Université de Provence 2009–2010

Mathématiques Générales 1 - Parcours PEI

POLYNÔMES.

Dans tout ce chapitre, $(A, +, \cdot)$ est un anneau commutatif unitaire.

1 Polynômes à une variable.

1.1 Définition.

Définition. On appelle *polynôme à une variable X et à coefficients a_k dans A pour $k \in \{0, 1, \dots n\}$* une expression de la forme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n.$$

On note $A[X]$ l'ensemble de polynômes à coefficients dans A.

Si un coefficient a_k est nul, le terme correspondant $a_k X^k$ (ou *monôme*) peut ne pas s'écrire. On supposera donc en général que le dernier coefficient a_n n'est pas nul, sauf si tous les coefficients sont nuls auquel cas le polynôme est appelé *polynôme nul* ou *zéro* et se note $P = 0$.

Exemple. $1 + 0X + (-1)X^2 + 0X^3 + 0X^4 + 0X^5 + 0X^6 + 1X^7$ s'écrit plus simplement $1 - X^2 + X^7$.

Deux polynômes non nuls

$$P = a_0 + a_1 X + \cdots a_n X^n$$

$$Q = b_0 + b_1 X + \cdots + b_m X^m$$

sont égaux si $m = n$ et $a_k = b_k$ pour $k \in \{0, \dots, n\}$. On écrit alors $P = Q$.

1.2 Degré d'un polynôme.

Définition. Si $P = a_0 + a_1 + \cdots a_n X^n$ avec $a_n \neq 0$ est un polynôme non nul, n s'appelle le *degré du polynôme* P et se note $d^\circ P$ ou deg P.

Si de plus $a_n = 1$, on dit que P est *unitaire*.

On note $A_n[X]$ l'ensemble de polynômes à coefficients dans A de degré inférieur ou égal à n.

En particulier, deux polynômes sont égaux si et seulement si ils ont même degré et mêmes coefficients.

Le polynôme nul n'a pas de degré.

Le polynôme nul et les polynômes de degré zéro sont appelés *les polynômes constants*.

1.3 Somme de deux polynômes.

Définition. Soient les deux polynômes

$$P = a_0 + a_1X + \cdots a_nX^n$$

$$Q = b_0 + b_1X + \cdots + b_mX^m$$

Si $n = m$, on appelle *somme* de P et Q et on note $P + Q$ le polynôme

$$P + Q = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n.$$

Cette définition s'étend au cas $m < n$ à condition d'écrire Q sous la forme

$$Q = b_0 + b_1X + \cdots + b_mX^m + 0X^{m+1} + \cdots + 0X^n.$$

On procède de même pour P si $n < m$.

Exemple. Si $P = 1 - X^2 + X^7$ et $Q = 2X + 3X^2 + X^5 + X^9$, alors $P + Q = 1 + 2X + 2X^2 + X^5 + X^7 + X^9$.

La proposition suivante est immédiate.

Proposition. $(A[X], +)$ *est un groupe commutatif. Enfin, pour tout* $n \in \mathbb{N}$, $(A_n[X], +)$ *est un groupe commutatif.*

Preuve. En effet, $A[X]$ est non vide, l'addition est associative et est une loi de composition interne sur $A[X]$. Le polyôme nul est l'élément neutre, et le symétrique d'un polynôme P pour l'addition est le polynôme $-P$ obtenu à partir de P en changeant le signe de tous les coefficients de P. Ceci prouve bien que $(A[X], +)$ est un groupe.

$A_n[X]$ est stable pour l'addition car le degré de la somme de deux polynômes est inférieur ou égal au plus grand des degrés des polynômes. $0 \in A_n[X]$ et si $P \in A_n[X]$, $(-P) \in A_n[X]$ aussi. Ceci prouve bien que $(A_n[X], +)$ est un sous-groupe de $(A[X], +)$ donc que $(A_n[X], +)$ est un groupe. □

Remarque. On remarque que, pour deux polynômes P et Q, si $P + Q \neq 0$, on a

$$d^\circ(P + Q) \leq \max(d^\circ P, d^\circ Q).$$

Il n'y a pas égalité en général. En effet, si $P = 2 + X^2$ et $Q = X - X^2$, alors P et Q sont tous les deux de degré 2, et $P + Q = 2 + X$ est de degré 1.

1.4 Produit de deux polynômes.

Définition. Soient les deux polynômes

$$P = a_0 + a_1 X + \cdots a_n X^n$$

$$Q = b_0 + b_1 X + \cdots + b_m X^m.$$

On appelle *produit des polynômes P et Q* le polynôme noté PQ défini par

$$PQ = \sum_{k=0}^{n} \sum_{\ell=0}^{m} a_k b_\ell X^{k+\ell}.$$

En pratique, pour calculer le produit de deux polynômes, on développe et on ordonne les puissances. Par exemple, si $P = 1 + X + X^2$ et $Q = 1 - X$, on a

$$PQ = (1+X+X^2)(1-X) = (1+X+X^2)-(1+X+X^2)X = (1+X+X^2)-(X+X^2+X^3) = 1+X+X^2-X-X^2-X^3$$

$$= 1 - X^3.$$

En particulier, si P est de degré n et Q de degré m, on a $a_n \neq 0$ et $b_m \neq 0$. Le coefficient devant X^{n+m} dans PQ est alors $a_n b_m$, et celui-ci est non nul si l'anneau A est intègre. Enfin tous les termes de degré strictement supérieur à $n + m$ sont nuls.

On en déduit que si l'anneau A est intègre, le degré du produit de deux polynômes est la somme des degrés.

En d'autre termes, si $P \neq 0$ et $Q \neq 0$, $d^\circ(PQ) = d^\circ P + d^\circ Q$.

On en déduit le théorème suivant :

Théorème. *Si $(A, +, \cdot)$ est un anneau, $(A[X], +, \times)$ est aussi un anneau. De plus, si A est intègre, alors $A[X]$ l'est aussi.*

1.5 Racines d'un polynôme

Définition. Soit un polynôme

$$P = a_0 + a_1 X + \cdots a_n X^n$$

et soit $a \in A$. On note $P(a)$ l'élément de A défini par

$$P(a) = a_0 + a_1 \times a + a_2 \times a^2 + \cdots + a_n \times a^n.$$

On dit que a est *racine de P* si et seulement si $P(a) = 0$.

Le théorème suivant est fondamental en Analyse (il a été énoncé par d'Alembert, et prouvé par Gauss), et nous l'admettrons car sa preuve est très difficile :

Théorème (dit "de d'Alembert"). *Tout polynôme $P \in \mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.*

2 Divisibilité

2.1 Division euclidienne.

Définition. Soient A un anneau et P, Q deux polynômes dans $A[X]$. On dit que P *divise* Q dans $A[X]$ ou que Q est divisible par R et on note $P|Q$ si et seulement si il existe $R \in A[X]$ tel que $Q = PR$.

Théorème. *Soit K le corps $\mathbb{R}$ ou $\mathbb{C}$. Soit $B \in K[X]$ de degré supérieur ou égal à 1. Alors, pour tout $A \in K[X]$, il existe un unique couple $(Q, R) \in K[X]^2$ tel que $A = BQ + R$ et $d^\circ R < d^\circ B$.*

Preuve. Prouvons d'abord l'existence de (Q, R) vérifiant les conditions proposées.

On raisonne par récurrence sur le degré n de A. Si $n < d^\circ B$, alors $A = B \times 0 + A$ donne une décomposition souhaitée car $R = A$ et $n < d^\circ B$.

Supposons que, pour $n \in \mathbb{N}$, $n \geq d^\circ B - 1$ et pour tout polynôme A de degré inférieur ou égal à n, on puisse trouver $(Q, R) \in K[X]^2$ tel que $A = BQ + R$ avec $d^\circ R < d^\circ B$. Soit A un polynôme de degré $n+1$. Si $A = a_{n+1}X^{n+1} + \cdots + a_0$ et $B = b_m X^m + \cdots + b_0$, alors

$$A = B\left(\frac{a_{n+1}}{b_m}X^{n+1-m}\right) + \left(A - B\left(\frac{a_{n+1}}{b_m}X^{n+1-m}\right)\right)$$

et où le degré du polynôme $A - B\left(\frac{a_{n+1}}{b_m}X^{n+1-m}\right)$ est inférieur ou égal à n. D'après l'hypothèse de récurrence, on a l'existence de $(Q, R) \in K[X]^2$ tel que $d^\circ R < d^\circ B$ et

$$A - B\left(\frac{a_{n+1}}{b_m}X^{n+1-m}\right) = BQ + R.$$

On a alors

$$A = B\left(\frac{a_{n+1}}{b_m}X^{n+1-m} + Q\right) + R$$

et l'hypothèse est vraie au rang $n+1$. Ceci prouve l'existence de la décomposition par récurrence sur le degré de A.

Montrons l'unicité. Supposons que l'on ait $A = BQ + R = BQ' + R'$ où $d^\circ R < d^\circ B$ et $d^\circ R' < d^\circ B$. On a alors $B(Q - Q') = R' - R$. Si $Q - Q' \neq 0$, alors $d^\circ B + d^\circ(Q - Q') = d^\circ(R - R')$. Or $d^(R' - R) < d^\circ B$. Cecic entraîne donc que $d^\circ(Q - Q') < 0$, ce qui est absurde. Donc $Q = Q'$ et par suite $R = R'$. □

Corollaire. *Soit K le corps $\mathbb{R}$ ou $\mathbb{C}$ et $a \in K$. Un polynôme A est divisible par $X - a$ (*i.e. *il existe $P \in K[X]$ tel que $A = (X - a)P$) si et seulement si $A(a) = 0$.*

Preuve. En effet, si $A = (X - a)P$, alors $A(a) = 0 \times P(a) = 0$.

Réciproquement, supposons que $A(a) = 0$. D'après le théorème, il existe Q et R tels que $A = (X - a)Q + R$ avec $d^\circ R < d^\circ(X - a) = 1$. On en déduit que R est un polynôme constant. Or $A(a) = 0$. On en déduit que $R(a) = 0$ et donc que le polynôme constant R est le polynôme nul. □

En pratique, la division euclidienne se fait de la manière suivante :

$$\begin{array}{cccccccc}
X^5 & & +X^3 & +2X^2 & +X & +1 & & X^3 \quad +X^2 \quad +1 \\
-X^5 & -X^4 & & -X^2 & & & & \\
 & -X^4 & +X^3 & +X^2 & +X & +1 & & X^2 \quad -X \quad +2 \\
 & +X^4 & +X^3 & & +X & & & \\
 & & 2X^3 & +X^2 & +2X & +1 & & \\
 & & -2X^3 & -2X^2 & & -2 & & \\
 & & & -X^2 & +2X & -1 & &
\end{array}$$

et donc

$$X^5 + X^3 + 2X^2 + X + 1 = (X^3 + X^2 + 1)(X^2 - X + 2) + (-X^2 + 2X - 1).$$

2.2 Polynômes irréductibles de $K[X]$ où $K = \mathbb{R}$ ou $\mathbb{C}$.

Définition. Soit $K = \mathbb{R}$ ou $\mathbb{C}$ et $P \in K[X]$. On dit que P est *irréductible* si et seulement si P n'est pas constant et on ne peut pas écrire $P = QR$ avec $Q, R \in K[X]$ et $d^\circ P \geq 1$ et $d^\circ Q \geq 1$.

Exemples. $P = X^2 - 3X + 2$ n'est pas irréductible dans $\mathbb{R}[X]$ car $P = (X - 2)(X - 1)$ est le produit de deux polynômes de degré 1.

$P = X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$. En effet, si P n'était pas irréductible, il existerait Q et R de degrés ≥ 1 tels que $P = QR$. Comme P est de degré 2, on en déduit que $d^\circ Q = d^\circ R = 1$, donc que $Q = aX + b$ et $R = a'X + b'$ avec $a \neq 0 \neq a'$. En particulier, P admettrait au moins une racine réelle, ce qui n'est pas le cas car le discriminant de P est strictement négatif.

Par contre, $P = X^2 + X + 1 = (X - j)(X - j^2)$, avec $j = e^{\frac{2i\pi}{3}}$, n'est pas irréductible dans $\mathbb{C}[X]$.

Théorème. *Les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Preuve. En effet, si un polynôme $P \in \mathbb{C}[X]$ est de degré supérieur ou égal à 2, P admet au moins une racine complexe a, et donc P est divisible par $X - a$. On en déduit qu'il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - a)Q$, ce qui entraîne que P n'est pas irréductible.

Réciproquement, si un polynôme P n'est pas irréductible, on peut écrire $P = QR$ avec $d^\circ Q \geq 1$ et $d^\circ R \geq 1$. On en déduit que $d^\circ P \geq 1 + 1 = 2$.

En conclusion, on a bien prouvé que les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1. □

Théorème. *Les seuls polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 ou bien les polynômes de degré 2 dont le discriminant est strictement négatif.*

Preuve. Si P est un polynôme de degré 1, il est irréductible. Si P est un polynôme de degré 2 dont le discriminant est strictement négatif, alors P est irréductible. En effet, si $P = QR$ avec Q et R dans $\mathbb{R}[X]$ et $d^\circ Q \geq 1$ et $d^\circ R \geq 1$, alors nécessairement P admet au moins une racine réelle, ce qui est impossible.

Si maintenant P est un polynôme de degré 2 à discriminant positif ou nul, il admet au moins une racine réelle a. Donc P est divisible par $X - a$, ce qui entraîne que P n'est pas irréductible.

Si maintenant P est un polynôme dans $\mathbb{R}[X]$ de degré ≥ 3, soit P admet une racine réelle, auquel cas P n'est pas irréductible. Sinon, P admet une racine complexe α. Comme P est à coefficients réels, on a $P(\overline{\alpha}) = 0$ donc $Q = (X - \alpha)(X - \overline{\alpha})$ divise P. Or $Q = X^2 - (\alpha + \overline{\alpha})X + |\alpha|^2 \in \mathbb{R}[X]$ et $P = QR$ où $R \in \mathbb{R}[X]$ et $d^\circ R \geq 1$. On en déduit que P n'est pas irréductible. □

2.3 Polynômes premiers entre eux.

K est le corps $\mathbb{R}$ ou $\mathbb{C}$.

Définition. Soient P et Q deux polynômes dans $K[X]$. On dit que P et Q sont *premiers entre eux* si et seulement si les seuls polynômes qui divisent à la fois P et à la fois Q sont constants. En d'autres termes, ($R|P$ et $R|Q$) $\Rightarrow d^\circ R = 0$.

Nous avons le théorème suivant (admis) :

Théorème (dit de Bezout). *Soient P et Q dans $K[X]$. Alors P et Q sont premiers entre eux si et seulement si il existe A et B dans $K[X]$ tels que $AP + BQ = 1$.*

En pratique, pour si P et Q sont deux polynômes premiers entre eux, pour trouver un couple de polynômes (U, V) tel que $AU + BV$, on utilise l'algorithme dit d'Euclide : on fait la division euclidienne de A par B. On obtient un quotient Q et un reste R. Si le reste est de degré 0, alors on s'arrête. Sinon, on recommence la division euclidienne en remplaant A par B et B par reste. En réitérant ce procédé, on finit par aboutir à un reste de degré 0. Il suffit alors de faire le point sur les identités obtenues en pratiquant les divisions euclidiennes pour aboutir à un couple (U, V) tel que $AU + BV = 1$.

Regardons cet algorithme d'Euclide sur un exemple : si $A = X^5 + 1$ et $B = X^4 + X^2$, alors A et B sont premiers entre eux (leus racines de A sont les racines cinquièmes de -1, tandis que les racines de B sont $0, i, -i$; elles sont donc différentes).

Une division euclidienne de A par B nous donne $X^5 + 1 = (X^4 + X^2)X - X^3 + 1$ (a).

La division euclidienne de $X^4 + X^2$ par $-X^3 + 1$ nous donne $X^4 + X^2 = (-X^3 + 1)(-X) + (X^2 + X)$ (b).

La division euclidienne de $-X^3 + 1$ par $X^2 + X$ nous donne $-X^3 + 1 = (-X + 1)(X^2 + X) - X + 1$ (c).

La division euclidienne de $X^2 + X$ par $-X + 1$ nous donne $X^2 + X = (-X - 2)(-X + 1) + 2$ (d).

La dernière égalité nous donne $1 = \frac{1}{2}(X^2 + X) + \frac{1}{2}(X + 2)(-X + 1)$.

En utilisant l'égalité (c), $-X + 1 = (-X^3 + 1) + (X - 1)(X^2 + X)$, donc

$$1 = \frac{1}{2}(X^2+X)+\frac{1}{2}(X+2)[(-X^3+1)+(X-1)(X^2+X)] = \frac{1}{2}[(X+2)(X-1)+1](X^2+X)+\frac{1}{2}(X+2)(-X^3+1)$$

$$= \frac{1}{2}(X^2 + X - 1)(X^2 + X) + \frac{1}{2}(X + 2)(-X^3 + 1)$$

En utilisant l'égalité (b), $X^2+X=(X^4+X^2)+X(-X^3+1)$, donc

$$1=\frac{1}{2}(X^2+X-1)[(X^4+X^2)+X(-X^3+1)]+\frac{1}{2}(X+2)(-X^3+1)$$

$$=\frac{1}{2}(X^2+X-1)(X^4+X^2)+\frac{1}{2}[(X^2+X-1)X+(X+2)](-X^3+1)$$

$$=\frac{1}{2}(X^2+X-1)(X^4+X^2)+\frac{1}{2}(X^3+X^2+2)(-X^3+1).$$

En utilisant l'égalité (a), $-X^3+1=X^5+1-X(X^4+X^2)$, donc

$$1=\frac{1}{2}(X^2+X-1)(X^4+X^2)+\frac{1}{2}(X^3+X^2+2)[X^5+1-X(X^4+X^2)]$$

$$=\frac{1}{2}[X^2+X-1-(X^3+X^2+2)X](X^4+X^2)+\frac{1}{2}(X^3+X^2+2)(X^5+1)$$

$$=\frac{1}{2}(-X^4-X^3+X^2-X-1)(X^4+X^2)+\frac{1}{2}(X^3+X^2+2)(X^5+1).$$

D'où un couple

$$(U,V)=\left(\frac{1}{2}(X^3+X^2+2),\frac{1}{2}(-X^4-X^3+X^2-X-1)\right).$$