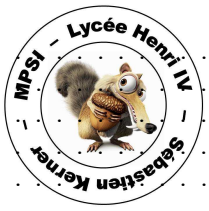
Lycée Henri IV
MPSI

Cours
Durée : 10 h 45

POLYNÔMES

Les énoncés et parties suivis du symbole [✠] ne seront pas traités en cours.



Prérequis

Revoir le chapitre sur :

- les nombres ;
- les sommes ;
- les fonctions.

Dans tout ce chapitre, la lettre K désigne un corps commutatif.

Les lettres $i, j, k, \ell, m, n, p, q$ désignent des entiers naturels (qu'il convient parfois de supposer non nuls).

Les trois lettres AQT signifient « Âne Qui Trotte » et sont utilisées pour désigner une démonstration facile laissée au lecteur.

A. L'anneau des polynômes

A.1. Polynômes, degré et fonctions polynomiales

a) Polynôme formel

L'écriture polynomiale est très présente en mathématiques. On la rencontre évidemment dans les fonctions polynomiales comme $x \longmapsto 5x^4 - 3x^2 + x - 1$, mais aussi avec les polynômes trigonométriques comme $5\cos^4(\theta) - 3\cos^2(\theta) + \cos(\theta) - 1$, ou dans le calcul matriciel où, partant d'une matrice carrée $A \in \mathscr{M}_n(K)$, on peut calculer $5A^4 - 3A^2 + A - I_n$. Et l'on pourrait donner d'autres exemples avec des suites, des fonctions, des variables aléatoires...

Toutes ces écritures ont en commun d'être des sommes de puissances coefficientées. Dans les exemples ci-dessus, les trois quantités sont de la forme $5X^4 - 3X^2 + X - 1$ où X désigne successivement un nombre, une fonction circulaire ou une matrice carrée.

L'objectif de ce premier paragraphe est de mettre en place une notion unificatrice de toutes ces écritures : celle de polynôme formel.

Définition 1

On appelle polynôme sur K une suite $(a_k)_{k\geqslant 0}$ d'éléments de K qui stationne à la valeur 0 à partir d'un certain rang(†). Elle est notée, à l'aide d'une indéterminée X, sous la forme

$$P(X) = \sum_{j\geqslant 0} a_j X^j = a_0 + a_1 X + \cdots + a_n X^n + \cdots$$

Les termes de la suite $(a_k)_{k\geqslant 0}$ sont appelés les coefficients du polynôme $P(X)$.

L'ensemble des polynômes sur K d'indéterminée X est noté $K[X]$. Ainsi, $\mathbb{R}[X]$ désigne l'ensemble des polynômes à coefficients réels et $\mathbb{C}[X]$ celui des polynômes à coefficients complexes.

Le polynôme dont tous les coefficients sont nuls est appelé le polynôme nul et il est noté 0.

Un monôme est un polynôme dont seul un coefficient est non nul. En omettant les termes nuls, un monômes est donc de la forme $a_p X^p$ avec $a_p \neq 0$.

Les polynômes constants sont ceux de la forme $(a_0, 0, —, 0, —)$. Un tel polynôme est noté a_0.

(†) Une suite de $K^{\mathbb{N}}$ qui est nulle à partir d'un certain rang est dite « presque nulle » ou « à support fini » (le support est l'ensemble des rangs k pour lesquels $a_k \neq 0$).

S'il n'y a pas d'ambiguïté sur le nom de l'indéterminée, on note P à la place de $P(X)$.

Dans l'écriture $P = \sum_{j\geqslant 0} a_j X^j$, il est sous-entendu que la suite $(a_j)_{j\geqslant 0}$ stationne à la valeur 0 à partir d'un certain rang. Dans la pratique, on omet l'écriture des termes nuls.

Il faut comprendre que la notion de polynôme formel dépasse le concept de fonction polynomiale. En choisissant de définir les polynômes de manière purement algébrique comme une suite presque nulle d'éléments de K, on insiste sur ce qui fait la substance même d'un polynôme : ses coefficients !

La lettre X, appelée indéterminée, n'est alors qu'un symbole servant à séparer les coefficients. Autrement dit, dans l'écriture $P = a_0 + a_1 X + \cdots + a_n X^n + \cdots$, les symboles verts jouent le même rôle que des séparateurs (virgule ou parenthèse) dans un n-uplet.

En particulier, X n'est pas une variable. Elle ne correspond pas à une valeur de K et n'a d'ailleurs pas à être quantifiée.

Exemples :

- $\mathbb{R}[X]$ contient, par exemple, les polynômes 0, 4, $X + X^2$ et $1 - 3\pi X^{12} + \frac{1}{2}X^{1975}$.
- $\mathbb{C}[X]$ contient les polynômes à coefficients complexes, comme $X^2 + jX + i - 2$, mais aussi tous les polynômes à coefficients réels (i.e. $\mathbb{R}[X] \subset \mathbb{C}[X]$).

Un polynôme n'étant rien d'autre qu'une suite, on dispose immédiatement de l'unicité de son écriture. L'encadré ci-dessous exploite cette unicité.

Identification des coefficients

Par définition, deux polynômes sont égaux si, et seulement si, leurs coefficients le sont rang par rang. En particulier, un polynôme est nul si, et seulement si, tous ses coefficients sont nuls. C'est le principe d'identification des coefficients.

Nous verrons des applications de ce principe d'identification en exercice.

Un polynôme étant une suite à support fini, il existe un rang à partir duquel tous les coefficients sont nuls. L'importance de ce rang motive la définition suivante.

Définition 2

Soit P un polynôme sur K. On appelle degré de $P = \sum_{j\geqslant 0} a_j X^j$, et l'on note $\deg(P)$, l'élément de $\mathbb{N}\cup\{-\infty\}$ défini par

$$\deg(P) = \sup\{j \geqslant 0 : a_j \neq 0\}$$

avec la convention (compatible avec la borne inférieure de $\varnothing$ dans $\overline{\mathbb{R}}$) :

$$\deg(0) = -\infty.$$

Si le polynôme n'est pas nul, le monôme d'exposant $\deg(P)$ et son coefficient sont respectivement appelés monôme dominant et coefficient dominant du polynôme.

Un polynôme non nul est dit unitaire lorsque son coefficient dominant est égal à 1.

Le degré est donc l'exposant du monôme non nul de plus grand exposant.

Si P est un polynôme de degré $n \in \mathbb{N}$, alors on peut omettre l'écriture des monômes dont l'exposant est strictement supérieur au degré. On obtient donc une écriture du type

$$P = a_0 + a_1 X + \cdots + a_n X^n = \sum_{j=0}^{n} a_j X^j,$$

où $a_n \neq 0$ est le coefficient dominant de P et $a_n X^n$ est son monôme dominant. Le monôme X^0 est alors « transparent ».

Exemples :

- Les polynômes de degré nul sont les polynômes constants sauf le polynôme nul.
- $\deg\left(1 - 3\pi X^{12} + \frac{1}{2}X^{1975}\right) = 1975.$

Dans de nombreuses situations (en particulier en algèbre linéaire), on se contente de travailler sur des polynômes dont le degré est majoré. Pour cette raison, on introduit la notation suivante.

Définition 3

L'ensemble des polynômes de degré inférieur ou égal à n est noté $K_n[X]$.

Exemples :

- $K_0[X]$ est l'ensemble des polynômes constants (y compris le polynôme nul).
- $\mathbb{R}_2[X] = \{aX^2 + bX + c : a, b, c \in \mathbb{R}\}$.

b) Fonctions polynomiales

Il est souvent commode de considérer les polynômes non comme des objets algébriques mais comme des fonctions numériques.

Définition 4

On associe à tout polynôme $P = \sum_{j=0}^{n} a_j X^j$ sur K la fonction polynomiale $\widetilde{P}$ définie par

$$\widetilde{P}\left\{\begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & \displaystyle\sum_{j=0}^{n} a_j x^j. \end{array}\right.$$

La fonction polynomiale associée à un polynôme permet d'envisager d'évaluer le polynôme en un élément de K.

Définition 5

Soient P un polynôme sur K et $\alpha \in K$.

On appelle évaluation de P en α l'élément de K, notée $P(\alpha)$, égal à la valeur prise par la fonction $\widetilde{P}$ en α, c'est-à-dire $\widetilde{P}(\alpha)$.

Pour évaluer P en α, on dit que l'on substitue α à X dans P.

Il est courant d'évaluer un polynôme sur K en un élément d'un sur-corps L de K. Ainsi, pour un polynôme P sur $\mathbb{Q}$ ou $\mathbb{R}$, il est possible d'évaluer P en n'importe quel nombre complexe α.

Nous verrons plus loin que si K est un corps infini, il existe une correspondance bijective entre l'ensemble des polynômes $K[X]$ et l'ensemble des fonctions polynomiales sur K. C'est pour cette raison que nous identifierons souvent un polynôme P et sa fonction polynomiale $\widetilde{P}$.

Toutefois, cette identification entre polynômes et fonctions polynomiales ne fonctionne pas lorsque K est un corps fini. Par exemple, dans $\mathbb{F}_p[X]$, la fonction polynomiale associée au polynôme $X^p - X$ est l'application nulle en vertu du petit théorème de Fermat. Autrement dit, $X^p - X$ et le polynôme nul ont la même fonction polynomiale associée, alors que ce sont deux polynômes parfaitement distincts.

A.2. Addition et multiplication

Les polynômes sur K étant des suites à coefficients dans K, l'ensemble $K[X]$ est naturellement pourvu de l'addition des suites. On définit également une multiplication sur $K[X]$, qui ne coïncide pas, elle, avec la multiplication des suites mais avec celles des fonctions polynomiales associées.

Définition 6

L'addition des polynômes sur K est définie, pour $P = \sum_{j\geqslant 0} a_j X^j$ et $Q = \sum_{j\geqslant 0} b_j X^j$, par

$$P+Q = \sum_{j\geqslant 0} (a_j + b_j) X^j.$$

La multiplication des polynômes sur K est définie, pour $P = \sum_{j\geqslant 0} a_j X^j$ et $Q = \sum_{j\geqslant 0} b_j X^j$, par

$$PQ = \sum_{j\geqslant 0} \left(\sum_{i=0}^{j} a_i b_{j-i} \right) X^j.$$

■ Il faut justifier que $P+Q$ et PQ sont des polynômes, c'est-à-dire leurs coefficients stationnent à la valeur 0. Pour cela, on va utiliser le fait que $\forall k > \deg(P),\ a_k = 0$ et $\forall k > \deg(Q),\ b_k = 0$.

Cela entraîne que, pour tout $j > \max\{\deg(P); \deg(Q)\}$, on a $a_j + b_j = 0$. Donc $P+Q$ est un polynôme.

Cela implique également que, pour tout $j > \deg(P) + \deg(Q)$, on a

$$\sum_{i=0}^{j} a_i b_{j-i} = \sum_{i=0}^{\deg(P)} a_i \underbrace{b_{j-i}}_{=0} + \sum_{i=\deg(P)+1}^{j} \underbrace{a_i}_{=0} b_{j-i} = 0,$$

où la nullité de b_{j-i}, lorsque $i \in [\![0; \deg(P)]\!]$, est justifiée par le fait que $j - i \geqslant j - \deg(P) > \deg(Q)$. Cela prouve que PQ est un polynôme. ■

On retiendra que l'addition et la multiplication entre polynômes s'effectuent comme celles des fonctions polynomiales associées. Autrement dit, pour tous polynômes P et Q, on a

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q} \qquad \text{et} \qquad \widetilde{PQ} = \widetilde{P} \times \widetilde{Q}.$$

En particulier, pour la multiplication, l'« affreuse » formule donnant les coefficients d'un produit en fonction des coefficients des facteurs, que l'on peut réécrire sous la forme d'un produit de Cauchy :

$$\sum_{i=0}^{j} a_i b_{j-i} = \sum_{\substack{i,i'\geqslant 0 \\ i+i'=j}} a_i b_{i'}$$

n'est rien d'autre que ce que l'on obtient naturellement en développant le produit PQ et en tenant compte de la règle habituelle sur les puissances : $X^i X^j = X^{i+j}$ pour tous $i, j \in \mathbb{N}$.

La multiplication des polynômes définie ci-dessus permet, en particulier, de multiplier un polynôme $P = a_0 + a_1 X + \cdots + a_n X^n$ par un scalaire $\lambda \in K$ (i.e. un polynôme constant), ce qui donne $\lambda P = \lambda a_0 + \lambda a_1 X + \cdots + \lambda a_n X^n$.

Exemples :

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

L'addition et la multiplication sur les polynômes induisent sur $K[X]$ une structure d'anneau.

Proposition 1

$(K[X],+,\times)$ est un anneau commutatif.

■ Commençons par démontrer que $(K[X],+)$ est un sous-groupe de $(K^{\mathbb{N}},+)$. L'addition des polynômes est interne sur $K[X]$ (nous avons déjà justifié que la somme de deux polynômes est un polynôme). La suite nulle est bien sûr un polynôme : le polynôme nul. Enfin, l'opposé d'un polynôme $P=a_0+a_1X+\cdots+a_nX^n$ (vu comme suite) est $-P=(-a_0)+(-a_1)X+\cdots+(-a_n)X^n$ et c'est bien sûr un polynôme.

La multiplication des polynômes est une loi de composition interne (nous avons déjà justifié que le produit de deux polynômes est un polynôme).

Le polynôme constant 1 est clairement un élément neutre pour $\times$.

Pour les autres propriétés, on pose $P=\sum_{j\geqslant 0} a_jX^j$, $Q=\sum_{j\geqslant 0} b_jX^j$ et $R=\sum_{j\geqslant 0} c_jX^j$.

Vérifions que la multiplication est associative. Notons $(ab)_j$ les coefficients de PQ, $(bc)_j$ ceux de QR, $((ab)c)_j$ ceux de $(PQ)R$ et $(a(bc))_j$ ceux de $P(QR)$. Pour tout $\ell\in\mathbb{N}$, on a

$$\begin{aligned}((ab)c)_\ell &= \sum_{k=0}^{\ell}(ab)_kc_{\ell-k} &&= \sum_{k=0}^{\ell}\Big(\sum_{i=0}^{k}a_ib_{k-i}\Big)c_{\ell-k} &&= \sum_{k=0}^{\ell}\sum_{i=0}^{k}a_ib_{k-i}c_{\ell-k}\\ &= \sum_{0\leqslant i\leqslant k\leqslant\ell} a_ib_{k-i}c_{\ell-k} &&= \sum_{i=0}^{\ell}\sum_{k=i}^{\ell}a_ib_{k-i}c_{\ell-k} &&= \sum_{i=0}^{\ell}a_i\sum_{k=i}^{\ell}b_{k-i}c_{\ell-k}\\ &= \sum_{i=0}^{\ell}a_i\sum_{k'=0}^{\ell}b_{k'}c_{\ell-i-k} &&= \sum_{i=0}^{\ell}a_i(bc)_{\ell-i} &&= (a(bc))_\ell,\end{aligned}$$

ce qui justifie que $(PQ)R=P(QR)$.

Vérifions que $\times$ est commutative. Notons $(ab)_j$ les coefficients de PQ et $(ba)_j$ les coefficients de QP. Pour tout $k\in\mathbb{N}$, on a

$$(ab)_j=\sum_{i=0}^{j}a_ib_{j-i}\underset{i'=j-i}{=}\sum_{i'=0}^{j}a_{j-i'}b_{i'}=(ba)_i,$$

ce qui justifie que $PQ=QP$.

Vérifions que la multiplication est distributive sur l'addition. Notons $(a(b+c))_j$ les coefficients de $P(Q+R)$, $(b+c)_j$ ceux de $Q+R$, $(ab)_j$ ceux de PQ et $(ac)_j$ ceux de PR. Pour tout $j\in\mathbb{N}$, on a

$$\begin{aligned}(a(b+c))_j &= \sum_{i=0}^{j}a_i(b+c)_{j-i} &&= \sum_{i=0}^{j}a_i(b_{j-i}+c_{j-i})\\ &= \sum_{i=0}^{j}(a_ib_{j-i}+a_ic_{j-i}) &&= \sum_{i=0}^{j}a_ib_{j-i}+\sum_{i=0}^{j}a_ic_{j-i}\\ &= (ab)_j+(ac)_j\end{aligned}$$

ce qui démontre que $P(Q+R)=PQ+PR$. ■

Toutes les règles opératoires concernant les anneaux commutatifs s'appliquent dans $K[X]$. En particulier, il est tout à fait possible de développer une expression du type $(P+Q)^n$, où P et Q sont deux polynômes, en utilisant la formule du binôme. De même, on peut factoriser P^n-Q^n à l'aide de la formule de Bernoulli.

Jusqu'ici, nous n'avons pas utilisé pleinement le fait que K soit un corps ; nous nous sommes simplement servi des propriétés d'anneau de K. Il est donc tout à fait possible de construire l'ensemble des polynômes à coefficients dans un anneau commutatif A. L'ensemble obtenu, noté évidemment $A[X]$, peut être muni de l'addition et de la multiplication définies ci-avant et le triplet $(A[X],+,\times)$ conserve sa structure d'anneau commutatif. Mézalors, pourquoi ne pas l'avoir dit plus tôt ? D'une part parce que cela dépasse le cadre strict du programme de MPSI, d'autre part parce que cela s'accompagne de certaines subtilités pour toutes les autres propriétés que nous allons énoncer (en particulier si A n'est pas intègre).

Cela dit, il y a de fortes chances que vous rencontriez un jour l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers relatifs…

1 h 15

La proposition suivante décrit les règles opératoires sur le degré.

Proposition 2

Soient P, Q deux polynômes sur K et $\lambda \in K$. On a

(i) $\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}$
avec égalité si, et seulement si, les monômes dominants ne se compensent pas ;

(ii) $\deg(PQ) = \deg(P) + \deg(Q)$;

(iii) $\deg(\lambda P) = \begin{cases} \deg(P) & \text{si } \lambda \neq 0 ; \\ -\infty & \text{si } \lambda = 0. \end{cases}$

■ Si P ou Q est nul, ces propriétés sont claires (le choix $\deg(0) = -\infty$ a justement été fait pour cela...).

Sinon, on note $P = a_0 + a_1 X + \cdots + a_p X^p$ et $Q = b_0 + b_1 X + \cdots + b_q X^q$ et l'on raisonne sur les monômes dominants de la façon suivante :

(i) Le monôme dominant de $P+Q$ est ou bien $a_p X^p$ lorsque $p > q$, ou bien $b_q X^q$ lorsque $p < q$, ou bien $(a_p + b_p)X^p$ lorsque $p = q$ et $a_p + b_p \neq 0$, ou encore un monôme de degré strictement inférieur à p lorsque $p = q$ et $a_p + b_p = 0$. Donc $\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}$ avec égalité si, et seulement si, les monômes dominants ne se compensent pas.

(ii) Le monôme dominant de PQ est $a_p b_q X^{p+q}$ avec $a_p b_q \neq 0$ (car K est intègre). On en déduit bien que $\deg(PQ) = \deg(P) + \deg(Q)$.

(iii) La relation (iii) découle de (ii). ■

L'inégalité (i) implique que l'addition de polynômes de degrés inférieurs ou égaux à n est un polynôme de degré inférieur ou égal à n. Autrement dit, l'addition est une loi de composition interne dans $K_n[X]$.

La règle (ii) sur le degré permet d'énoncer la propriété d'intégrité suivante.

Proposition 3

La multiplication dans $K[X]$ est intègre, c'est-à-dire que si P, Q sont deux polynômes sur K tels que $PQ = 0$, alors on a nécessairement $P = 0$ ou $Q = 0$.

■ Soient $P, Q \in K[X]$ tels que $PQ = 0$. Alors $\deg(PQ) = -\infty$, c'est-à-dire $\deg(P) + \deg(Q) = -\infty$, ce qui donne $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$. Donc $P = 0$ ou $Q = 0$. ■

Il est important de bien noter que l'intégrité n'est pas satisfaite dans l'anneau des fonctions ou des suites. Il n'est donc pas du tout anecdotique que cela soit vrai pour les polynômes.

L'intégrité implique que si l'on a l'égalité polynomiale $PR = QR$ avec $R \neq 0$, alors on peut affirmer que $P = Q$. On dit que l'on peut simplifier par R.

La règle (ii) sur le degré permet en outre de déterminer le sous-groupe des éléments inversibles de l'anneau $K[X]$.

Proposition 4

Le groupe des éléments inversibles de l'anneau $\big(K[X], +, \times\big)$ est l'ensemble des polynômes constants non nuls (c'est-à-dire l'ensemble des polynômes de degré 0).

■ Soit P un polynôme inversible dans $K[X]$. Alors il existe $Q \in K[X]$ tel que $PQ = 1$. D'où $\deg(PQ) = 0$, ce qui donne $\deg(P) + \deg(Q) = 0$. Cela force $\deg(P) = \deg(Q) = 0$ et donc P est bien constant non nul.

Réciproquement, supposons que $\deg(P) = 0$. Alors $P = a_0$ avec $a_0 \in K^*$. D'où P est inversible dans $K[X]$ d'inverse $Q = {a_0}^{-1}$. ■

A.3. Composition

Définition 7

La composition des polynômes sur K est définie, pour $P = \sum_{j\geqslant 0} a_j X^j$ et $Q = \sum_{j\geqslant 0} b_j X^j$, par

$$P \circ Q = \sum_{j\geqslant 0} a_j Q^j.$$

Le polynôme $P \circ Q$ est souvent noté $P(Q)$.

■ Posons $n = \deg(P)$. On a $P \circ Q = a_0 + a_1 Q + \cdots + a_n Q^n$, donc $P \circ Q$ est un polynôme car $K[X]$ est un anneau. ■

On retiendra que la composition entre polynômes s'effectuent comme celles des fonctions polynomiales associées. Autrement dit, pour tous polynômes P et Q, on a

$$\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}.$$

Exemples :

- On a $X \circ P = P$ et $P \circ X = P$.
  L'égalité $P \circ X = P$ justifie que l'on utilise indifféremment les notations P ou $P(X)$.
- Si $P = X^3 + 1$ et $Q = X^2 - 1$, on a

$$P \circ Q = (X^2-1)^3 + 1 = X^6 - 3X^4 + 3X^2 \quad \text{et} \quad Q \circ P = (X^3+1)^2 - 1 = X^6 + 2X^3.$$

La composition des polynômes partage les caractéristiques de la composition des fonctions.

Proposition 5

Dans $K[X]$, la loi $\circ$ est :

(i) distributive sur $+$ et sur $\times$ à droite, c'est-à-dire $(P+Q)\circ R = P\circ R + Q \circ R$ et $(P \times Q)\circ R = (P\circ R) \times (Q \circ R)$, mais pas à gauche ;

(ii) associative ;

(iii) non commutative.

■ On note a_j les coefficients de P et b_j ceux de Q.

(i) On a

$$(P+Q)\circ R = \sum_{j\geqslant 0} (a_j + b_j) R^j = \sum_{j\geqslant 0} a_j R^j + \sum_{j\geqslant 0} b_j R^j = P \circ R + Q \circ R$$

et

$$(P \times Q)\circ R = \sum_{j\geqslant 0} \Big(\sum_{i=0}^{j} a_i b_{j-i} \Big) R^j = \Big(\sum_{j\geqslant 0} a_j R^j \Big) \Big(\sum_{j\geqslant 0} b_j R^j \Big) = (P\circ R) \times (Q \circ R).$$

Pour l'absence de distributivité à gauche, on rend $P = X$, $Q = -X$ et $R = X^2 + 1$ de sorte que, d'une part, $R\circ(P+Q) = 1$ alors que $R\circ P + R \circ Q = 2X^2 + 2$ et, d'autre part, $R\circ(P\times Q) = X^4 + 1$ alors que $(R\circ P) \times (R \circ Q) = (X^2+1)^2$.

(ii) On constate tout d'abord que $(\lambda P)\circ R = \lambda(P \circ R)$ pour tout $\lambda \in K$. En utilisant cette propriété et les résultats de (i), on a alors

$$(P\circ Q)\circ R = \Big(\sum_{j\geqslant 0} a_j Q^j \Big) \circ R = \sum_{j\geqslant 0} (a_j Q^j) \circ R = \sum_{j\geqslant 0} a_j (Q^j \circ R) = \sum_{j\geqslant 0} a_j (Q\circ R)^j = P \circ (Q \circ R).$$

(iii) Le second exemple qui précède cette proposition illustre l'absence de commutativité de la loi $\circ$. ■

La proposition suivante donne le degré de la composée de deux polynômes.

Proposition 6

Soient P et Q deux polynômes sur K tels que Q n'est pas un polynôme constant. On a

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

■ Si $a_n X^n$ est le monôme dominant de P et si $b_m X^m$ est celui de Q, alors $a_n (b_m)^n X^{mn}$ est le monôme dominant de $P \circ Q$ (car $m > 0$). Donc $\deg(P \circ Q) = nm = \deg(P) \times \deg(Q)$. ■

Lorsque Q est un polynôme constant non nul, la formule $\deg(P \circ Q) = \deg(P) \times \deg(Q)$ est vraie sauf lorsque la valeur prise par Q annule $P \circ Q$. On dit alors que cette valeur est une racine de P (nous reviendrons sur la notion fondamentale de racine plus tard dans ce cours).

Exemples :

- $\deg\big(P(X+1)\big) = \deg(P) \times \deg(X+1) = \deg(P)$.

A.4. Dérivation

Définition 8

La dérivation formelle des polynômes sur K est définie, pour $P = a_0 + a_1X + \cdots + a_nX^n$, par

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Autrement dit, si $P = \sum_{j=0}^{n} a_jX^j$, son polynôme dérivé est donné par

$$P' = \sum_{j=1}^{n} ja_jX^{j-1} = \sum_{i=0}^{n-1} (i+1)a_{i+1}X^i.$$

On peut évidemment itérer le processus de dérivation : P'' est le polynôme dérivé de P' puis P''' est le polynôme dérivé de P'', etc. On utilise ensuite les notations $P^{(4)}, P^{(5)}, \ldots, P^{(m)}, \ldots$ pour désigner les polynômes dérivés successifs de P. La notation $P^{(0)}$ est alors le polynôme P lui-même. Pour tout $m \in \mathbb{N}^*$, le polynôme dérivé m-ème de P est ainsi défini par récurrence par la formule

$$P^{(m)} = (P^{(m-1)})'$$

mais aussi explicitement par la formule

$$P^{(m)} = \sum_{j=m}^{n} j(j-1)\cdots(j-m+1)a_jX^{j-m}.$$

Dans $\mathbb{R}$, on peut retenir que la dérivation d'un polynôme s'effectue comme celle de sa fonction polynomiale associée, c'est-à-dire que, pour tout $m \in \mathbb{N}$, on a

$$\widetilde{P^{(m)}} = \widetilde{P}^{(m)}.$$

Il est toutefois important de bien comprendre que la dérivation formelle des polynômes n'est pas la dérivation des fonctions. Tout simplement parce qu'un polynôme n'est pas une fonction !

Exemples :

- Le polynôme dérivé d'un polynôme constant est clairement le polynôme nul.

  La réciproque est vraie lorsque K est de caractéristique nulle (par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). En effet, dans ce cas, si $P' = 0$, alors $\forall j \in \mathbb{N}^*,\ ja_j = 0$, c'est-à-dire $\forall j \in \mathbb{N}^*,\ a_j = 0$, donc $P = a_0$, c'est-à-dire que P est un polynôme constant.
- Dans $\mathbb{F}_p[X]$, le polynôme dérivé de X^p est le polynôme nul.

La dérivation formelle des polynômes partage les propriétés de la dérivation des fonctions.

Proposition 7

Soient P, Q deux polynômes sur K et $\lambda, \mu \in K$. On a

(i) $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$

plus généralement, pour tout $m \in \mathbb{N}$, on a $(\lambda P + \mu Q)^{(m)} = \lambda P^{(m)} + \mu Q^{(m)}$;

(ii) $(PQ)' = P'Q + PQ'$

plus généralement, pour tout $m \in \mathbb{N}$, on a la formule de Leibniz :

$$(PQ)^{(m)} = \sum_{k=0}^{m} \binom{m}{k} P^{(k)}Q^{(m-k)} ;$$

(iii) $(P \circ Q)' = Q'(P' \circ Q)$.

■ On note a_j les coefficients de P et b_j ceux de Q.

(i) Pour tout $m \in \mathbb{N}$, on a

$$\begin{aligned}(\lambda P+\mu Q)^{(m)} &= \left(\sum_{j\geqslant 0}(\lambda a_j+\mu b_j)X^j\right)^{(m)}\\ &= \sum_{j\geqslant m} j(j-1)\cdots(j-m+1)(\lambda a_j+\mu b_j)X^{j-m}\\ &= \lambda\sum_{j\geqslant m} j(j-1)\cdots(j-m+1)a_jX^{j-m}+\mu\sum_{j\geqslant m} j(j-1)\cdots(j-m+1)b_jX^{j-m}\\ &= \lambda P^{(m)}+\mu Q^{(m)}.\end{aligned}$$

(ii) Pour tout $k \in \mathbb{N}$, on a

$$\begin{aligned}(PX^k)' &= \left(\sum_{j\geqslant 0} a_jX^{j+k}\right)' = \sum_{j\geqslant 0}(j+k)a_jX^{k+j-1} = \sum_{j\geqslant 0} ja_jX^{k+j-1}+\sum_{j\geqslant 0} ka_jX^{k+j-1}\\ &= \left(\sum_{j\geqslant 0} ja_jX^{j-1}\right)X^k+\left(\sum_{j\geqslant 0} a_jX^j\right)kX^{k-1} = P'X^k+P.kX^{k-1},\end{aligned}$$

donc, avec la convention $0.X^{0-1}=0$,

$$(PQ)' = \left(\sum_{k\geqslant 0} b_kPX^k\right)' = \sum_{k\geqslant 0} b_k(P'X^k+P.kX^{k-1}) = P'\sum_{k\geqslant 0} b_kX^k+P\sum_{k\geqslant 0} kX^{k-1} = P'Q+PQ'.$$

Démontrons la formule de Leibniz par récurrence sur m.

Initialisation : Le résultat est évident pour $m=0$ et vient d'être démontré pour $m=1$.

Hérédité : Supposons la propriété vraie pour $m \in \mathbb{N}$ fixé et démontrons la au rang $m+1$. On a

$$\begin{aligned}(PQ)^{(m+1)} &= \left(\sum_{k=0}^{m}\binom{m}{k}P^{(k)}Q^{(m-k)}\right)' && \text{par H.R.}\\ &= \sum_{k=0}^{m}\binom{m}{k}\left(P^{(k+1)}Q^{(m-k)}+P^{(k)}Q^{(m+1-k)}\right) && \text{d'après (i) et le début de (ii)}\\ &= \sum_{k=0}^{m}\binom{m}{k}P^{(k+1)}Q^{(m-k)}+\sum_{k=0}^{m}\binom{m}{k}P^{(k)}Q^{(m+1-k)}\\ &= \sum_{\ell=k+1}^{m+1}\binom{m}{\ell-1}P^{(\ell)}Q^{(m+1-\ell)}+\sum_{k=0}^{m}\binom{m}{k}P^{(k)}Q^{(m+1-k)} && \ell=1\text{ ✓ }0,\ m\text{ ✓ }m+1\\ &= \sum_{k=0}^{m+1}\left(\binom{m}{k-1}+\binom{m}{k}\right)P^{(k)}Q^{(m+1-k)}\\ &= \sum_{k=0}^{m+1}\binom{m+1}{k}P^{(k)}Q^{(m+1-k)} && \text{d'après la relation de Pascal,}\end{aligned}$$

ce qui démontre le résultat au rang $m+1$.

Conclusion : Le principe de récurrence dit alors que la formule de Leibniz est vraie pour tout $m \in \mathbb{N}$.

(iii) Une récurrence immédiate utilisant la formule $(PQ)' = P'Q+PQ'$ permet de justifier que, pour tout $j \in \mathbb{N}^*$, on a $(Q^j)' = jQ'Q^{j-1}$. Par suite, on a

$$(P\circ Q)' = \left(\sum_{j\geqslant 0} a_jQ^j\right)' = \sum_{j\geqslant 1} a_j(Q^j)' = \sum_{j\geqslant 1} ja_jQ'Q^{j-1} = Q'\sum_{j\geqslant 1} ja_jQ^{j-1} = Q'(P'\circ Q),$$

ce qui correspond au résultat attendu. ■

Exemples :

- Soient $a \in K$ et $n \in \mathbb{N}$. Le polynôme dérivée de $P=(X-a)^n$ est $P'=n(X-a)^{n-1}$.

Cette fois encore, le résultat liant la dérivation et le degré est très utile dans la pratique.

Proposition 8

Soit P un polynôme sur K. On a

$$\deg(P') \leqslant \deg(P) - 1.$$

Si K est de caractéristique nulle et $\deg(P) \neq 0$, il y a égalité dans cette inégalité.

Plus généralement, on a

$$\forall m \in \mathbb{N}, \qquad \deg(P^{(m)}) \leqslant \deg(P) - m.$$

Si K est de caractéristique nulle et $\deg(P) \geqslant m$, il y a égalité dans cette inégalité.

■ AQT. ■

Pour $m \geqslant \deg(P) + 1$, on a $P^{(m)} = 0$.

On énonce ici la formule de Taylor pour les polynômes. Nous verrons plus tard qu'il existe aussi une formule de Taylor pour les fonctions (lorsqu'elles sont suffisamment dérivables).

Théorème 1

Ici K est de caractéristique nulle (par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). Soient $\alpha \in K$ et P un polynôme sur K de degré n. On a

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k.$$

Autrement dit,

$$P = P(\alpha) + P'(\alpha)(X-\alpha) + \frac{P''(\alpha)}{2}(X-\alpha)^2 + \cdots + \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n.$$

■ Notons a_j les coefficients du polynôme $P(X+\alpha)$. Pour tout $k \in [\![0;n]\!]$, on a

$$P^{(m)}(X+\alpha) = \sum_{j=k}^{n} j(j-1)\cdots(j-k+1)a_j X^{j-k}.$$

Lorsqu'on substitue 0 à X dans cette relation, seul le terme d'indice $j = k$ de la somme de droite n'est pas nul, donc, pour tout $k \in [\![0;n]\!]$, on a

$$P^{(k)}(\alpha) = k!a_k \qquad \text{c'est-à-dire} \qquad a_k = \frac{P^{(k)}(\alpha)}{k!}.$$

On a donc

$$P(X+\alpha) = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}X^k,$$

ce qui donne le résultat en composant avec $X - \alpha$. ■

La formule de Taylor est souvent utilisée dans le cas particulier $\alpha = 0$. On obtient alors la formule de Mac Laurin :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}X^k$$

qui permet d'exprimer les coefficients du polynôme $P = a_0 + a_1X + \cdots + a_nX^n$ en fonction des dérivées successives de P calculées en 0 :

$$\forall k \in [\![0;n]\!], \qquad a_k = \frac{P^{(k)}(0)}{k!}.$$

3 h 15

B. Arithmétique des polynômes

Dans cette section, on met en évidence les similarités arithmétiques entre $\mathbb{Z}$ et $K[X]$.

B.1. Multiples et diviseurs d'un polynôme

Définition 9

Soient A et B deux polynômes sur K. On dit que B divise A, et l'on note $B \mid A$, s'il existe un polynôme Q sur K tel que $A = BQ$.

On dit alors que B est un diviseur de A et que A est un multiple de B.

L'ensemble des diviseurs de A est noté $\mathscr{D}(A)$ et l'ensemble des multiples de B est noté $BK[X]$ ou $\mathscr{M}(B)$.

Exemples :

- Tout polynôme est un diviseur de 0.
- Un polynôme constant non nul divise tout autre polynôme et n'est divisible que par les polynômes constants non nuls.
- $X - i \mid X^2 + 1$ car $X^2 + 1 = (X - i)(X + i)$.

La divisibilité établit une relation de préordre sur $K[X]$.

Proposition 9

Sur $K[X]$, la relation « divise » est une relation de préordre, c'est-à-dire

(i) $\forall A \in K[X], \quad A \mid A$ (réflexivité) ;

(ii) $\forall A, B, C \in K[X], \quad (A \mid B \text{ et } B \mid C) \Longrightarrow (A \mid C)$ (transitivité).

Ce n'est pas une relation d'ordre car l'antisymétrie n'est pas satisfaite. On a seulement

(iii) $\forall A, B \in K[X], \quad (A \mid B \text{ et } B \mid A) \Longleftrightarrow (\exists \lambda \in K^*,\ A = \lambda B)$

et l'on dit alors que A et B sont associés.

La divisibilité restreinte à l'ensemble des polynômes unitaires est une relation d'ordre.

■ (i) et (ii) AQT

(iii) $\Rightarrow$ Soient $A, B \in K[X]$ tels que $A \mid B$ et $B \mid A$. Si A ou B est nul, alors ils sont nul tous les deux et le résultat est évident. On peut donc supposer dans la suite que ni A ni B n'est le polynôme nul. Il existe alors $Q_1, Q_2 \in K[X]$ non nuls tels que $A = BQ_1$ et $B = AQ_2$. En passant aux degrés, il vient $\deg(A) = \deg(B) + \deg(Q_1)$ et $\deg(B) = \deg(A) + \deg(Q_2)$, ce qui donne $\deg(A) \leqslant \deg(B)$ et $\deg(B) \leqslant \deg(A)$ et donc $\deg(A) = \deg(B)$. Mézalors $\deg(Q_1) = 0$, ce qui permet d'écrire $Q_1 = \lambda$ avec $\lambda \in K^*$. On a bien $A = \lambda B$ avec $\lambda \in K^*$.

$\Leftarrow$ AQT

Restreinte à l'ensemble des polynômes unitaires, la propriété (iii) exprime l'antisymétrie. Dans ce cas, la divisibilité est donc bien un ordre. ■

Cette proposition implique que $\big(\mathscr{D}(B) \subset \mathscr{D}(A)\big) \iff (B \mid A) \iff (AK[X] \subset BK[X])$.

Deux polynômes associés ont souvent les mêmes propriétés de divisibilité. Par conséquent, en pratique, on utilise souvent, comme représentant d'une famille de polynômes associés, l'unique polynôme unitaire de cette famille.

Sur $K[X]$, la divisibilité est une relation de préordre « plus forte » que la comparaison des degrés au sens où, pour tous polynômes A et B avec $A \neq 0$, le fait que B divise A implique que $\deg(B) \leqslant \deg(A)$, avec égalité si, et seulement si, A et B sont associés.

L'énoncé suivant complète les propriétés élémentaires de la relation de divisibilité dans $K[X]$.

Proposition 10

Soient A, B, C, D quatre polynômes sur K. On a

(i) si $B \mid A$ et $B \mid C$ alors $B \mid A + C$;

(ii) si $B \mid A$ et $D \mid C$ alors $BD \mid AC$.

En particulier, la propriété (ii) nous dit que

(ii)' pour tout $p \in \mathbb{N}$, si $B \mid A$ alors $B^p \mid A^p$.

■ AQT ■

La propriété (i) énonce la stabilité de la divisibilité par addition. Si l'on combine cette propriété avec la transitivité de la divisibilité et une simple récurrence, on obtient que si le polynôme B divise les polynômess $A_1, \ldots, A_n$ alors pour tous polynômes $M_1, \ldots, M_n$, le polynôme B divise $M_1A_1 + \cdots + M_nA_n$. On dit alors que la divisibilité est stable par combinaison linéaire à coefficients dans $K[X]$.

Attention, la stabilité de la divisibilité par addition vaut pour l'addition des multiples, pas des diviseurs ! Ainsi, 1 et X divisent X mais $1 + X$ ne divise pas X.

B. 2. Division euclidienne

L'anneau $K[X]$ possède, tout comme $\mathbb{Z}$, une division euclidienne. On dit qu'ils sont euclidiens.

Théorème 2

Soient A et B deux polynômes sur K tels que B n'est pas le polynôme nul. Il existe alors un unique couple (Q, R) de polynômes sur K tel que

$$A = BQ + R \qquad \text{et} \qquad \deg(R) < \deg(B).$$

Les polynômes Q et R sont appelés respectivement le quotient et le reste de la division euclidienne du dividende A par le diviseur B.

■ On démontre l'existence du couple (Q, R) puis son unicité.

▷ Existence : On procède par récurrence forte sur le degré de A. Autrement dit, on considère, pour tout $n \in \mathbb{N}$, l'assertion $\mathscr{P}(n)$ définie par « pour tout $A \in K_n[X]$ et tout $B \in K[X]$, il existe $Q, R \in K[X]$ tels que $A = BQ + R$ où $\deg(R) < \deg(B)$. »

Initialisation : Quand le polynôme A est constant non nul, on prend $Q = 0$ et $R = A$ sauf dans le cas où B est lui-même constant où l'on prend $Q = A/B$ et $R = 0$. Donc $\mathscr{P}(0)$ est vraie.

Hérédité : Fixons $n \geqslant 0$ tel que $\mathscr{P}(n)$ est vraie et démontrons $\mathscr{P}(n+1)$. Soient A et B deux polynômes de degrés respectifs $n+1$ et d et de coefficients dominants respectifs a_{n+1} et b_d. Si $d > n+1$, il suffit de prendre $Q = 0$ et $R = A$. Sinon, considérons le polynôme

$$A_1 = A - \frac{a_{n+1}}{b_d} X^{n+1-d} B.$$

Il est de degré inférieur ou égal à n (les monômes de degré $n+1$ se détruisent), donc l'hypothèse de récurrence s'applique : il existe un couple (Q_1, R_1) de polynômes vérifiant

$$A_1 = BQ_1 + R_1 \qquad \text{et} \qquad \deg(R_1) < \deg(B).$$

En remplaçant A_1 par sa définition, on obtient

$$A = B \times \left(\frac{a_{n+1}}{b_d} X^{n+1-d} + Q_1\right) + R_1 \qquad \text{et} \qquad \deg(R_1) < \deg(B),$$

ce qui prouve l'existence d'un quotient et d'un reste dans la division de $A \in K_{n+1}[X]$ par $B \in K[X]$. Ainsi $\mathscr{P}(n+1)$ est vraie.

Conclusion : Le principe de récurrence nous permet de conclure.

▷ Unicité : Soient (Q_1, R_1) et (Q_2, R_2) deux couples de polynômes sur K tels que $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$ avec $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$. On a alors $B(Q_1 - Q_2) = R_2 - R_1$. Or, $\deg(R_2 - R_1) < \deg(B)$ et $\deg(R_2 - R_1) = \deg\big(B(Q_1 - Q_2)\big) = \deg(B) + \deg(Q_1 - Q_2)$. On a donc $\deg(B) + \deg(Q_1 - Q_2) < \deg(B)$, d'où $\deg(Q_1 - Q_2) < 0$, c'est-à-dire $Q_1 - Q_2 = 0$. Il vient alors immédiatement que $R_2 - R_1 = B(Q_1 - Q_2) = 0$, c'est-à-dire $R_1 = R_2$. ■

Lorsque $\deg(B) > \deg(A)$, on a $A = B.0 + A$.

Nous pouvons faire, comme dans le cas des entiers, un lien immédiat entre la divisibilité d'un polynôme par un autre et le reste obtenu dans la division euclidienne.

Corollaire 1

Soient A et B deux polynômes sur K tels que B n'est pas le polynôme nul. Le polynôme B divise le polynôme A si, et seulement si, le reste de la division euclidienne de A par B est nul.

■ AQT ■

Voyons maintenant sur des exemples comment mettre en pratique cette division euclidienne.

Exemples :

- La division euclidienne de $A_1 = X^4 + X^3 - X^2 + X - 2$ par $B_1 = X^2 - X + 1$ donne

$$\begin{array}{rrrrr|l} X^4 & +X^3 & -X^2 & +X & -2 & X^2 - X + 1 \\ \cline{6-6} -(X^4 & -X^3 & +X^2) & & & X^2 + 2X \\ \cline{1-3} & 2X^3 & -2X^2 & +X & -2 & \\ & -(2X^3 & -2X^2 & +2X) & & \\ \cline{2-4} & & & -X & -2 & \end{array}$$

  donc

$$A_1 = (X^2 + 2X)B_1 + (-X - 2).$$

- La division euclidienne de $A_1 = X^4 + X^3 - X^2 + X - 2$ par $B_2 = X^2 + 1$ donne

$$\begin{array}{rrrrr|l} X^4 & +X^3 & -X^2 & +X & -2 & X^2 + 1 \\ \cline{6-6} -(X^4 & & +X^2) & & & X^2 + X - 2 \\ \cline{1-3} & X^3 & -2X^2 & +X & -2 & \\ & -(X^3 & & +X) & & \\ \cline{2-4} & & -2X^2 & & -2 & \\ & & -(-2X^2 & & -2) & \\ \cline{3-5} & & & & 0 & \end{array}$$

  donc

$$A_1 = (X^2 + X - 2)B_2,$$

  ce qui démontre que A_1 est un multiple de B_2.

Lorsque A et B sont des polynômes à coefficients entiers (c'est-à-dire $A, B \in \mathbb{Z}[X]$), la division euclidienne s'effectue dans $\mathbb{Q}[X]$. Le quotient et le reste de la division euclidienne de A par B sont donc des polynômes à coefficients rationnels. Cependant, lorsque B est unitaire, l'analyse de l'algorithme de la division euclidienne montre que l'on n'effectue aucune division de scalaires et donc que, dans ce cas, le quotient et le reste sont à coefficients dans $\mathbb{Z}$.

B.3. Idéaux de $K[X]$

Rappelons que, dans un anneau commutatif $(A, +, \times)$, un idéal I est une partie de A telle que $(I, +)$ est un sous-groupe de $(A, +)$ et I est hyperstable pour $\times$, c'est-à-dire $\forall i \in I,\ \forall a \in A,\ ia \in I$.

Dans $\mathbb{Z}$, la description des idéaux découlait directement de celle des sous-groupes additifs. En effet, les ensembles de multiples (les $n\mathbb{Z}$ avec n décrivant $\mathbb{N}$) sont exactement les sous-groupes additifs de $\mathbb{Z}$ donc les seuls candidats possibles pour être des idéaux de l'anneau $\mathbb{Z}$. Comme ce sont bien des idéaux, on en conclut immédiatement que les idéaux de $\mathbb{Z}$ sont bien les ensembles de multiples.

Les choses se compliquent avec les polynômes. En effet, les sous-groupes additifs de $K[X]$ ne se limitent pas aux ensembles de multiples (les $BK[X]$ avec B décrivant $K[X]$). Par exemple, pour tout $n \in \mathbb{N}$, l'ensemble $K_n[X]$ des polynômes de degré inférieur ou égal à n est un sous-groupe additif de $K[X]$ sans être un ensemble de multiples. Ainsi, lorsqu'on recherche les idéaux de $K[X]$, les sous-groupes additifs, candidats pour être des idéaux, ne se limitent pas aux ensembles de multiples. Le résultat de la proposition suivante n'en est que plus fort : il dit que les ensembles de multiples sont les seuls sous-groupes additifs de $K[X]$ à satisfaire l'hypersatibilité et qu'ils sont donc les seuls idéaux de $K[X]$.

Proposition 11

Les idéaux de l'anneau $K[X]$ sont exactement les ensembles de multiples, c'est-à-dire les $BK[X]$ où $B \in K[X]$.

■ $\Leftarrow$ Soit $B \in K[X]$.
Il est clair que $BK[X]$ est un sous-groupe de $K[X]$.
Si P est un multiple de B et Q est un polynôme quelconque, alors PQ est un multiple de B. Ainsi, si $P \in BK[X]$ et $Q \in K[X]$, alors $PQ \in BK[X]$. Cela prouve l'hyperstabilité de $BK[X]$.
Ainsi $BK[X]$ est bien un idéal de $K[X]$.

$\Rightarrow$ Réciproquement, considérons I un idéal de $K[X]$.
Si $I = \{0\}$, on a $I = 0K[X]$ et c'est terminé.
Si $I \neq \{0\}$, on remarque que $\{\deg(P) : P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$. Cela permet d'introduire son plus petit élément $n_0 \in \mathbb{N}$ ainsi qu'un polynôme B de I tel que $\deg(B) = n_0$.
Comme $B \in I$ et comme I est hyperstable, on a $BK[X] \subset I$.
Soit $A \in I$. La division de A par B donne $A = BQ + R$ où $\deg(R) < n_0$. On a $A \in I$ et $BQ \in I$ (car $B \in I$ et I est hyperstable) donc $R = A - BQ \in I$. Comme $\deg(R) < \deg(B)$ et comme B est un polynôme non nul de degré minimal dans I, on a forcément $R = 0$. Mézalors, $A = BQ$, c'est-à-dire $A \in BK[X]$. Donc $I \subset BK[X]$.
Ainsi, $I = BK[X]$, ce qui démontre bien que I est un ensemble de multiples. ■

On constate que les idéaux de $\mathbb{Z}$ et de $K[X]$ sont les ensembles de multiples d'un seul élément. On dit que ce sont des anneaux principaux. Cela leur confère de fortes propriétés arithmétiques.

B.4. Diviseurs et multiples communs

a) Plus grand diviseur commun

Définition 10

Soient A et B deux polynômes sur K. Le pgcd de A et B, noté $A \wedge B$ ou $\operatorname{pgcd}(A, B)$, est

(i) le diviseur commun à A et B, unitaire, et de plus haut degré parmi les diviseurs communs à A et B, lorsque $(A, B) \neq (0, 0)$;

(ii) égal à 0 si $(A, B) = (0, 0)$.

■ Il convient de justifier l'existence du pgcd.

Si $(A, B) \neq (0, 0)$, alors l'ensemble des degrés des diviseurs communs à A et B est une partie de $\mathbb{N}$, non vide (puisqu'elle contient $0 = \deg(1)$) et majorée par $\max\{\deg(A), \deg(B)\}$. Elle possède donc un plus grand élément d. Pour justifier l'existence et l'unicité du pgcd, nous allons démontrer que tous les diviseurs communs à A et B qui sont de degré d sont associés. Pour cela, on considère D un diviseur commun de A et B qui est de degré d.

Comme $AK[X]$ et $BK[X]$ sont des idéaux de $K[X]$, la somme $AK[X] + BK[X]$ est encore un idéal de $K[X]$. D'après la proposition 11, il existe alors $P_0 \in K[X]$ tel que $AK[X] + BK[X] = P_0K[X]$. Il est alors évident que les diviseurs commun à A et B sont des diviseurs de P_0, donc $D \mid P_0$. De plus, comme $AK[X] \subset AK[X] + BK[X]$ et $BK[X] \subset AK[X] + BK[X]$, on a $P_0 \mid A$ et $P_0 \mid B$, donc P_0 est un diviseur commun de A et B. La maximalité de d implique alors que $\deg(P_0) \leqslant d = \deg(D)$. La conjonction des conditions $D \mid P_0$ et $\deg(P_0) \leqslant \deg(D)$ implique alors que P_0 et D sont associés. Cela prouve bien que tous les diviseurs communs à A et B de degré d sont associés (car associés à P_0).

Il suffit donc de choisir pour $A \wedge B$ l'unique polynôme unitaire dans cette famille de polynômes associés.

On a démontré au passage que $AK[X] + BK[X] = (A \wedge B)K[X]$. ■

Notons que le pgcd est inchangé lorsqu'on remplace A ou B par des polynômes associés puisque, pour tous $\lambda, \mu \in K^*$, on a $(\lambda A) \wedge (\mu B) = A \wedge B$.

Commençons par établir un lemme qui généralise l'équivalence $\big(\mathscr{D}(B) \subset \mathscr{D}(A)\big) \iff (B \mid A)$.

Lemme 1

Soient A et B deux polynômes sur K tels que $B \neq 0$. Si l'on a $A = BQ + R$, alors

$$\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(R) \cap \mathscr{D}(B).$$

En particulier,

$$A \wedge B = B \wedge R.$$

■ $\subset$ Si $D \in \mathscr{D}(A) \cap \mathscr{D}(B)$, alors $D \mid BQ$ et $D \mid A$, donc $D \mid (A - BQ) = R$. Ainsi, $D \in \mathscr{D}(R) \cap \mathscr{D}(B)$. On a donc $\mathscr{D}(A) \cap \mathscr{D}(B) \subset \mathscr{D}(R) \cap \mathscr{D}(B)$.

$\supset$ Si $D \in \mathscr{D}(R) \cap \mathscr{D}(B)$, alors $D \mid BQ$ et $D \mid R$, donc $D \mid BQ + R = A$. Ainsi, $D \in \mathscr{D}(A) \cap \mathscr{D}(B)$. On a donc $\mathscr{D}(R) \cap \mathscr{D}(B) \subset \mathscr{D}(A) \cap \mathscr{D}(B)$.

En conclusion, $\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(R) \cap \mathscr{D}(B)$.

Les polynômes unitaires, de degré maximal, des ensembles $\mathscr{D}(A) \cap \mathscr{D}(B)$ et $\mathscr{D}(R) \cap \mathscr{D}(B)$ sont donc égaux, ce qui donne $A \wedge B = B \wedge R$. ■

On voit bien tout l'intérêt de cet énoncé : il ramène le calcul du pgcd d'un couple de polynômes à celui d'un autre couple dont l'un des deux polynômes est de degré plus petit. C'est cette remarque que l'algorithme d'Euclide exploite pour le calcul du pgcd.

Le lemme précédent permet de déterminer un ensemble de diviseurs communs.

Proposition 12

Soient A et B deux polynômes sur K. L'ensemble des diviseurs communs de A et B est aussi l'ensemble des diviseurs du pgcd de A et B, c'est-à-dire

$$\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(A \wedge B).$$

■ On suppose que $A \neq 0$ et $B \neq 0$ car le cas où A ou B est nul est évident. On pose $R_0 = A$, $R_1 = B$ et, pour tout $n \geqslant 2$, on note R_n le reste de la division de R_{n-1} par R_n si $R_{n-1} \neq 0$. D'après le lemme 1, on a $\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(B) \cap \mathscr{D}(R_2) = \mathscr{D}(R_2) \cap \mathscr{D}(R_3) = \cdots = \mathscr{D}(R_N) \cap \mathscr{D}(0) = \mathscr{D}(R_N)$, où la présence d'un reste nul est assurée par le fait que $\big(\deg(R_n)\big)_{n\geqslant 0}$ est une suite strictement décroissante d'entiers naturels.

Les polynômes unitaires, de degré maximal, des ensembles $\mathscr{D}(A) \cap \mathscr{D}(B)$ et $\mathscr{D}(R_N)$ sont donc égaux, ce qui signifie que $A \wedge B$ et R_N sont associés. Ainsi $\mathscr{D}(R_N) = \mathscr{D}(A \wedge B)$, ce qui établit le résultat. ■

Ce résultat signifie que $A \wedge B$ est le plus grand, au sens de la divisibilité, des diviseurs communs à A et B (c'est même valable lorsque $A = B = 0$).(†) On retiendra donc que

un polynôme D divise A et B si, et seulement si, D divise $A \wedge B$.

La proposition suivante introduit la notion de coefficients de Bézout.

Proposition 13

Soient A et B deux polynômes sur K. Il existe des couples $(U, V) \in K[X]^2$, appelés couples de coefficients de Bézout de A et B, tels que

$$UA + VB = A \wedge B.$$

Autrement dit,

$$AK[X] + BK[X] = (A \wedge B)K[X].$$

■ Ce résultat a été démontré au cours de la démonstration justifiant la validité de la définition 10. ■

L'algorithme d'Euclide que nous avons décrit dans le chapitre sur les entiers relatifs se généralise au cas des polynômes avec les modifications évidentes nécessaires. Donnons un exemple.

Exemples :

- Déterminons, à l'aide de l'algorithme d'Euclide, le pgcd et un couple de coefficients de Bézout pour les polynômes $A = X^3 + 2X^2 + 2X + 1$ et $B = X^5 + X^4 + 1$. On a

Quotients	Restes	Coefficients de Bézout	
	$X^5 + X^4 + 1$	1	0
$X^2 - X$	$X^3 + 2X^2 + 2X + 1$	0	1
$X + 1$	$X^2 + X + 1$	1	$-X^2 + X$
	0		

d'où

$$A \wedge B = X^2 + X + 1 \qquad \text{et} \qquad A \wedge B = 1 \times A + (-X^2 + X) \times B.$$

(†) Pour la relation de divisibilité sur l'ensemble des polynômes unitaires, un minorant est un diviseur. Par conséquent, $A \wedge B$ est le plus grand des minorants de $\{A; B\}$, c'est-à-dire que $A \wedge B$ est la borne inférieure de $\{A; B\}$.

La proposition 12 permet aussi d'établir la distributivité, dans $K[X]$, du produit sur le pgcd.

Proposition 14

Soient $A, B \in K[X]$ et $P \in K[X]$ un polynôme unitaire. On a

$$P(A \wedge B) = PA \wedge PB.$$

En particulier, si D est un diviseur unitaire de A et B, on a

$$\frac{A}{D} \wedge \frac{B}{D} = \frac{A \wedge B}{D}.$$

■ On a $P(A \wedge B)K[X] = P(AK[X] + BK[X]) = PAK[X] + PBK[X] = (PA \wedge PB)K[X]$, ce qui donne $P(A \wedge B) = PA \wedge PB$. ■

En particulier, si l'on choisit $D = A \wedge B$ (avec $AB \neq 0$) dans la seconde formule de cette proposition, on constate qu'en divisant A et B par leur pgcd, on obtient deux polynômes dont le pgcd est 1 (c'est-à-dire des polynômes premiers entre eux). Nous utiliserons cette remarque pour caractériser le pgcd dans la proposition 15.

b) Polynômes premiers entre eux

Définition 11

Les polynômes A et B sont dits premiers entre eux lorsque $A \wedge B = 1$, c'est-à-dire si les seuls diviseurs communs de A et B sont les polynômes constants non nuls.

Exemples :

- Deux polynômes qui diffèrent d'une constante non nulle sont toujours premiers entre eux. En effet, un diviseur commun à ces deux polynômes divise leur différence, c'est-à-dire une constante. Ce diviseur commun est donc bien constant non nul.
- Nous avons vu qu'en divisant deux polynômes par leur pgcd, on obtient deux polynômes premiers entre eux.

La proposition ci-dessous donne une caractérisation très utile du pgcd, utilisant la notion de polynômes premiers entre eux.

Proposition 15

Soient A, B deux polynômes sur K. Un polynôme unitaire D est le pgcd de A et B si, et seulement si,

$$\exists Q_A, Q_B \in K[X], \qquad A = DQ_A, \quad B = DQ_B \quad \text{et} \quad Q_A \wedge Q_B = 1.$$

■ On raisonne par double implication.

⇒ Supposons que $D = A \wedge B$. Comme D est un diviseur commun de A et B, il existe $Q_A, Q_B \in K[X]$ tels que $A = DQ_A$ et $B = DQ_B$. Alors $Q_A \wedge Q_B = (A/D) \wedge (B/D) = (A \wedge B)/D = D/D = 1$ d'après la proposition 14.

⇐ Réciproquement, supposons qu'il existe Q_A et Q_B dans $K[X]$ tels que $A = DQ_A$, $B = DQ_B$ et $Q_A \wedge Q_B = 1$. Alors, par la proposition 14, on a $A \wedge B = DQ_A \wedge DQ_B = D(Q_A \wedge Q_B) = D$. ■

Le théorème suivant, dit théorème de Bézout, permet de caractériser simplement deux polynômes premiers entre eux.

Théorème 3

Deux polynômes A et B sont premiers entre eux si, et seulement si, il existe $U, V \in K[X]$ tels que $UA + VB = 1$ (ou bien : $UA + VB$ est un polynôme constant non nul).

■ ⇒ Si A et B sont premiers entre eux, alors $A \wedge B = 1$ et l'on prend pour A et B les coefficients de Bézout fournis par la proposition 13.

⇐ S'il existe un couple $(U, V) \in K[X]^2$ tel que $UA + VB = 1$, alors $A \wedge B$ divise $UA + VB = 1$, ce qui force $A \wedge B = 1$. Donc A et B sont premiers entre eux. ■

En général, l'égalité $UA + VB = D$ implique seulement que D est un multiple de $A \wedge B$. C'est seulement lorsque D est un polynôme constant non nul que l'on peut affirmer que $A \wedge B = 1$.

Exemples :

- Si $\alpha, \beta \in K$ et $\alpha \neq \beta$, alors $X - \alpha$ et $X - \beta$ sont premiers entre eux. On peut le voir en invoquant le fait qu'il diffère d'une constante non nulle ou alors en écrivant la relation de Bézout : $(X - \alpha) - (X - \beta) = \beta - \alpha$.
- Les polynômes d'un couple de Bézout sont toujours premiers entre eux. En effet, on peut réécrire l'égalité $UA + VB = A \wedge B$ sous la forme $U(A/A \wedge B) + V(B/A \wedge B) = 1$.

Il existe de nombreuses applications du théorème de Bézout. Nous en proposons quelques unes dans les énoncés suivants.

On commence par le lemme de Gauss.

Théorème 4

Soient A, B, C trois polynômes sur K. On a

$$(A \wedge B = 1 \quad \text{et} \quad A \mid BC) \quad \Longrightarrow \quad (A \mid C).$$

■ Soient A, B, C trois polynômes tels que $A \wedge B = 1$ et $A \mid BC$. D'après le théorème de Bézout, on a $UA + VB = 1$ pour un couple $(U, V) \in K[X]^2$. D'où $UAC + VBC = C$. Le membre de gauche étant clairement divisible par A, il s'ensuit bien que $A \mid C$. ■

La proposition suivante énonce la compatibilité du produit avec la relation « être premier avec ».

Proposition 16

Soient $A_1, A_2, \ldots, A_n$ et B des polynômes sur K. On a

$$(A_1 \wedge B = 1, \ldots, A_n \wedge B = 1) \quad \Longrightarrow \quad (A_1 A_2 \cdots A_n \wedge B = 1).$$

■ On traite le cas $n = 2$. Le cas général s'obtient ensuite par récurrence.

Soient A_1, A_2, B trois polynômes sur K tels que $A_1 \wedge B = A_2 \wedge B = 1$. Par le théorème de Bézout, il existe $(U_1, V_1), (U_2, V_2) \in K[X]^2$ tels que $U_1 A_1 + V_1 B = 1$ et $U_2 A_2 + V_2 B = 1$. En multipliant ces relations, il vient $(U_1 A_1 + V_1 B)(U_2 A_2 + V_2 B) = 1$, ce qui donne, après développement et regroupement, $(U_1 U_2) A_1 A_2 + (U_1 A_1 V_2 + V_1 U_2 A_2 + V_1 V_2 B) B = 1$. Le théorème de Bézout nous permet d'en déduire que $A_1 A_2 \wedge B = 1$. ■

Exemples :

- Si A et B sont premiers entre-eux, alors pour tous $\alpha, \beta \in \mathbb{N}$, les polynômes A^α et B^β sont également premiers entre eux.

On termine avec l'indépendance divisorielle.

Proposition 17

Soient $A_1, \ldots, A_n, C$ des polynômes sur K. On a

$$(A_1 \mid C, \ \ldots, \ A_n \mid C \quad \text{et} \quad A_1, \ldots, A_n \text{ premiers entre eux deux à deux}) \quad \Longrightarrow \quad (A_1 \cdots A_n \mid C).$$

■ On traite le cas $n = 2$. Le cas général s'obtient ensuite par récurrence.

Soient A, B, C trois polynômes sur K tels que $A \wedge B = 1$, $A \mid C$ et $B \mid C$. Alors $UA + VB = 1$ avec $(U, V) \in K[X]^2$. En multipliant par C, on a $C = UAC + VBC$. Or il existe $Q_A, Q_B \in K[X]$ tels que $C = AQ_A$ et $C = BQ_B$, d'où $C = UABQ_B + VBAQ_A = (UQ_B + VQ_A)AB$. On a donc bien $AB \mid C$. ■

5 h 45

c) *Plus petit multiple commun*

Définition 12

Soient A et B deux polynômes sur K. Le ppcm de A et B, noté $A \vee B$ ou $\text{ppcm}(A, B)$, est

(j) le multiple commun à A et B, unitaire et de plus petit degré parmi les multiples communs non nuls de A et B, lorsque ni A ni B n'est nul ;

(jj) 0 lorsque A ou B est nul.

■ Il convient de justifier l'existence du ppcm.

Si $AB \neq 0$, alors l'ensemble des degrés des multiples non nuls communs à A et B est une partie de $\mathbb{N}$ non vide (puisqu'elle contient $\deg(AB)$) et possède donc, à ce titre, un plus petit élément d. Démontrons que tous les multiples communs à A et B qui sont de degré d sont associés.

Si M_1 et M_2 sont deux multiples communs à A et B de degré d, on effectue la division euclidienne de M_1 par M_2 de sorte que $M_1 = M_2Q + R$ avec $\deg(R) < \deg(M_2) = d$. Alors $R = M_1 - M_2Q$ est un multiple commun à A et B, ce qui force $R = 0$, par minimalité de d. Alors M_2 divise M_1 et ces deux polynômes sont de même degré, donc M_1 et M_2 sont associés.

On prend donc pour $A \vee B$ l'unique polynôme unitaire dans cette famille de polynômes associés. ■

Notons que le ppcm est inchangé lorsqu'on remplace A ou B par des polynômes associés puisque, pour tous $\lambda, \mu \in K^*$, on a $A \vee B = (\lambda A) \vee (\mu B)$.

L'énoncé ci-dessous permet de déterminer un ensemble de multiples communs.

Proposition 18

Soient A et B deux polynômes. L'ensemble des multiples communs de A et B est aussi l'ensemble des multiples du ppcm de A et B, c'est-à-dire

$$AK[X] \cap BK[X] = (A \vee B)K[X].$$

■ Si A ou B est constant, c'est clair. Supposons donc que $\deg(A) \geqslant 1$ et $\deg(B) \geqslant 1$.

Comme $AK[X]$ et $BK[X]$ sont des idéaux de $K[X]$, $AK[X] \cap BK[X]$ est un idéal de $K[X]$. D'après la proposition 11, il existe alors $P_0 \in K[X]$ tel que $AK[X] \cap BK[X] = P_0K[X]$. Les polynômes non nuls unitaires, de degré minimal, des ensembles $AK[X] \cap BK[X]$ et $P_0K[X]$ sont donc égaux, ce qui démontre que $A \vee B$ et P_0 sont associés. Donc $AK[X] \cap BK[X] = P_0K[X] = (A \vee B)K[X]$. ■

Ce résultat signifie que $A \vee B$ est le plus petit, au sens de la divisibilité, des multiples communs à A et B (ce résultat est valable même si $A = 0$ ou $B = 0$).(†) On retiendra que

un polynôme M est multiple de A et B si, et seulement si, M est multiple de $A \vee B$.

Ce résultat permet par exemple d'établir la distributivité, dans $K[X]$, du produit sur le ppcm.

Proposition 19

Soient P, A, B trois polynômes sur K tel que P est unitaire. Alors

$$(PA) \vee (PB) = P \times (A \vee B).$$

En particulier, si D est un diviseur unitaire de A et B, on a

$$\frac{A}{D} \vee \frac{B}{D} = \frac{A \vee B}{D}.$$

■ On a $(PA)K[X] \cap (PB)K[X] = P(AK[X] \cap BK[X]) = \big(P(A \vee B)\big)K[X]$, d'où le résultat. ■

(†) Pour la relation de divisibilité sur l'ensemble des polynômes unitaires, un majorant est un multiple. Par conséquent, $A \vee B$ est le plus petit des majorants de $\{A; B\}$, c'est-à-dire que $A \vee B$ est la borne supérieure de $\{A; B\}$.

d) Lien entre le pgcd et le ppcm

Commençons par un lemme donnant le ppcm de deux polynômes premiers entre eux.

Lemme 2

Soient A, B deux polynômes sur K unitaires premiers entre eux. Alors $A \vee B = AB$.

■ Soit $M = A \vee B$. On sait que $M = BC$ avec $C \in K[X]$. Comme $A \wedge B = 1$ et $A \mid M = BC$, le lemme de Gauss donne $A \mid C$, d'où l'existence de $Q \in K[X]$ tel que $C = AQ$, ce qui donne $M = BAQ$. Donc AB divise M, ce qui force $M = AB$, par minimalité divisorielle de M. ■

On peut alors énoncer la formule liant le pgcd et le ppcm de deux polynômes unitaires.

Proposition 20

Soient A et B deux polynômes sur K, unitaires. Alors

$$(A \wedge B) \times (A \vee B) = AB.$$

■ Posons $D = A \wedge B$ et $M = A \vee B$. On sait qu'il existe $Q_A, Q_B \in K[X]$ tels que $A = DQ_A$ et $B = DQ_B$ et $Q_A \wedge Q_B = 1$. Alors $M = DQ_A \vee DQ_B = D \times (Q_A \vee Q_B) = DQ_AQ_B$ d'après la proposition et le lemme qui précédent. Donc $DM = DQ_ADQ_B = AB$. ■

On peut retenir de cet énoncé que le calcul effectif du ppcm de deux polynômes revient au calcul du pgcd d'iceux (qui se fait par l'algorithme d'Euclide).

e) Généralisation au cas de plusieurs polynômes

Les résultats de ce paragraphe sont des généralisations des propriétés démontrées jusqu'ici dans le cas de deux polynômes. Les démonstrations sont donc omises.

Définition 13

Soient $A_1, \dots, A_m$ des polynômes sur K. Le pgcd de $A_1, \dots, A_m$, noté $A_1 \wedge \cdots \wedge A_m$ ou $\operatorname{pgcd}(A_1, \dots, A_m)$, est

(i) le diviseur commun à $A_1, \dots, A_m$, unitaire, et de plus haut degré parmi les diviseurs communs à $A_1, \dots, A_m$, lorsque $(A_1, \dots, A_m) \neq (0, \dots, 0)$;

(ii) égal à 0 si $(A_1, \dots, A_m) = (0, \dots, 0)$.

On commence par justifier que le pgcd est le plus grand diviseur au sens de la divisibilité.

Proposition 21

Soient $A_1, \dots, A_m$ des polynômes sur K. L'ensemble des diviseurs communs de $A_1, \dots, A_m$ est aussi l'ensemble des diviseurs du pgcd de $A_1, \dots, A_m$, c'est-à-dire

$$\mathscr{D}(A_1) \cap \cdots \cap \mathscr{D}(A_m) = \mathscr{D}(A_1 \wedge \cdots \wedge A_m).$$

On retiendra que

> un polynôme D divise $A_1, \dots, A_m$ si, et seulement si, D divise $A_1 \wedge \cdots \wedge A_m$.

La notation $A_1 \wedge \cdots \wedge A_m$ ne fait pas apparaître de parenthèses, présupposant l'associativité de la loi $\wedge$. L'énoncé suivant valide cette écriture.

Proposition 22

Soient $A_1, \dots, A_m$ des polynômes sur K. La loi $\wedge$ est associative, c'est-à-dire

$$A_1 \wedge \cdots \wedge A_m = (A_1 \wedge \cdots \wedge A_{m-1}) \wedge A_m.$$

Cette associativité est à la base du calcul du pgcd de plusieurs polynômes : on applique itérativement l'algorithme d'Euclide à A_1 et A_2, puis à $A_1 \wedge A_2$ et A_3, etc.

On peut aussi introduire la notion de coefficients de Bézout.

Proposition 23

Soient $A_1, \dots, A_m$ des polynômes sur K. Il existe des polynômes $U_1, \dots, U_m$, appelés coefficients de Bézout de $A_1, \dots, A_m$, tels que

$$U_1 A_1 + \cdots + U_m A_m = A_1 \wedge \cdots \wedge A_m.$$

Autrement dit,

$$A_1 K[X] + \cdots + A_m K[X] = (A_1 \wedge \cdots \wedge A_m) K[X].$$

La technique décrite ci-dessus pour le calcul du pgcd permet aussi de déterminer les coefficients de Bézout de plusieurs polynômes.

On peut alors généraliser la distributivité du produit sur le pgcd.

Proposition 24

Soient $A_1, \dots, A_m, P$ des polynômes sur K tels que P est unitaire. Alors

$$P(A_1 \wedge \cdots \wedge A_m) = PA_1 \wedge \cdots \wedge PA_m.$$

En particulier, si D est un diviseur unitaire de $A_1, \dots, A_m$, on a

$$\frac{A_1}{D} \wedge \cdots \wedge \frac{A_m}{D} = \frac{A_1 \wedge \cdots \wedge A_m}{D}.$$

On peut aussi généraliser la notion de polynômes premiers entre eux.

Définition 14

Soient $A_1, \dots, A_m$ des polynômes sur K.

On dit que $A_1, \dots, A_m$ sont premiers entre eux deux à deux lorsque, pour tous $i, j \in [\![1; m]\!]$ avec $i \neq j$, on a $A_i \wedge A_j = 1$.

On dit que $A_1, \dots, A_m$ sont premiers entre eux dans leur ensemble lorsque $A_1 \wedge \cdots \wedge A_m = 1$, c'est-à-dire lorsque les seuls diviseurs communs de $A_1, \dots, A_m$ sont les polynômes constants.

La notion de « polynômes premiers dans leur ensemble » est plus faible que celle de « polynômes premiers deux à deux ». Autrement dit, lorsque des polynômes sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fausse. Par exemple, on a $(X-1)X \wedge X(X+1) \wedge (X-1)(X+1) = 1$ mais $(X-1)X \wedge X(X+1) = X$, $(X-1)X \wedge (X-1)(X+1) = X-1$ et $X(X+1) \wedge (X-1)(X+1) = X+1$.

Si l'on choisit $D = A_1 \wedge \cdots \wedge A_m$ (avec les A_k tous non nuls) dans la seconde formule de la proposition 24, on constate qu'en divisant $A_1, \dots, A_m$ par leur pgcd, on obtient des polynômes premiers entre eux dans leur ensemble. Plus précisément, on a le résultat suivant.

Proposition 25

Soient $A_1, \dots, A_m$ des polynômes sur K. Un polynôme unitaire D est le pgcd de $A_1, \dots, A_m$ si, et seulement si,

$$\exists Q_1, \dots, Q_m \in K[X], \qquad A_1 = Q_1 D, \quad \dots, \quad A_m = Q_m D \quad \text{et} \quad Q_1 \wedge \cdots \wedge Q_m = 1.$$

Le théorème de Bézout se généralise au cas de plusieurs polynômes.

Théorème 5

Une famille $A_1, \dots, A_m$ de polynômes sur K sont premiers entre eux dans leur ensemble si, et seulement si, il existe $U_1, \dots, U_m \in K[X]$ tel que $U_1 A_1 + \cdots + U_m A_m = 1$.

En général, l'égalité $U_1 A_1 + \cdots + U_m A_m = D$ implique seulement que D est un multiple de $A_1 \wedge \cdots \wedge A_m$. C'est seulement dans le cas où D est un polynôme constant non nul, que l'on peut affirmer que $A_1 \wedge \cdots \wedge A_m = 1$.

On peut aussi généraliser le ppcm à plusieurs polynômes.

Définition 15

Soient $A_1, \dots, A_m$ des polynômes sur K. Le ppcm de $A_1, \dots, A_m$, noté $A_1 \vee \cdots \vee A_m$ ou $\text{ppcm}(A_1, \dots, A_m)$, est

(j) le multiple commun à $A_1, \dots, A_m$, unitaire et de plus petit degré parmi les multiples non nuls communs de $A_1, \dots, A_m$, lorsque $A_1 \times \cdots \times A_m \neq 0$;

(jj) 0 lorsque A_1 ou A_2 ou … ou A_m est nul.

On commence par justifier que le ppcm est le plus petit diviseur au sens de la divisibilité.

Proposition 26

Soient $A_1, \dots, A_m$ des polynômes sur K. L'ensemble des multiples communs de $A_1, \dots, A_m$ est aussi l'ensemble des multiples du ppcm de $A_1, \dots, A_m$, c'est-à-dire

$$A_1K[X] \cap \cdots \cap A_mK[X] = (A_1 \vee \cdots \vee A_m)K[X].$$

On retiendra que

un polynôme M est multiple de $A_1, \dots, A_m$ si, et seulement si, M est multiple de $A_1 \vee \cdots \vee A_m$.

La notation $A_1 \vee \cdots \vee A_m$ ne fait pas apparaître de parenthèses, présupposant l'associativité de la loi $\vee$. L'énoncé suivant valide cette écriture.

Proposition 27

Soient $A_1, \dots, A_m$ des polynômes sur K. La loi $\vee$ est associative, c'est-à-dire

$$A_1 \vee \cdots \vee A_m = (A_1 \vee \cdots \vee A_{m-1}) \vee A_m.$$

On peut alors généraliser la distributivité du produit sur le ppcm.

Proposition 28

Soient $A_1, \dots, A_m, P$ des polynômes sur K. On a

$$P(A_1 \vee \cdots \vee A_m) = PA_1 \vee \cdots \vee PA_m.$$

En particulier, si D est un diviseur unitaire de $A_1, \dots, A_m$, on a

$$\frac{A_1}{D} \vee \cdots \vee \frac{A_m}{D} = \frac{A_1 \vee \cdots \vee A_m}{D}.$$

B. 5. Polynômes irréductibles

a) Définition et premières propriétés des polynômes irréductibles

Définition 16

Un polynôme P de $K[X]$ est dit irréductible sur K lorsqu'il est non constant ($\deg(P) \geqslant 1$) et lorsque ses seuls diviseurs sont 1 et P et leurs associés (autrement dit lorsque tout diviseur Q de P vérifie ou bien $\deg(Q) = 0$ ou bien $\deg(Q) = \deg(P)$).

Les polynômes irréductibles sont aux polynômes ce que les nombres premiers sont aux entiers relatifs.

Exemples :

- Les polynômes de degré 1 sont irréductibles.

La proposition suivante donne une caractérisation des polynômes irréductibles.

Proposition 29

Un polynôme non constant est irréductible si, et seulement si, il est premier avec tous les polynômes qu'il ne divise pas.

■ $\Rightarrow$ Soient P un polynôme irréductible et A un polynôme qui n'est pas divisible par P. Les diviseurs communs à P et A sont avant tout des diviseurs de P. Ils sont donc ou bien constants ou bien associés à P. Comme P ne divise pas A, les seuls diviseurs communs à P et A sont donc les polynômes constants. Cela signifie bien que P et A sont premiers entre eux.

$\Leftarrow$ Soit P un polynôme qui est premier avec tous les polynômes qu'il ne divise pas. Soit Q un diviseur de P qui n'est pas associé à P. Alors P ne divise pas Q donc P est premier avec son diviseur Q, ce qui signifie que Q est un polynôme constant non nul. Cela démontre que P est irréductible. ■

Exemples :

- Si P et Q sont deux polynômes irréductibles non associés, la proposition ci-dessus nous dit que P et Q sont premiers entre eux.

  Dès lors, P^α et Q^β sont premiers entre eux, pour tous $\alpha, \beta \in \mathbb{N}$.

b) Décomposition primaire

Théorème 6

Tout polynôme $P \in K[X]$, unitaire et non constant, admet une décomposition en polynômes irréductibles unitaires, qui est unique à l'ordre des facteurs près. Autrement dit,

(i) pour tout polynôme P tel que $\deg(P) \geqslant 1$, il existe une famille $P_1, \dots, P_r$ de polynômes irréductibles distincts tels que $P = {P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$ où $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$;

(ii) cette décomposition est unique à l'ordre près des facteurs et à une constante multiplicative près.

L'existence de cette décomposition primaire fait de $\big(K[X], +, \times\big)$ un anneau dit factoriel.

■ ▶ Démontrons l'existence par récurrence forte. Pour tout $n \geqslant 1$, on note $\mathscr{P}_n$ l'assertion « tout polynôme non constant de $K_n[X]$ admet une décomposition en polynômes irréductibles ».

Initialisation : La propriété $\mathscr{P}_1$ est vérifiée car les polynômes de degré 1 sont irréductibles.

Hérédité : Fixons $n \geqslant 2$ tel que $\mathscr{P}_{n-1}$ est vraie et démontrons $\mathscr{P}_n$. Soit P un polynôme de degré n. On distingue deux cas :

▷ Si P est un polynôme irréductible alors c'est le produit d'un seul polynôme irréductible.

▷ Sinon, P admet un diviseur irréductible Q (il suffit de prendre un diviseur de P non constant de degré minimal parmi les diviseurs non constants de P). On a $Q \neq P$ puisque P n'est pas irréductible donc le degré du polynôme P/Q appartient à $[\![1; n-1]\!]$. L'hypothèse de récurrence nous permet de décomposer P/Q en un produit de facteurs irréductibles, d'où l'existence de polynômes irréductibles $P_1, \dots, P_r$ tels que $P/Q = {P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$. Cela fournit la décomposition de P en polynômes irréductibles : $P = Q{P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$.

Donc $\mathscr{P}_n$ est vraie.

Conclusion : D'après le principe de récurrence, $\mathscr{P}_n$ est vraie pour tout $n \geqslant 1$, ce qui justifie l'existence de la décomposition en polynômes irréductibles.

▶ Démontrons ensuite l'unicité d'une telle décomposition. Supposons qu'un polynôme P non constant admette deux décompositions $P = {P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$ et $P = \lambda {P_1}^{\beta_1} \cdots {P_r}^{\beta_r}$ où les P_i sont des polynômes irréductibles deux à deux distincts, $\alpha_i \in \mathbb{N}$, $\beta_i \in \mathbb{N}$ et $\lambda \in K^*$.
Raisonnons alors par l'absurde en supposant que'il existe $k \in [\![1; r]\!]$ est tel que $\alpha_k \neq \beta_k$, par exemple $\alpha_k < \beta_k$. En simplifiant l'égalité ${P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r} = \lambda {P_1}^{\beta_1} \cdots {P_r}^{\beta_r}$ par ${P_k}^{\alpha_k}$, on voit qu'il reste un facteur ${P_k}^{\beta_k - \alpha_k}$ à droite, ce qui implique que le membre de gauche est divisible par P_k, c'est-à-dire

$$P_k \,\Big|\, \prod_{\substack{j=1 \\ j \neq k}}^{r} {P_j}^{\alpha_j}.$$

Or, lorsque $j \neq k$, les polynômes irréductibles P_k et P_j sont distincts donc premiers entre eux. D'après la proposition 16, on a donc

$$P_k \wedge \prod_{\substack{j=1 \\ j \neq k}}^{r} {P_j}^{\alpha_j} = 1.$$

Il s'ensuit que P_k est constant, ce qui est absurde !
Par suite, on a $\forall i \in [\![1; r]\!]$, $\alpha_i = \beta_i$, ce qui démontre l'unicité de la décomposition, à la constante multiplicative près λ. ■

Exemples :

- Soit $a > 1$. Décomposons $X^4 - 2aX^2 + 1$ dans $\mathbb{R}[X]$. Pour cela, on écrit

$$\begin{aligned} & X^4 - 2aX^2 + 1 \\ = \; & (X^2 - a)^2 - (a^2 - 1) \\ = \; & \big(X^2 - a - \sqrt{a^2-1}\big)\big(X^2 - a + \sqrt{a^2-1}\big) \\ = \; & \Big(X + \sqrt{a + \sqrt{a^2-1}}\Big)\Big(X - \sqrt{a + \sqrt{a^2-1}}\Big)\Big(X + \sqrt{a - \sqrt{a^2-1}}\Big)\Big(X - \sqrt{a - \sqrt{a^2-1}}\Big). \end{aligned}$$

Donnons quelques applications de la décomposition primaire.

En général, lorsque $C \mid AB$, on ne peut pas en déduire que $C \mid A$ ou $C \mid B$. En revanche, dans le cas d'un diviseur irréductible, la propriété suivante dit que c'est vrai.

Proposition 30

Soient A, B, P trois polynômes sur K. On a

$$(P \text{ irréductible} \quad \text{et} \quad P \mid AB) \quad \Longrightarrow \quad (P \mid A \quad \text{ou} \quad P \mid B).$$

Ainsi, un polynôme irréductible divise un produit si, et seulement si, il divise l'un de ses facteurs.

■ Le cas où A ou B est constant est évident. Sinon, si un polynôme irréductible P divise AB, c'est qu'il est dans la décomposition primaire de AB et donc qu'il est nécessairement aussi dans la décomposition primaire de A ou dans celle de B, ce qui signifie bien que P divise A ou B. ■

La décomposition en polynômes irréductibles permet de déterminer si un polynôme en divise un autre.

Proposition 31

Soient A et B deux polynômes sur K non constants dont les décompositions primaires sont $A = {P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$ et $B = {P_1}^{\beta_1} \cdots {P_r}^{\beta_r}$ où $P_1, \dots, P_r$ sont des polynômes irréductibles distincts et $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$. Alors B divise A si, et seulement si, $\beta_k \leqslant \alpha_k$ pour tout $k \in [\![1; r]\!]$.

■ $\Rightarrow$ Supposons que A divise B. Alors, pour tout $k \in [\![1; r]\!]$, on a ${P_k}^{\alpha_k} \mid A$ et donc ${P_k}^{\alpha_k} \mid B$, ce qui démontre que $\alpha_k \leqslant \beta_k$.

$\Leftarrow$ Supposons réciproquement que $\forall k \in [\![1; r]\!]$, $\beta_k \leqslant \alpha_k$. En posant $Q = {P_1}^{\alpha_1 - \beta_1} \cdots {P_r}^{\alpha_r - \beta_r}$, on a $A = BQ$, ce qui démontre que B divise A. ■

La décomposition en polynômes irréductibles permet également de calculer le pgcd et le ppcm de deux polynômes.

Proposition 32

Soient A et B deux polynômes sur K non constants dont les décompositions primaires sont $A = {P_1}^{\alpha_1} \cdots {P_r}^{\alpha_r}$ et $B = {P_1}^{\beta_1} \cdots {P_r}^{\beta_r}$ où $P_1, \dots, P_r$ sont des polynômes irréductibles distincts et $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$. Alors

$$A \wedge B = \prod_{i=1}^{r} {P_i}^{\min\{\alpha_i, \beta_i\}} \qquad \text{et} \qquad A \vee B = \prod_{i=1}^{r} {P_i}^{\max\{\alpha_i, \beta_i\}}.$$

■ Les diviseurs communs de A et B sont de la forme ${P_1}^{\delta_1} \cdots {P_r}^{\delta_r}$ avec $\forall i,\ \delta_i \leqslant \alpha_i$ et $\delta_i \leqslant \beta_i$. Le plus grand des diviseurs communs à A et B est donc obtenu lorsque $\forall i,\ \delta_i = \min\{\alpha_i, \beta_i\}$, ce qui démontre la première égalité.

Les multiples communs de A et B sont de la forme ${P_1}^{\mu_1} \cdots {P_r}^{\mu_r}$ avec $\forall i,\ \mu_i \leqslant \alpha_i$ et $\mu_i \leqslant \beta_i$. Le plus petit des multiples communs à A et B est donc obtenu lorsque $\forall i,\ \mu_i = \max\{\alpha_i, \beta_i\}$, ce qui démontre la seconde égalité. ■

C. Racines

C.1. Racines

Définition 17

Soient P un polynôme sur K et $\alpha \in K$. Les propriétés suivantes sont équivalentes :

(i) $P(\alpha) = 0$,

(ii) le polynôme P est divisible par $X - \alpha$.

Par conséquent, si l'une de ces deux propriétés est vérifiée, l'autre l'est aussi et l'on dit que α est une racine de P.

■ $\Leftarrow$ Si (ii) est vraie, on a $P = (X - \alpha)Q$ où $Q \in K[X]$. Alors $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$ et l'on a (i).

$\Rightarrow$ Supposons réciproquement que (i) soit vérifiée. On donne alors trois démonstrations de (ii).

▷ Pour tout nombre entier k, la formule de Bernoulli nous dit que

$$X^k - \alpha^k = (X - \alpha)(\underbrace{X^{k-1} + \alpha X^{k-2} + \alpha^2 X^{k-3} + \cdots + \alpha^{k-2} X + \alpha^{k-1}}_{=Q_k})$$

Donc, si $P = a_0 + a_1 X + \cdots + a_n X^n$, on a

$$P = P - P(\alpha) = \sum_{k=0}^{n} a_k (X^k - \alpha^k) = \sum_{k=0}^{n} a_k (X - \alpha) Q_k = (X - \alpha) \sum_{k=0}^{n} a_k Q_k,$$

ce qui démontre que $X - \alpha$ divise P.

▷ Effectuons la division euclidienne de P par $X - \alpha$. On obtient la relation $P = (X - \alpha)Q + k$ où k est une constante (puisque le degré du reste doit être strictement inférieur au degré du diviseur). En substituant α à X, on obtient $P(\alpha) = (\alpha - \alpha)Q(\alpha) + k$, c'est-à-dire $k = 0$. On a donc $P = (X - \alpha)Q$ ce qui démontre (ii) une deuxième fois.

▷ Lorsque K est de caractéristique nulle, on peut également utiliser la formule de Taylor. En effet, celle-ci nous donne

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k = (X - \alpha) \sum_{k=1}^{n} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^{k-1},$$

ce qui prouve, une troisième fois, que $X - \alpha$ divise P. ■

Exemples :

- Soit $A_2 = X^4 - 2X^3 + 2X^2 - 2X + 1$. On remarque que 1 est une racine de A_2, ce qui permet de factoriser $X - 1$ dans A_2. On a

$$\begin{array}{rrrrr|l}
X^4 & -2X^3 & +2X^2 & -2X & +1 & X-1 \\
\cline{6-6}
-(X^4 & -X^3) & & & & X^3 - X^2 + X - 1 \\
\cline{1-5}
 & -X^3 & +2X^2 & -2X & +1 & \\
 & -(-X^3 & +X^2) & & & \\
\cline{2-5}
 & & X^2 & -2X & +1 & \\
 & & -(X^2 & -X) & & \\
\cline{3-5}
 & & & -X & +1 & \\
 & & & -(-X & +1) & \\
\cline{4-5}
 & & & & 0 &
\end{array}$$

d'où

$$A_2 = (X - 1)(X^3 - X^2 + X - 1).$$

C. 2. Multiplicité

Définition 18

Soient P un polynôme sur K, $\alpha \in K$ et $m \geqslant 1$. On dit que α est une racine de P de multiplicité m lorsque P est divisible par $(X-\alpha)^m$ mais n'est pas divisible par $(X-\alpha)^{m+1}$.

La multiplicité de α est la plus grande puissance de $X-\alpha$ factorisable dans le polynôme. C'est donc aussi l'exposant que $(X-\alpha)$ dans la décomposition primaire de P.

Un élément de K est de multiplicité 0 lorsque ce n'est pas une racine. Une racine de multiplicité 1 est dite simple. Une racine de multiplicité supérieure ou égale à 2 est dite multiple. De plus, pour abréger, une racine de multiplicité 2, 3 ou 4 est dite double, triple ou quadruple.
Si l'on sait seulement que $(X-\alpha)^m$ divise P, on dit que α est de multiplicité au moins m.

En caractéristique nulle, on dispose de la caractérisation suivante de l'ordre de multiplicité.

Proposition 33

Ici K est de caractéristique nulle. Soient P un polynôme sur K, $\alpha \in K$ et $m \geqslant 1$. Le nombre α est une racine de P de multiplicité m si, et seulement si, $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

■ On note n le degré de P.

⇒ Supposons que α est une racine de P de multiplicité m. Comme $(X-\alpha)^m$ divise P, il existe $Q \in K[X]$ tel que $P = (X-\alpha)^m Q$. La formule de Leibniz nous dit que, pour tout $\ell \in \mathbb{N}$, on a

$$P^{(\ell)} = \sum_{k=0}^{\ell} \binom{\ell}{k} \left((X-\alpha)^m\right)^{(k)} Q^{(\ell-k)} = \sum_{k=0}^{\ell} \binom{\ell}{k} m(m-1)\cdots(m-k+1)(X-\alpha)^{m-k} Q^{(\ell-k)}.$$

Tant que $\ell < m$, tous les termes de cette somme contiennent au moins un facteur $(X-\alpha)$, ce qui implique que $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$. Pour $\ell = m$, tous les termes de cette somme contiennent au moins un facteur $(X-\alpha)$ sauf celui d'indice $k = m$, ce qui donne $P^{(m)}(\alpha) = m!Q$. Comme $Q(\alpha) \neq 0$ (sinon Q serait divisible par $X-\alpha$ et P serait donc divisible par $(X-\alpha)^{m+1}$, ce qu'il n'est pas), on a $P^{(m)}(\alpha) \neq 0$ (car $m! \neq 0$ puisqu'on est en caractéristique nulle).

⇐ Supposons que $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$. La formule de Taylor nous dit alors que

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = \frac{P^{(m)}(\alpha)}{k!}(X-\alpha)^m + (X-\alpha)^{m+1} \sum_{k=m+1}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m-1}.$$

Comme tous les termes sont divisibles par $(X-\alpha)^m$, on en déduit que P l'est aussi. Par ailleurs, comme le second terme est divisible par $(X-\alpha)^{m+1}$ mais pas le premier (puisque $P^{(m)}(\alpha) \neq 0$), on peut affirmer que P n'est pas divisible par $(X-\alpha)^{m+1}$. ■

En caractéristique nulle, on constate qu'une racine de multiplicité m de P est une racine de multiplicité $m-1$ de P'.

Exemples :

- Reprenons $A_2 = X^4 - 2X^3 + 2X^2 - 2X + 1$.
  Nous avons vu que A_2 est divisible par $X-1$ et que le quotient est égal à $X^3 - X^2 + X - 1$. On remarque alors que 1 est à nouveau une racine de ce quotient, ce qui permettrait de factoriser $X-1$ une fois de plus, à l'aide d'une nouvelle division euclidienne.
  On peut cependant déterminer la multiplicité de 1 plus directement. On a $A_2(1) = 0$ donc 1 est racine au moins simple. On a $A_2' = 4X^3 - 6X^2 + 4X - 2$ et $A_2'(1) = 0$ donc 1 racine au moins double. On a $A_2'' = 12X^2 - 12X + 4$ et $A_2''(0) = 4 \neq 0$ donc 1 est une racine double de A_2.
  On peut alors se contenter de faire directement une seule division euclidienne de A_2 par $(X-1)^2$, ce qui donne $A_2 = (X-1)^2(X^2+1)$. On a alors $A_2 = (X-1)^2(X-i)(X+i)$, donc les deux autres racines de A_2 sont i et $-i$ et sont simples.

Lorsque l'on connait plusieurs racines d'un polynôme ainsi que leurs multiplicités, on peut factoriser davantage le polynôme.

Proposition 34

Soit P un polynôme sur K. Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P de multiplicités respectives $m_1, \ldots, m_k$, alors P est divisible par $(X-\alpha_1)^{m_1} \cdots (X-\alpha_k)^{m_k}$.

■ Les hypothèses permettent de factoriser P par $(X-\alpha_1)^{m_1}$, par $(X-\alpha_2)^{m_2}$, ..., par $(X-\alpha_k)^{m_k}$. Or les polynômes $(X-\alpha_j)^{m_j}$ sont premiers entre eux deux à deux puisque ce sont des puissances de polynômes irréductibles distincts. La proposition 17 sur l'indépendance divisorielle implique alors que P est divisible par $(X-\alpha_1)^{m_1} \cdots (X-\alpha_k)^{m_k}$. ■

8 h 00

C.3. Comptage des racines

a) Nombre maximal de racines

Proposition 35

Un polynôme de $K[X]$ de degré $n \geqslant 0$ possède au plus n racines dans K, comptées avec leurs ordres de multiplicités.

■ Soit $\alpha_1, \dots, \alpha_p$ la liste des racines distinctes du polynôme P. On note $m_1, \dots, m_p$ leurs multiplicités respectives. Le polynôme P est alors divisible par $Q = \prod_{j=1}^{p} (X - \alpha_j)^{m_j}$ d'après le corollaire 34. Le degré d'un diviseur étant toujours inférieur au degré d'un polynôme (non nul) qu'il divise, on a $\deg(Q) \leqslant \deg(P)$, c'est-à-dire $m_1 + \cdots + m_p \leqslant n$. C'est précisément ce que l'on souhaitait démontrer. ■

Nous verrons que, dans $\mathbb{C}$, un polynôme admet un nombre de racines exactement égal à son degré. Ce n'est pas le cas dans $\mathbb{R}$: le polynôme $X^2 + 1$ n'admet aucune racine réelle.

L'encadré ci-dessous explique comment on utilise en général le résultat précédent.

Y'a que les nuls qui ont trop de zéros !

Le seul polynôme qui possède strictement plus de racines (comptées avec leurs ordres de multiplicité) que son degré est le polynôme nul. En particulier, si K est infini, le polynôme nul est le seul polynôme qui possède une infinité de racines.

Par conséquent, pour démontrer que les polynômes P et Q sont égaux, on peut introduire le polynôme différence $R = P - Q$ et démontrer que ce polynôme possède plus de racines que son degré. Cela prouve qu'il est nul et donc que $P = Q$.

Exemples :

- Soient P, Q deux polynômes de degré $\leqslant n-1$ qui ont n valeurs en commun, c'est-à-dire tels qu'il existe $a_1, \dots, a_n \in K$ distincts deux à deux vérifiant $\forall j \in [\![1; n]\!]$, $P(a_j) = Q(a_j)$. Démontrons que P et Q sont égaux. Pour cela, on introduit le polynôme $R = P - Q$. Alors $\deg(R) \leqslant \max\{\deg(P), \deg(-Q)\} \leqslant n-1$ et R s'annule en chaque a_j. Il possède donc plus de racines que son degré ce qui l'oblige à être nul. Ainsi $P = Q$.

La règle « trop de racines » permet de justifier, dans le cas d'un corps infini, l'identification d'un polynôme avec sa fonction polynomiale.

Proposition 36

Notons $\mathscr{P}$ l'ensemble des fonctions polynomiales sur K. Si K est un corps infini, l'application $\varphi : K[X] \longrightarrow \mathscr{P}$ qui, à tout polynôme P de $K[X]$, associe sa fonction polynomiale $\widetilde{P}$ est un isomorphisme d'anneaux.

■ On sait que $K[X]$ et $\mathscr{P}$ sont des anneaux. De plus, on a $\widetilde{1} = 1$, $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$ et $\widetilde{PQ} = \widetilde{P}\,\widetilde{Q}$ donc φ est bien un morphisme d'anneaux.

Par construction, φ est surjective. Par ailleurs, si l'on considère un polynôme P dans le noyau de φ, alors $\widetilde{P}$ est la fonction nulle, ce qui signifie que P admet chaque élément de K comme racine. Comme K est infini, on en déduit que P est le polynôme nul. Donc $\operatorname{Ker}\varphi = \{0\}$ et φ est injective. Ainsi, φ est bien un isomorphisme entre $K[X]$ et $\mathscr{P}$. ■

Dans le cas d'un corps fini $\mathbb{L}$, les polynômes 0 et $\prod_{\lambda \in \mathbb{L}} (X - \lambda)$ sont distincts, puisqu'ils sont respectivement de degré $-\infty$ et $\operatorname{card}\mathbb{L}$, mais leurs fonctions polynomiales sont égales.

b) Le théorème de d'Alembert-Gauss

Ce paragraphe est consacré au théorème de d'Alembert–Gauss qui énonce en substance que le corps $\mathbb{C}$ se suffit à lui-même : il contient toutes les racines des polynômes à coefficients complexes (ce résultat est faux sur $\mathbb{R}$ puisque le polynôme à coefficients réels X^2+1 admet deux racines, $-i$ et i, qui ne sont pas des nombres réels).

Il est remarquable de noter que ce résultat, qui constitue le théorème fondamental de l'algèbre, ne peut pas être démontré sans analyse. Cette démonstration est difficile et hors programme en première année. Elle n'est donc proposée ici qu'à titre culturel.

Théorème 7

Tout polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}$ possède exactement n racines complexes comptées avec leurs multiplicités.

■ [✠] Nous allons démontrer que tout polynôme sur $\mathbb{C}$ non constant admet au moins une racine dans $\mathbb{C}$. Cela fournira le résultat par factorisations successives de facteurs du type $X-\alpha$ où α est une racine.

Soit P un polynôme à coefficients complexes de degré $d \geqslant 1$. On pose $m = \inf\{|P(z)| : z \in \mathbb{C}\}$, qui existe puisque $\{|P(z)| : z \in \mathbb{C}\}$ est une partie non vide et minorée (par 0) de $\mathbb{R}$. Nous allons démontrer successivement que cette borne inférieure est atteinte puis qu'elle est nulle.

▷ Écrivons $P = a_0+a_1X+\cdots+a_dX^d$ avec $a_d \neq 0$. L'inégalité triangulaire « inversée » nous dit que, pour tout $z \in \mathbb{C}$, on a $|P(z)| \geqslant |a_d||z|^d - |a_{d-1}||z|^{d-1} - \cdots - |a_0|$, donc $\lim_{|z|\to+\infty} |P(z)| = +\infty$. Il s'ensuit qu'il existe $R > 0$ tel que $\forall z \in \mathbb{C},\ (|z| > R) \Longrightarrow (|P(z)| \geqslant m+1)$. Puisque $m = \inf\{|P(z)| : z \in \mathbb{C}\}$, on peut trouver une suite $(z_n)_{n\geqslant 0} \in \mathbb{C}^{\mathbb{N}}$ telle que $\lim_{n\to+\infty} |P(z_n)| = m$. La suite $(z_n)_{n\geqslant 0}$ est donc, à partir d'un certain rang, dans le disque de centre 0 et de rayon R, et par suite, elle est bornée. D'après le théorème de Bolzano–Weierstrass, on peut en extraire une sous-suite $(z_{n_k})_{k\geqslant 0}$ convergeant vers un nombre complexe α. Un passage à la limite nous dit alors que $\lim_{k\to+\infty} |P(z_{n_k})| = |P(\alpha)|$ (en utilisant les théorèmes généraux sur les limites de suites complexes). On a donc $|P(\alpha)| = m$.

▷ Supposons que $m = |P(\alpha)| \neq 0$. Quitte à changer P en $P(X+\alpha)/P(\alpha)$, on peut alors supposer que $\alpha = 0$ et $m = 1$. Le polynôme non constant P s'écrit donc $P = 1 + a_qX^q + \cdots + a_dX^d$ avec $a_q \neq 0$ où $1 \leqslant q \leqslant d$. Posons $a_q = \rho\,\mathrm{e}^{i\theta}$ avec $\rho > 0$ et $\theta \in \mathbb{R}$. Pour $z = r\,\mathrm{e}^{i(\pi-\theta)/q}$ avec $r > 0$, on a

$$|P(z)| = \left|1 - \rho r^q + \sum_{k=q+1}^{p} a_k r^k\,\mathrm{e}^{ik(\pi-\theta)/q}\right| \leqslant |1-\rho r^q| + \sum_{k=q+1}^{p} |a_k| r^k.$$

Si l'on suppose $r \leqslant \sqrt[q]{1/\rho}$, on a $|1-\rho r^q| = 1-\rho r^q$ et donc

$$|P(z)| - 1 \leqslant -\rho r^q + \sum_{k=q+1}^{p} |a_k| r^k.$$

Ce majorant définissant une fonction polynomiale de r, équivalente en 0 à $-\rho r^q$, il est strictement négatif au voisinage de 0. Par conséquent, il existe $z \in \mathbb{C}$ tel que $|P(z)| < 1 = m$, ce qui contredit la minimalité de m. Donc $m = 0$, c'est-à-dire $P(\alpha) = 0$. Par conséquent, le polynôme P possède bien au moins une racine complexe. ■

Un corps commutatif K est dit algébriquement clos lorsque tout polynôme de degré supérieur ou égal à 1 possède au moins une racine dans K. Le théorème de d'Alembert–Gauss énonce par conséquent que $\mathbb{C}$ est un corps algébriquement clos.

Plus généralement, on peut démontrer que tout corps commutatif admet une cloture algébrique, c'est-à-dire que pour tout corps commutatif K, il existe un plus petit sur-corps L de K qui est algébriquement clos.

La cloture algébrique de $\mathbb{R}$ est $\mathbb{C}$.

La cloture algébrique de $\mathbb{Q}$ est en revanche plus petite que $\mathbb{C}$: c'est un sous-corps dénombrable de $\mathbb{C}$, constitué des nombres dits algébriques (ce sont les nombres complexes qui sont racines d'un polynôme non nul à coefficients entiers relatifs). Les nombres $\sqrt{2}$ et i sont algébriques puisque racines respectives de X^2-2 et X^2+1.

Un nombre qui n'est pas algébrique est dit transcendant. Les nombres e et π sont transcendants (mais ce n'est pas évident à démontrer).

C.4. Décomposition primaire dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

La description des polynômes irréductibles est facile dans $\mathbb{C}[X]$, assez facile dans $\mathbb{R}[X]$ et difficile dans $\mathbb{Q}[X]$. Le programme de MPSI se limite aux deux premiers cas.

a) Factorisation sur $\mathbb{C}$

Le théorème de d'Alembert–Gauss permet de caractériser très simplement les polynômes irréductibles de $\mathbb{C}[X]$.

Proposition 37

Dans $\mathbb{C}[X]$, les polynômes irréductibles sont exactement les polynômes de degré 1, c'est-à-dire les polynômes P de la forme $P = aX + b$ avec $a, b \in \mathbb{C}$ et $a \neq 0$.

■ Si P est un polynôme de degré supérieur ou égal à 2, il possède dans $\mathbb{C}$ au moins deux racines α et β et admet donc au moins deux facteurs irréductibles $X - \alpha$ et $X - \beta$, ce qui lui interdit d'être irréductible. Donc P est nécessairement de degré 1. Un tel polynôme est bien irréductible. ■

On peut alors décrire la décomposition primaire dans $\mathbb{C}[X]$.

Proposition 38

Soit P un polynôme sur $\mathbb{C}$ dont le coefficient dominant est noté $a \in \mathbb{C}$. Si $\alpha_1, \dots, \alpha_k$ désignent toutes les racines distinctes de P, de multiplicités respectives $m_1, \dots, m_k$, le polynôme P se décompose sous la forme

$$P = a \prod_{j=1}^{k} (X - \alpha_j)^{m_j}.$$

On dit que $P \in K[X]$ est scindé sur K pour exprimer que c'est un produit de polynômes du premier degré de $K[X]$. Le résultat ci-dessus nous dit donc que tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

■ On associe le théorème de décomposition primaire et la proposition précédente. ■

Décomposer un polynôme sur $\mathbb{C}$ revient donc à déterminer ses racines et leurs multiplicités.

Nous verrons en exercice plusieurs méthodes pour déterminer les racines d'un polynôme. Outre les astucieuses (dont il serait difficile de faire une liste exhaustive ici), on peut noter qu'il existe des méthodes générales pour les polynômes de degré inférieur ou égal à 4 : pour les trinômes du second degré, on utilise bien évidemment la méthode classique de résolution des équations du second degré et pour les polynômes de degré 3 ou 4, on recourt plus souvent à la recherche de racines évidentes qu'aux méthodes générales (Tartaglia 1499–1557, Cardan 1501–1576) qui sont très techniques.

Enfin, il faut noter qu'un très beau théorème, dû à Abel (1802–1829), dit qu'il n'existe pas de méthode universelle pour trouver les racines des polynômes de degré supérieur ou égal à 5. Les travaux de Galois (1811–1832) permettent de préciser quelles équations sont résolubles.

Il découle du résultat ci-dessus que le pgcd de deux polynômes complexes A et B est le polynôme unitaire dont les racines sont les racines communes de A et B (comptées avec multiplicités). En particulier, deux polynômes complexes sont premiers entre eux si, et seulement si, ils n'ont pas de racines complexes en commun.

Exemples :

- On a vu que $A_1 = X^4 + X^3 - X^2 + X - 2$ admet quatre racines simples 1, -2, i et $-i$. Donc, dans $\mathbb{C}[X]$, on a $A_1 = 1(X-1)(X+2)(X-i)(X+i)$.
- Les racines de $X^n - 1$ sont les racines n-èmes de l'unité donc

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega).$$

b) Factorisation sur $\mathbb{R}$

Proposition 39

Soit P un polynôme à coefficients réels. Si α est une racine complexe de P, alors $\overline{\alpha}$ est également une racine de P et sa multiplicité est la même que celle de α.

■ Soient $A = a_n X^n + \cdots + a_1 X + a_0$ un polynôme à coefficients réels et $\alpha \in \mathbb{C}$. On a

$$\begin{aligned} A(\alpha) = 0 &\iff a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0 \\ &\iff \overline{a_n\alpha^n + \cdots + a_1\alpha + a_0} = \overline{0} \qquad \text{en conjuguant} \\ &\iff \overline{a_n}\,\overline{\alpha}^n + \cdots + \overline{a_1}\,\overline{\alpha} + \overline{a_0} = \overline{0} \\ &\iff a_n\overline{\alpha}^n + \cdots + a_1\overline{\alpha} + a_0 = 0 \qquad \text{car les } a_i \text{ sont réels} \\ &\iff A(\overline{\alpha}) = 0, \end{aligned}$$

ce qui démontre que α est une racine de A si, et seulement si, $\overline{\alpha}$ est une racine de A. Notons que deux assertions équivalentes étant vraies simultanément mais aussi fausses simultanément, on sait aussi que α n'est pas une racine de A si, et seulement si, $\overline{\alpha}$ n'est pas une racine de A.

En appliquant ce résultat à $A = P$, puis à $A = P'$, …, puis à $A = P^{(m-1)}$ et enfin à $A = P^{(m)}$, on obtient

$$\begin{aligned} &\big(P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \text{ et } P^{(m)}(\alpha) \neq 0\big) \\ \iff \quad &\big(P(\overline{\alpha}) = P'(\overline{\alpha}) = \cdots = P^{(m-1)}(\overline{\alpha}) = 0 \text{ et } P^{(m)}(\overline{\alpha}) \neq 0\big), \end{aligned}$$

ce qui correspond au résultat attendu. ■

Grande promo sur les racines de polynômes réels

On peut retenir de l'énoncé précédent que si l'on démontre que $\alpha \in \mathbb{C} \setminus \mathbb{R}$ est une racine de multiplicité m d'un polynôme à coefficients réels alors on sait, sans effort supplémentaire, que $\overline{\alpha}$ est également une racine de multiplicité m de ce polynôme.

Dans le cas où α est un nombre réel, l'énoncé précédent n'apporte rien.

On peut alors décrire les polynômes irréductibles de $\mathbb{R}[X]$.

Proposition 40

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont exactement les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif, c'est-à-dire les polynômes P de la forme

$$P = aX + b \qquad \text{ou} \qquad \begin{cases} P = aX^2 + bX + c \\ b^2 - 4ac < 0 \end{cases}$$

avec $a, b, c \in \mathbb{R}$ et $a \neq 0$.

■ Soit P un polynôme irréductible de $\mathbb{R}[X]$. Comme P n'est pas constant, le théorème de d'Alembert–Gauss permet de dire que P admet au moins une racine $\alpha \in \mathbb{C}$.

Si $\alpha \in \mathbb{R}$, alors $X - \alpha$ divise P et comme P est irréductible dans $\mathbb{R}[X]$, on en déduit que P et $X - \alpha$ sont associés, c'est-à-dire que P est un polynôme du premier degré. Un tel polynôme est bien irréductible.

Si $\alpha \in \mathbb{C} \setminus \mathbb{R}$, la proposition 39 nous dit que $\overline{\alpha}$ est aussi une racine de P. Mézalors, le polynôme $(X - \omega)(X - \overline{\omega}) = X^2 - 2\Re\mathrm{e}(\alpha)X + |\alpha|^2$ est un diviseur à coefficients réels de P donc, comme P est irréductible dans $\mathbb{R}[X]$, les polynômes P et $X^2 - 2\Re\mathrm{e}(\alpha)X + |\alpha|^2$ sont associés, c'est-à-dire que P est un polynôme de degré 2 à discriminant strictement négatif. Un tel polynôme est bien irréductible puisqu'une décomposition non triviale d'icelui utiliserait nécessairement un polynôme de degré 1 qui aurait donc une racine réelle. ■

La décomposition d'un polynôme réel dans $\mathbb{R}[X]$ est un peu plus compliquée que dans $\mathbb{C}[X]$.

Proposition 41

Soit P un polynôme sur $\mathbb{R}$ dont le coefficient dominant est noté $a \in \mathbb{R}$. Si $x_1, \dots, x_k$ désignent les racines réelles distinctes de P, de multiplicités respectives $n_1, \dots, n_k$, et si $\alpha_1, \overline{\alpha_1}, \dots, \alpha_h, \overline{\alpha_h}$ sont les racines complexes distinctes non réelles de P, de multiplicités respectives $m_1, \dots, m_h$, le polynôme P se décompose sous la forme

$$P = a \prod_{j=1}^{k} (X - x_j)^{n_j} \prod_{\ell=1}^{h} \left(X^2 - 2\Re\mathrm{e}(\alpha_\ell)X + |\alpha_\ell|^2\right)^{m_\ell}.$$

■ On associe le théorème de décomposition primaire et la proposition précédente. ■

Il découle du résultat ci-dessus que le pgcd de deux polynômes réels A et B est le polynôme unitaire dont les racines sont les racines communes de A et B dans $\mathbb{C}$ (comptées avec multiplicités). En particulier, deux polynômes réels sont premiers entre eux si, et seulement si, ils n'ont pas de racines complexes en commun.

La proposition ci-dessus dit que les polynômes de $\mathbb{R}[X]$ qui sont scindés sur $\mathbb{R}$ sont ceux n'admettant pas de racines complexes non réelles.

En pratique, pour factoriser un polynômes à coefficients réels P dans $\mathbb{R}[X]$, on commence par décomposer P dans $\mathbb{C}[X]$, puis, pour chaque couple $(\alpha, \overline{\alpha})$ de racines complexes non réelles, on développe le produit $(X - \alpha)(X - \overline{\alpha})$, de sorte que $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\Re\mathrm{e}(\alpha)X + |\alpha|^2$. On obtient ainsi une écriture de P sous forme d'un produit de polynômes du premier degré à coefficients réels (correspondant aux racines réelles) et de polynômes du second degré à coefficients réels (correspondant aux couples de racines complexes conjuguées).

Exemples :

- Décomposons $A_2 = X^4 - 2X^3 + 2X^2 - 2X + 1$ sur $\mathbb{C}$ puis sur $\mathbb{R}$.
  On a déjà vu que A_2 admettait une racine double : 1 et deux racines simples : i et $-i$. Donc A_2 se décompose dans $\mathbb{C}[X]$ sous la forme
  $$A_2 = (X - 1)^2(X - i)(X + i)$$
  et dans $\mathbb{R}[X]$ sous la forme
  $$A_2 = (X - 1)^2(X^2 + 1).$$
- Soit $A_3 = X^5 - X^3 - 4X^2 - 3X - 2$.
  On constate que $A_3(j) = 0$, $A_3'(j) = 0$ et $A_3''(j) \neq 0$. Donc j est une racine double de A_3. Comme A_3 est à coefficients réels, cela implique que $\overline{j} = j^2$ est aussi une racine double de A_3.
  On peut alors factoriser A_3 par $(X - j)^2(X - j^2)^2$, ce qui donne, après calculs, la décomposition sur $\mathbb{C}$ suivante :
  $$A_3 = (X - 2)(X - j)^2(X - j^2)^2,$$
  Comme $(X - j)(X - j^2) = X^2 + X + 1$, on obtient la décomposition sur $\mathbb{R}$ suivante :
  $$A_3 = (X - 2)(X^2 + X + 1)^2.$$

C. 5. Relations entre coefficients et racines

Définition 19

Soient $x_1, x_2, \dots, x_n \in K$. Pour tout $k \in [\![1; n]\!]$, la k-ème fonction symétrique élémentaire de $x_1, x_2, \dots, x_n$ est définie par

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

En particulier, on a

$$\sigma_1 = x_1 + x_2 + \cdots + x_n \qquad \text{et} \qquad \sigma_n = x_1 x_2 \cdots x_n.$$

Notons qu'il y a $\binom{n}{k}$ termes dans σ_k.

Exemples :

- Les fonctions symétriques élémentaires de x_1, x_2, x_3, x_4 sont

$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 + x_4 \\ \sigma_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 + x_1x_3 + x_2x_4 \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ \sigma_4 = x_1x_2x_3x_4 \end{cases}$$

La proposition suivante fait le lien entre les racines d'un polynôme et les fonctions symétriques élémentaires d'icelles.

Proposition 42

Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de $K[X]$ de degré n qui est scindé sur K. On note $\alpha_1, \alpha_2, \dots, \alpha_n$ les racines (non nécessairement distinctes) de P, de sorte que

$$P = a_n \prod_{j=1}^{n} (X - \alpha_j).$$

Alors, en notant $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires de $\alpha_1, \alpha_2, \dots, \alpha_n$, on a

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \qquad \sigma_2 = \frac{a_{n-2}}{a_n}, \qquad \dots \qquad , \ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, \qquad \dots \qquad , \ \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

■ Il suffit de développer et d'identifier. ■

Exemples :

- Dans le cas des trinômes du second degré, on retrouve que si α_1 et α_2 sont les racines de $aX^2 + bX + c$ alors $\alpha_1 + \alpha_2 = -b/a$ et $\alpha_1\alpha_2 = c/a$.
- Si α, β, γ sont les racines de $X^3 + X^2 - 4$, alors $\alpha + \beta + \gamma = -1$, $\alpha\beta + \beta\gamma + \gamma\alpha = 0$ et $\alpha\beta\gamma = 4$. Cela permet, par exemple, de calculer $\alpha^2 + \beta^2 + \gamma^2$, de la façon suivante :

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = 1.$$

Il faut savoir que toute expression polynomiale symétrique en les racines d'un polynôme peut s'exprimer de façon polynomiale à l'aide des fonctions symétriques élémentaires et donc des coefficients des polynômes (c'est un résultat difficile à démontrer). En particulier, une telle expression appartient au même corps que les coefficients du polynôme : ainsi la somme des racines d'un polynôme à coefficients réels est réelle même si ces racines ne le sont pas nécessairement.

D. Polynômes d'interpolation de Lagrange

Vous savez, depuis tout petit, que par deux points distincts du plan passe une et une seule droite. Vous avez peut-être également vu en exercice de Terminale que par trois points du plan, d'abscisses distinctes, passe une et une seule parabole d'équation $y = a^2x+bx+c$. L'énoncé suivant généralise ce résultat à un plus grand nombre de points.

Proposition 43

Soient $x_1, x_2, \dots, x_n$ des éléments distincts de K et $y_1, y_2, \dots, y_n$ d'autres éléments de K (ceux-là ne sont pas nécessairement distincts).

Il existe un unique polynôme L sur K, de degré inférieur ou égal à $n-1$, tel que, pour tout $i \in [\![1;n]\!]$, on ait $L(x_i) = y_i$. On l'appelle le polynôme d'interpolation de Lagrange du nuage de points $\big((x_i, y_i)\big)_{i\in[\![1;n]\!]}$. Il est donné par

$$L = y_1L_1 + y_2L_2 + \cdots + y_nL_n,$$

où, pour tout $k \in [\![1;n]\!]$, L_k désigne le polynôme

$$L_k = \prod_{\substack{j=1\\ j\neq k}}^{n} \frac{X - x_j}{x_k - x_j}.$$

En outre, les autres polynômes P (de degré quelconque) vérifiant $\forall k \in [\![1;n]\!]\,,\ P(x_k) = y_k$ sont donnés par $P = L + (X-x_1)\cdots(X-x_n)Q$ où Q parcourt $K[X]$.

■ Notons tout d'abord que $\deg(L) \leqslant n-1$ puisque tous les L_k sont de degré $n-1$. Par ailleurs, pour tout $k \in [\![1;n]\!]$, on a

$$L(x_i) = \sum_{k=1}^{n} y_kL_k(x_i) = \sum_{k=1}^{n} y_k \prod_{\substack{j=1\\ j\neq k}}^{n} \frac{x_i - x_j}{x_k - x_j} = \sum_{\substack{k=1\\ k\neq i}}^{n} y_k \prod_{\substack{j=1\\ j\neq k}}^{n} \frac{x_i - x_j}{x_k - x_j} + y_i \prod_{\substack{j=1\\ j\neq k}}^{n} \frac{x_i - x_j}{x_i - x_j} = \sum_{\substack{i=1\\ i\neq k}}^{n} y_k \times 0 + y_i \times 1 = y_i,$$

ce qui démontre que $\forall k \in [\![1;n]\!]\,,\ L(x_k) = y_k$. D'où l'existence du polynôme interpolateur de Lagrange.

Soit M un polynôme de degré inférieur ou égal à $n-1$ tel que $\forall i \in [\![1;n]\!]\,,\ M(x_i) = y_i$. Le polynôme $M-L$ est alors de degré inférieur ou égal à $n-1$ et il admet n racines (les x_i), ce qui prouve que $L-M = 0$ et donc $L = M$. D'où l'unicité du polynôme interpolateur de Lagrange.

Dire qu'un polynôme P vérifie $\forall k \in [\![1;n]\!]\,,\ P(x_k) = y_k$ est équivalent à dire que le polynôme $P-L$ admet les x_i comme racines, ou encore que $P-L$ se factorise sous la forme $P-L = (X-x_1)\cdots(X-x_n)Q$ où $Q \in K[X]$. D'où le résultat attendu. ■

Comment retenir un pareil résultat ? En fait, ce n'est pas si difficile !

À la base, il faut retenir que, pour tout $k \in [\![1;n]\!]$, L_k est un polynôme de degré $n-1$ caractérisé par le fait que $\forall \ell \in [\![1;n]\!]\,,\ L_k(x_\ell) = \delta_{k,\ell}$ où $\delta_{k,\ell}$ désigne le symbole de Kronecker qui vaut 1 si $k = \ell$ et 0 sinon. Autrement dit, la fonction polynomiale associée à L_k s'annule sur tous les x_j sauf x_k, sur lequel elle vaut 1. Le polynôme L_k admet donc tous les x_j comme racines, sauf x_k. Comme il est de degré $n-1$, il s'écrit $L_k = a(X-x_1)\cdots(X-x_{k-1})(X-x_k)\cdots(X-x_n)$ où $a \in K$. La condition $L_k(x_k) = 1$ impose alors que $a = 1/(x_k-x_1)\cdots(x_k-x_{k-1})(x_k-x_k)\cdots(x_k-x_n)$, ce qui fournit l'expression de L_k.

Ensuite, l'interpolation consiste à combiner les polynômes L_k en attribuant à L_k un poids égal à y_k de sorte qu'en x_k, la valeur obtenue soit celle donnée par le terme y_kL_k, c'est-à-dire $y_k \times 1 = y_k$.

Exemples :

- Soient $a, b, c \in K$ distincts et $\alpha, \beta, \gamma \in K$. Le polynôme interpolateur L tel que $L(a) = \alpha$, $L(b) = \beta$ et $L(c) = \gamma$ est donné par

$$L = \alpha\frac{(X-b)(X-c)}{(a-b)(a-c)} + \beta\frac{(X-c)(X-a)}{(b-c)(b-a)} + \gamma\frac{(X-a)(X-b)}{(c-a)(c-b)}.$$

10 h 45