P un tel polynôme. Alors son terme dominant s'écrit aX^d avec d impair et a non nul. En étudiant la fonction polynomiale $P_{\mathbb{R}}$, on observe que
— si $a > 0$ alors $\lim_{x\to+\infty} P_{\mathbb{R}}(x) = +\infty$ et $\lim_{x\to-\infty} P_{\mathbb{R}}(x) = -\infty$,
— si $a < 0$ alors $\lim_{x\to+\infty} P_{\mathbb{R}}(x) = -\infty$ et $\lim_{x\to-\infty} P_{\mathbb{R}}(x) = +\infty$,
dans les deux cas $P_{\mathbb{R}}$ prend des valeurs positives et des valeurs négatives, par le théorème des valeurs intermédiaires ont en déduit que la fonction $P_{\mathbb{R}}$ s'annule en au moins un point a de $\mathbb{R}$, ce qui signifie que a est racine de P et donc que P est divisible par $X - a$. □

Ce résultat est un cas de propriété algébrique (un critère de réductibilité pour des polynômes) obtenue à partir d'une propriété fondamentale de l'analyse (le théorème des valeurs intermédiaires). Il est en fait assez naturel qu'il y ait besoin d'avoir recours à l'analyse pour obtenir ce résultat puisque c'est précisément le sujet de l'analyse réelle que d'étudier les propriétés de l'ensemble des réels. On retrouvera ce phénomène avec le théorème de d'Alembert qui est son analogue dans $\mathbb{C}$ et établit que tout polynôme non constant de $\mathbb{C}[X]$ a une racine.

4.68 **Théorème.** *Un polynôme non nul de degré n a au plus n racines.*

Démonstration. On montre par récurrence sur n que si P n'est pas nul et admet n racines distinctes alors $\deg(P) \geq n$, ce qui implique le théorème. Pour le cas initial, le fait que P ne soit pas nul garantit que son degré n'est pas $-\infty$ donc que $\deg(P) \geq 0$. Pour l'étape de récurrence, supposons que le résultat soit établi pour un certain n et considérons un polynôme P et une famille $a_1, \ldots, a_{n+1}$ de racines distinctes de P. Par la proposition 4.66, on a donc que $X - a_{n+1}$ divise P. □

4.69 **Corollaire.** *Soient $P, Q \in \mathbb{K}[X]$ deux polynômes. Si les fonctions polynomiales $P_{\mathbb{K}}$ et $Q_{\mathbb{K}}$ sont égales et si $\mathbb{K}$ est infini alors $P = Q$.*

Démonstration. Par hypothèse la fonction polynomiale $(P - Q)_{\mathbb{K}} = P_{\mathbb{K}} - Q_{\mathbb{K}}$ est donc nulle en tout point de $\mathbb{K}$. Cela signifie que tous les éléments de $\mathbb{K}$ sont racines de $P - Q$. Supposons alors que $P - Q$ n'est pas le polynôme nul. Il a donc un degré $d \geq 0$. Comme $\mathbb{K}$ est infini, on peut y trouver $d + 1$ éléments distincts. On a donc un polynôme de degré d qui a au moins $d + 1$ racines. Ceci contredit le théorème 4.68. Par conséquent $P - Q$ est le polynôme nul et $P = Q$. □

4.70 **Définition (multiplicité d'une racine).** Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit a un élément de $\mathbb{K}$. La *multiplicité* de a comme racine de P est le plus grand entier n tel que $(X - a)^n$ divise P.

Une racine de multiplicité 1 est appelée *racine simple*, un racine de multiplicité 2 est appelée *racine double*, et ainsi de suite.

4.71 Il est clair que si a n'est pas racine de P alors sa multiplicité comme racine de P est 0, puisque sinon $X - a$ diviserait P. D'autre part, si pour un n donné $(X - a)^n$ divise P alors on a directement que n est majoré par le degré de P, puisque P est supposé non nul. Par conséquent, la multiplicité est toujours bien définie et majorée par le degré du polynôme.

4.72 *Exemple.* Prenons $P = X^3 - 4X^2 + 5X - 2$. On observe que 1 est racine de P puisque $P(1) = 1 - 4 + 5 - 2 = 0$. Si on divise P par $X - 1$ on obtient $X^2 - 3X + 2$ et on observe que 1 est aussi racine de ce polynôme. Si on divise à nouveau par $X - 1$ on obtient $X - 2$, dont 1 n'est pas racine. Ainsi 1 est racine double de P (et on observe aussi que 2 est racine simple).

4.73 **Proposition.** *Soit $P \in \mathbb{K}[X]$ un polynôme et soit a un élément de $\mathbb{K}$. Alors a est racine de P de multiplicité n si et seulement si P s'écrit $(X - a)^n Q$ pour un certain polynôme Q tel que $Q(a) \neq 0$.*

4.74 En généralisant l'argument donné pour le théorème 4.68, on peut observer que la somme des multiplicités des racines d'un polynôme non nul est toujours majorée par le degré de ce polynôme.

4.75 **Définition (polynôme scindé).** Un polyôme est *scindé* s'il peut s'écrire comme produit de polynômes de degré 1.

4.76 *Exemple.* Un polynôme comme $(X - 1)(X + 2)^3(2X - 5)$ est scindé.

4.77 *Exemple.* Dans $\mathbb{R}[X]$, le polynôme $X^2 + 1$ n'est pas scindé. En effet, il n'a pas de racine et ne peut donc pas s'écrire comme produit de polynômes de degré 1 (lesquels ont toujours une racine).

4.78 *Exemple.* Considéré comme élément de $\mathbb{C}[X]$, ce même polynôme $X^2 + 1$ est scindé, en effet, on $X^2 + 1 = (X - i)(X + i)$.

4.79 Le fait d'être scindé est lié à la décomposition en produit d'irréductibles. En effet, on peut observer qu'un polynôme est scindé si et seulement si sa décomposition en produit d'irréductibles ne contient que des facteurs de degré 1.

4.5 Le théorème fondamental de l'algèbre

Le corps $\mathbb{C}$ des nombres complexes a été inventé dans le but de résoudre des équations polynomiales que l'on ne pouvait pas résoudre dans les nombres réels. Le phénomène n'est pas propre à $\mathbb{C}$, en effet :

- l'équation $x + 2 = 0$ n'a pas de solution dans $\mathbb{N}$ mais elle en a une dans $\mathbb{Z}$,
- l'équation $2x - 1 = 0$ n'a pas de solution dans $\mathbb{Z}$ mais elle en a une dans $\mathbb{Q}$,
- l'équation $x^2 - 2 = 0$ n'a pas de solution dans $\mathbb{Q}$ (on sait que $\sqrt{2}$ est irrationnel) mais elle en a deux dans $\mathbb{R}$,
- l'équation $x^2 + 1 = 0$ n'a pas de solution dans $\mathbb{R}$ (puisqu'un carré est toujours positif) mais elle en a deux dans $\mathbb{C}$.

Le miracle est que ce processus s'arrête là : toute équation polynomiale $P(x) = 0$ a au moins une solution dans $\mathbb{C}$ (sauf bien sûr si P est constant). Techniquement, on dit que $\mathbb{C}$ est *algébriquement clos*. Ce fait figure parmi les énoncés les plus importants des mathématiques, ce qui lui vaut d'être parfois qualifié de *théorème fondamental de l'algèbre*. Toutes les démonstrations connues de ce résultat d'algèbre reposent sur la complétude topologie de $\mathbb{C}$, qui est une notion fondamentale d'analyse (déjà évoquée dans la section 1.4 du chapitre sur les suites).

Dans la suite, on donne une démonstration de ce théorème. Elle utilise quelques éléments liés à la structure de $\mathbb{C}$ qui sont très classiques mais n'ont pas été rappelés dans ce

cours. Il est tout-à-fait acceptable de passer cette démonstration en première lecture, en revanche le résultat du théorème est à connaître, ainsi que les conséquences qui suivent.

4.80 **Théorème (d'Alembert-Gauss).** *Tout polynôme de $\mathbb{C}[X]$ non constant a une racine.*

Démonstration. Soit $P \in \mathbb{C}[X]$ un polynôme non constant, soit d son degré (donc $d \geq 1$). Notons $P = a_0 + a_1X + \cdots + a_dX^d$, comme d est le dergé de P on a $a_d \neq 0$. Pour tout complexe z on nul on a

$$\begin{aligned} |P(z)| &= \left|a_dz^d + \cdots + a_1z + a_0\right| \\ &\geq \left|a_dz^d\right| - \left|a_{d-1}z^{d-1} + \cdots + a_1z + a_0\right| \\ &= \left|z^d\right| \left(|a_d| - \left|a_{d-1}z^{-1} + \cdots + a_1z^{-d+1} + a_0z^-d\right|\right). \end{aligned}$$

Quand $|z|$ tend vers l'infini, le terme droit de la soustraction tend vers 0 (puisque les puissances négatives de z tendent vers 0) donc $|P(z)|/\left|z^d\right|$ tend vers $|a_d|$ qui est strictement positif, ainsi $|P(z)|$ tend vers l'infini. Il existe donc un réel $R > 0$ tel que pour tout $|z| > R$ on a $|P(z)| > |P(0)|$. Par conséquent, $|P(z)|$ a un minimum et il est atteint pour un certain complexe α tel que $|\alpha| \leq R$. On va maintenant montrer que ce minimum est 0, ce qui permettra de conclure que α est racine de P.

Quitte à considérer le polynôme $P(X + \alpha)$, on peut considérer que l'on a $\alpha = 0$ sans perte de généralité. On veut donc montrer que $P(0) = 0$. Soit k le plus petit entier tel que $k \leq 1$ et $a_k \neq 0$. Quitte à considérer le polynôme P/a_k, on peut considérer que l'on a $a_k = 1$ sans perte de généralité. On a donc

$$P(X) = a_0 + X^k + a_{k+1}X^{k+1} + \cdots + a_dX^d.$$

Soit w un complexe tel que $w^k = -a_0$ (un tel nombre existe forcément, par exemple si on écrit a_0 en forme exponentielle $\lambda e^{i\theta}$, il suffit de considérer $\lambda^{1/k}e^{i(\pi-\theta/k)}$). Pour tout réel $t \in [0, 1]$ on a alors

$$\begin{aligned} P(tw) &= a_0 + (tw)^k + a_{k+1}(tw)^{k+1} + \cdots + a_d(tw)^d \\ &= a_0 + t^k(-a_0) + a_{k+1}(tw)^{k+1} + \cdots + a_d(tw)^d \\ &= a_0(1 - t^k) + a_{k+1}(tw)^{k+1} + \cdots + a_d(tw)^d \\ &= a_0(1 - t^k) + t^kQ(t) \quad \text{avec } Q(X) = a_{k+1}w^{k+1}X + \cdots + a_dw^dX^{d-k}. \end{aligned}$$

Comme $a_0 = P(0)$ et $|P(0)|$ est le minimum de $|P(z)|$ par construction, on en déduit les inégalités suivantes pour tout $t \in [0, 1]$:

$$\begin{aligned} |P(0)| \leq |P(tw)| &\leq |P(0)|(1 - t^k) + t^k|Q(t)| \\ |P(0)| \leq |P(tw)| &\leq |P(0)| + t^k(|Q(t)| - |P(0)|) \\ 0 \leq |P(tw)| - |P(0)| &\leq t^k(|Q(t)| - |P(0)|) \end{aligned}$$

donc pour tout $t \in]0, 1]$ on a $|Q(t)| \geq |P(0)|$. Comme Q n'a pas de terme constant on a $\lim_{t\to 0} Q(t) = 0$ donc $|Q(t)|$ tend vers 0. Par conséquent on doit avoir $P(0) = 0$ et le théorème est démontré. □

4.81 **Corollaire.** *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont exactement ceux de degré* 1*.*

Démonstration. Les polynômes de degré 1 sont forcément irréductibles (c'est l'exemple 4.58 après la définition des irreductibles). Le théorème de d'Alembert-Gauss dit que tout polynôme non constant de $\mathbb{C}[X]$ admet une racine donc est divisible par un polynôme de degré 1, dans le cas d'un polynôme P de degré au moins 2 cela implique que P est réductible. □

4.82 **Corollaire.** *Tout polynôme de* $\mathbb{C}[X]$ *est scindé.*

Démonstration. Il suffit de considérer une décomposition en produit d'irréductibles et d'appliquer le corollaire précédent. □

4.83 **Corollaire.** *Dans* $\mathbb{R}[X]$*, les polynômes irréductibles sont exactement*
- *les polynômes de degré* 1*,*
- *les polynômes de degré* 2 *qui n'ont pas de racine.*

Démonstration. Il est clair que les polynômes en question sont tous irréductibles. Réciproquement, considérons un polynôme $P \in \mathbb{R}[X]$ et supposons-le irréductible. Si P est de degré 1 on est dans le premier cas, on suppose donc maintenant que $\deg(P) \geq 2$. On peut considérer P comme un élément de $\mathbb{C}[X]$ et dans ce cas on sait quer P admet au moins une racine α. Comme P n'a pas de racine réelle (puisqu'il est irréductible et de degré au moins 2) on en déduit que α est élément de $\mathbb{C} \setminus \mathbb{R}$. Observons que l'opératino de conjugaison dans $\mathbb{C}$ préserve l'addition et la multiplication, de plus les coefficients de P sont réels donc égaux à leurs conjugués, donc on a $P(\bar{\alpha}) = \overline{P(\alpha)} = 0$ et $\bar{\alpha}$ est aussi racine de P, or $\alpha \neq \bar{\alpha}$ donc P est divisible par $(X-\alpha)(X-\bar{\alpha})$. D'autre part on a $(X-\alpha)(X-\bar{\alpha}) = X^2-(\alpha+\bar{\alpha})X+\alpha\bar{\alpha}$ et ce plynôme de degré 2 est à coefficients réels puisque d'une part $\alpha+\bar{\alpha}$ est le doubble de la partie réelle de α et d'autre part $\alpha\bar{\alpha}$ est le carré du module de α. Ainsi P est divisible par un polynôme de $\mathbb{R}[X]$ de degré 2, or P est supposé irréductible donc P est de degré 2. □