

Polynômes

Le programme se restreint au cas où $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} , mais la plupart des résultats restent vrais sur un corps quelconque. Par conséquent, dans la suite, \mathbb{K} désignera \mathbb{R} ou \mathbb{C} , mais les résultats restent vrais sur un corps \mathbb{K} quelconque. Lorsque ce ne sera pas le cas (il faut parfois que le corps soit infini ou de caractéristique nulle, cf. exercice 66 du chapitre 18), nous le dirons explicitement.

Et même sur un anneau, cf. paragraphe I.6.

I L'anneau $\mathbb{K}[X]$

I.1 Suites presque nulles et polynômes

Définition. Une suite $(a_n)_{n \in \mathbb{N}}$ à valeurs dans \mathbb{K} est presque nulle si elle est nulle à partir d'un certain rang.

Remarque : En d'autres termes, une suite $(a_n)_{n \in \mathbb{N}}$ est presque nulle s'il existe $n_0 \in \mathbb{N}$ tel que, pour tout $n \geq n_0$, $a_n = 0$. Encore en d'autres termes, une suite est presque nulle lorsque l'ensemble des indices n tels que $a_n \neq 0$ est majoré. D'après le chapitre 17, on en déduit qu'une suite est presque nulle si et seulement si elle n'admet qu'un nombre fini de termes non nuls (possiblement aucun).

Notation : Nous noterons parfois (jusqu'à l'arrivée de X dans le paragraphe I.3) une suite presque nulle $(a_n)_{n \in \mathbb{N}}$ sous la forme $(a_0, a_1, a_2, \dots, a_n, \dots)$ tout en ayant conscience que cette suite est nulle à partir d'un certain rang. Ainsi, une suite presque nulle est une suite de la forme $(a_0, \dots, a_d, 0, 0, \dots)$.

Cette définition est encore valable sur un corps quelconque en notant 0 le neutre pour l'addition $0_{\mathbb{K}}$. On peut également noter 1 le neutre du produit $1_{\mathbb{K}}$, ce qui généralise les résultats suivants (en particulier ceux concernant le produit) à un corps quelconque.

Définition. Un polynôme (à coefficients dans \mathbb{K}) est une suite presque nulle à valeurs dans \mathbb{K} . Si $(a_n)_{n \in \mathbb{N}}$ est un polynôme (donc une suite presque nulle) et si $k \in \mathbb{N}$, on dit que a_k est son coefficient d'indice k ou d'ordre k .

On peut prendre la convention $a_d \neq 0$, mais cela n'est possible que pour une suite non nulle. Il paraît plus simple de ne pas se demander si les a_k sont nuls ou non : l'écriture ci-contre ne sous-entendra jamais que les a_k sont non nuls, seul compte le fait qu'à partir d'un certain rang, les termes sont tous nuls, on se fiche des termes précédents.

Remarques :

- Cette définition n'est pas si surprenante qu'elle en a l'air : on dit simplement qu'un polynôme est **égal**, par définition, à la suite de ses coefficients. C'est tout de même assez intuitif : on se dit qu'un polynôme est entièrement déterminé par ses coefficients, et que toutes les opérations qu'on a envie de faire avec des polynômes (somme, produit etc.) peuvent s'écrire à l'aide des coefficients. On suit donc cette idée et on va encore plus loin en disant donc qu'un polynôme est, par définition, la suite de ses coefficients.
- Vous avez bien lu : un polynôme n'est pas une fonction ! L'inconvénient d'une fonction est qu'elle a besoin d'un domaine de définition. Or, en gros, quand on parle de polynômes, on pense à des puissances, à des multiplications, à des sommes, opérations qu'on peut faire dans des ensembles extrêmement variés (des anneaux : on peut d'ailleurs définir de la même façon des polynômes à coefficients dans un anneau, cf. paragraphe I.6) : la définition d'un polynôme comme une suite presque nulle permet d'appliquer des polynômes à des éléments très variés, dans des anneaux quelconques, ce qui nous confère une plus grande liberté que si on étudiait simplement une fonction polynomiale définie sur un ensemble précis.
- Mais rassurez-vous : on pourra toujours évaluer un polynôme en 1.
- Dans la suite, quand on parlera de polynôme, il sera sous-entendu (sauf indication contraire) qu'on parlera de polynômes à coefficients dans \mathbb{K} .

Ou en $1_{\mathbb{K}}$ sur un corps quelconque, qu'on pourra toujours noter 1.

Proposition. Deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients.

DÉMONSTRATION. Découle de la définition : deux suites (qu'elles soient presque nulles ou non) $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ sont égales si et seulement si $a_n = b_n$ pour tout n .

I.2 Opérations algébriques

Pour la somme et le produit par un scalaire (i.e. un élément de \mathbb{K}), ce sont les opérations habituelles sur des suites de façon analogue à celles vues pour les suites (réelles ou complexes) dans le chapitre 12.

Définition. Soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes. On définit la somme de P et Q , que l'on note $P + Q$, par : $P + Q = (a_n + b_n)_{n \in \mathbb{N}}$. En d'autres termes, pour sommer des polynômes, on somme leurs coefficients.

Définition. Soient $P = (a_n)_{n \in \mathbb{N}}$ un polynôme et $\lambda \in \mathbb{K}$ un scalaire. On définit le produit de P par λ , que l'on note λP , par : $\lambda P = (\lambda \times a_n)_{n \in \mathbb{N}}$.

Remarque : Le fait que ce soit encore une suite presque nulle est immédiat. On trouve également parfois les notations $\lambda \times P$ ou $\lambda.P$.

Définition. Soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes. On définit le produit de P et Q , que l'on note $P \times Q$ ou plus simplement PQ , par : $P \times Q = (c_n)_{n \in \mathbb{N}}$ où, pour tout $n \in \mathbb{N}$,

$$c_n = \sum_{k=0}^n a_k \times b_{n-k}$$

Remarque : En d'autres termes, $P \times Q$ est le polynôme dont le coefficient d'ordre n est

$$c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-2} b_2 + a_{n-1} b_1 + a_n b_0$$

Montrons que cela définit bien un polynôme i.e. que la suite $(c_n)_{n \in \mathbb{N}}$ est bien une suite presque nulle. Reprenons les entiers n_0 et n_1 introduits dans la marge ci-dessus et notons $n_2 = n_1 + n_0 - 1$ (le raisonnement est le même que pour les éléments nilpotents dans le chapitre 18). Soit $n \geq n_2$ et soit $k \in \llbracket 0; n_2 \rrbracket$.

- Si $k \geq n_0$ alors $a_k = 0$ donc $a_k \times b_{n-k} = 0$.
- Si $k \leq n_0 - 1$ alors $n - k \geq n_2 - n_0 + 1 = n_1$ donc $b_{n-k} = 0$ si bien que $a_k \times b_{n-k} = 0$.

En d'autres termes, c_n est une somme de termes nuls donc est nul dès que $n \geq n_2$: la suite $(c_n)_{n \in \mathbb{N}}$ est bien une suite presque nulle.

Définition. Soit P un polynôme et soit $n \geq 1$. On définit le polynôme P^n par :

$$P^n = \underbrace{P \times \cdots \times P}_{n \text{ fois}}$$

Remarque : Cette notation vérifie les propriétés habituelles des puissances, par exemple $P^{n+m} = P^n \times P^m$ pour tous n et m . Comme dit ci-contre, cela découle de l'associativité du produit qui sera montrée au paragraphe I.5.

Définition. Soit $P = (a_n)_{n \in \mathbb{N}}$ un polynôme. On dit qu'il est constant si $a_n = 0$ dès que $n \geq 1$. En d'autres termes, P est constant s'il existe $\lambda \in \mathbb{K}$ tel que $P = (\lambda, 0, \dots, 0)$. Dans le cas où $\lambda = 0$ i.e. dans le cas où P est la suite nulle, on dit que P est le polynôme nul.

On commence à voir l'intérêt de la définition d'un polynôme comme une suite : ce qui est immédiat à prouver pour une suite le serait beaucoup moins si on considérait un polynôme comme une fonction !

$P+Q$ est encore une suite presque nulle : il existe (n_0, n_1) tel que pour tout $n \geq n_0, a_n = 0$ et pour tout $n \geq n_1, b_n = 0$. Il suffit de poser $n_2 = \max(n_0, n_1)$ pour avoir : $\forall n \geq n_2, a_n + b_n = 0$.

Cette définition est peut-être moins intuitive que celle de la somme ou celle du produit par un scalaire mais elle ne sort pas de nulle part, elle est tout à fait naturelle une fois que l'on dispose de la notation X , cf. paragraphe I.3.

Bon, comme dit dans le chapitre 18, cette définition présuppose l'associativité du produit, que nous prouverons dans le paragraphe I.5.

Notation : Si P est constant égal à $(\lambda, 0, 0, \dots)$, on dit que P est constant égal à λ . On note parfois $P = \tilde{\lambda}$ pour insister sur le fait que P n'est pas un élément de \mathbb{K} mais une suite (ou quand on manipulera des fonctions polynomiales, cf. paragraphe IV, mais par souci de simplicité, on écrit quand même la plupart du temps que $P = \lambda$. En particulier, $P = 0$ est le polynôme nul et $P = 1$ est le polynôme constant égal à 1.

Proposition. Soit $P = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$ et soit $\lambda \in \mathbb{K}$. Notons Q le polynôme constant égal à λ . Alors $P \times Q = Q \times P = \lambda P = (\lambda a_n)_{n \in \mathbb{N}}$.

DÉMONSTRATION. Rappelons que le polynôme constant égal à λ est $Q = (\lambda, 0, 0, \dots)$ i.e. le polynôme $(b_n)_{n \in \mathbb{N}}$ avec $b_0 = \lambda$ et $b_k = 0$ si $k \neq 0$. Notons $P \times Q = (c_n)_{n \in \mathbb{N}}$. Soit $n \in \mathbb{N}$.

$$\begin{aligned} c_n &= \sum_{k=0}^n a_k \times b_{n-k} \\ &= a_n \times b_0 \quad (\text{les autres termes sont nuls}) \\ &= \lambda a_n \end{aligned}$$

En d'autres termes, un polynôme est constant si tous ses coefficients à partir du rang 1 sont nuls, et le polynôme nul est l'unique polynôme dont tous les coefficients sont nuls.

En d'autres termes, on obtient le même résultat en multipliant par le scalaire λ ou le polynôme constant égal à λ : c'est pour cela qu'on les note de la même façon !

c'est-à-dire que $P \times Q = \lambda P$ et on montre de même que $Q \times P = \lambda P$.

Définition. Par convention, si P est polynôme, on pose $P^0 = 1$. En d'autres termes, par convention, P^0 est le polynôme constant égal à 1 i.e. $P^0 = (1, 0, 0, \dots)$.

I.3 Notation X , notion d'indéterminée

Définition. On note X le polynôme $X = (0, 1, 0, 0, \dots)$.

Remarques :

- X n'est pas une variable (au sens fonctionnelle) ni un élément de \mathbb{K} , c'est un polynôme (donc une suite presque nulle) bien précis auquel on choisit de donner un nom particulier, dont le but est évidemment l'analogie avec les fonctions polynomiales.
- En particulier, X n'étant pas une variable ni un élément de \mathbb{K} , il ne doit pas être quantifié ni être utilisé pour résoudre des équations. Écrire « $X = 0$ » ou « $\forall X \in \mathbb{K}$ » ou toute autre horreur du même genre est passible de châtiments corporels !
- X est appelée « l'indéterminée » c'est-à-dire (en termes plus simples mais ça rend moins bien) « le truc qu'on met après les coefficients » (voir ci-dessous) ou « la lettre qu'on utilise pour représenter les polynômes autrement que comme des suites ». C'est un choix purement arbitraire (mais pas tant que ça puisque la motivation est de rappeler les fonctions polynomiales) et on pourrait l'appeler autrement et parfois on le fait, c'est-à-dire qu'on pourrait appeler l'indéterminée Y , T etc. mais il faut bien reconnaître que dans 99.99% des cas, on la note X . On ne l'appelle différemment en général que quand le X est déjà pris (mais c'est très rare), cf. paragraphe I.6.

En d'autres termes, X est la suite presque nulle $(a_n)_{n \in \mathbb{N}}$ définie par $a_1 = 1$ et $a_n = 0$ pour tout $n \neq 1$.

⚠ X n'est pas un nombre ! De façon générale, un polynôme est une suite (presque nulle), pas un nombre ! Il n'y a que pour les polynômes constants (et X n'en est pas un) que l'on tolère l'écriture $P = \lambda$.

Proposition. $\forall n \in \mathbb{N}, X^n = (0, \dots, 0, 1, 0, \dots)$ où le n est en position n .

Remarque : Attention, la numérotation commence en 0 ! Par exemple, $X^0 = (1, 0, 0, \dots)$ et $X^1 = (0, 1, 0, 0, \dots)$.

DÉMONSTRATION. Par récurrence sur n .

- Si $n \in \mathbb{N}$, notons $H_n : \langle X^n = (0, \dots, 0, \underbrace{1}_n, 0, \dots) \rangle$.

- Puisque, par convention, $X^0 = 1 = (1, 0, 0, \dots)$ et que, par définition, $X^1 = X = (0, 1, 0, 0, \dots)$, H_0 et H_1 sont vraies.
- Soit $n \geq 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Tout d'abord, $X^{n+1} = X \times X^n$. Notons $X = (a_p)_{p \in \mathbb{N}}$ (on évite la notation n pour l'indice, mais p n'est pas forcément un nombre premier), $X^n = (b_p)_{p \in \mathbb{N}}$ et $X^{n+1} = (c_p)_{p \in \mathbb{N}}$. Soit $p \in \mathbb{N}$. Alors

$$c_p = \sum_{k=0}^n a_k \times b_{p-k} \quad \square$$

Or, $a_1 = 1$ et $a_k = 0$ si $k \neq 1$ si bien que $c_p = b_{p-1}$. Par hypothèse de récurrence, $b_{p-1} = 1$ si $p-1 = n$ et 0 sinon donc $c_p = 1$ si $p = n+1$ et 0 sinon. En d'autres termes, $X^{n+1} = (0, \dots, 0, \underbrace{1}_{n+1}, 0, \dots) : H_{n+1}$ est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$.

I.4 Notation des polynômes

La proposition ci-dessus nous permet d'écrire un polynôme sous une forme qui nous permettra de les manipuler plus facilement (en plus de renforcer la ressemblance avec les fonctions polynomiales) :

Corollaire. Soit $P = (a_n)_{n \in \mathbb{N}}$ un polynôme. Alors

$$P = \sum_{k=0}^{+\infty} a_k X^k,$$

cette somme ayant un sens puisqu'elle est en fait finie, les a_n étant nuls à partir d'un certain rang.

Cette notation présuppose l'associativité de la somme. Nous en parlerons dans le paragraphe I.5.

DÉMONSTRATION. Par définition, $P = (a_0, a_1, a_2, \dots)$ donc, d'après ce qui précède,

$$\begin{aligned} P &= a_0(1, 0, 0, 0, \dots) + a_1(0, 1, 0, 0, \dots) + a_2(0, 0, 1, 0, \dots) + \dots \\ &= a_0 \times 1 + a_1 \times X + a_2 \times X^2 + \dots \end{aligned} \quad \square$$

La somme est en fait finie : aucun problème avec les petits points !

ce qui permet de conclure.

Cette notation permet de travailler avec les lois de façon plus intuitive, comme dans \mathbb{Z} , \mathbb{R} ou \mathbb{C} :

- Pour la somme : soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes. Par définition, $P + Q = (a_n + b_n)_{n \in \mathbb{N}}$. Avec l'écriture ci-dessus, cela se traduit de la façon suivante :

$$\sum_{k=0}^{+\infty} a_k X^k + \sum_{k=0}^{+\infty} b_k X^k = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$$

- Pour la multiplication par un scalaire, c'est encore plus simple : si $P = (a_n)_{n \in \mathbb{N}}$ est un polynôme et $\lambda \in \mathbb{K}$ est un scalaire, alors $\lambda P = (\lambda \times a_n)_{n \in \mathbb{N}}$. Avec l'écriture ci-dessus, cela se traduit de la façon suivante :

$$\lambda \sum_{k=0}^{+\infty} a_k X^k = \sum_{k=0}^{+\infty} (\lambda \times a_k) X^k$$

- Pour le produit :

$$\sum_{n=0}^{+\infty} a_n X^n \times \sum_{n=0}^{+\infty} b_n X^n = \sum_{n=0}^{+\infty} c_n X^n$$

où, pour tout n ,

$$c_n = \sum_{k=0}^n a_k \times b_{n-k}$$

Remarque : La plupart du temps, cette somme étant finie, nous écrirons : « soit $P = \sum_{k=0}^n a_k X^k$ » ce qui signifiera : « soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et soit n tel que, pour tout $k \geq n+1$, $a_k = 0$ ». Attention, cela ne signifie pas que $a_n \neq 0$ (il faudra attendre pour cela la notion de degré) et il ne faut pas perdre de vue que le n dépend de P , si on prend un autre polynôme Q , il faut prendre un autre entier m (quitte ensuite à prendre le maximum de n et m). La somme infinie fait disparaître cette difficulté mais il faut reconnaître qu'il est plus intuitif de travailler avec des sommes finies qu'avec des sommes infinies (même si celles-ci sont en fait finies). Les relations précédentes deviennent alors :

- Pour la somme : on note $P = \sum_{k=0}^n a_k X^k$ et $Q = \sum_{k=0}^m b_k X^k$. Si $m > n$, alors

$$P + Q = \sum_{k=0}^n (a_k + b_k) X^k + \sum_{k=n+1}^m b_k X^k$$

De même si $n > m$, tandis que si $n = m$:

$$P + Q = \sum_{k=0}^n (a_k + b_k) X^k$$

Il est en fait inutile de différencier les cas : on peut se contenter de supposer sans perte de généralité que $m \geq n$ et écrire

$$P + Q = \sum_{k=0}^n (a_k + b_k) X^k + \sum_{k=n+1}^m b_k X^k$$

tout en étant conscient que la deuxième somme est indexée par l'ensemble vide donc nulle si $n = m$.

- Pour la multiplication par un scalaire : on a alors $\lambda P = \sum_{k=0}^n (\lambda \times a_k) X^k$.
- Pour le produit : avec les notations ci-dessus, on obtient

$$P \times Q = \sum_{k=0}^{n+m} c_k X^k$$

où, pour tout k , c_k est défini comme ci-dessus.

Avant d'adopter définitivement cette notation et de travailler sereinement, nous devons prouver que la somme et le produit vérifient les propriétés que nous avons envie d'utiliser avec une telle notation, par exemple la distributivité du produit sur la somme.

I.5 L'anneau $\mathbb{K}[X]$

C'est-à-dire que $a_k = 0$ si $k > n$ et $b_k = 0$ si $k > m$.

On prouve comme ci-dessus que $c_k = 0$ dès que $k \geq n + m$.

Définition. On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .

Remarque : L'ensemble $\mathbb{K}[X]$ est parfois appelé l'ensemble (ou l'anneau, voir ci-dessous) des polynômes à une indéterminée.

Théorème. $(\mathbb{K}[X], +, \times)$ est un anneau intègre commutatif, le neutre pour la somme étant le polynôme nul et le neutre pour le produit étant le polynôme constant égal à 1.

DÉMONSTRATION. • On sait déjà (cf. chapitre 18) que la suite nulle est l'élément neutre pour l'addition sur $\mathbb{K}^{\mathbb{N}}$ donc elle l'est sur l'ensemble plus petit $\mathbb{K}[X]$.

- Idem, on sait déjà que la somme est associative et il est immédiat qu'elle est commutative.
- On a déjà prouvé plus haut que la somme de deux suites presque nulles est presque nulle : la somme est interne. Idem pour le produit.
- Si $P = (a_n)_{n \in \mathbb{N}}$ est un polynôme, il est immédiat que $-P = (-a_n)_{n \in \mathbb{N}}$ est le symétrique de P pour la somme. En d'autres termes, $(\mathbb{K}[X], +)$ est un groupe abélien.
- Soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes. Notons $P \times Q = (c_n)_{n \in \mathbb{N}}$ et $Q \times P = (d_n)_{n \in \mathbb{N}}$. Soit $n \in \mathbb{N}$.

$$\begin{aligned} c_n &= \sum_{k=0}^n a_k \times b_{n-k} \\ &= \sum_{j=0}^n a_{n-j} \times b_j \quad (j = n - k) \\ &= \sum_{j=0}^n b_j \times a_{n-j} \quad (\mathbb{K} \text{ est commutatif}) \\ &= d_n \end{aligned}$$

c'est-à-dire que $P \times Q = Q \times P$: le produit est commutatif.

- On a déjà montré plus haut que $1 \times P = P \times 1 = P$: 1 est bien le neutre pour le produit.
- Soient $P = (P_n)_{n \in \mathbb{N}}$, $Q = (Q_n)_{n \in \mathbb{N}}$ et $R = (R_n)_{n \in \mathbb{N}}$ trois polynômes. Notons $P \times Q = ((PQ)_n)_{n \in \mathbb{N}}$ (à ne pas confondre avec $P_n \times Q_n$), etc. Soit $n \in \mathbb{N}$.

$$\begin{aligned} ((PQ)R)_n &= \sum_{k=0}^n (PQ)_k R_{n-k} \\ &= \sum_{k=0}^n \left(\sum_{i=0}^k (P_i Q_{k-i}) \right) R_{n-k} \\ &= \sum_{k=0}^n \sum_{i=0}^k ((P_i Q_{k-i}) R_{n-k}) \quad (\text{produit distributif sur la somme dans } \mathbb{K}) \\ &= \sum_{k=0}^n \sum_{i=0}^k P_i (Q_{k-i} R_{n-k}) \quad (\text{produit associatif dans } \mathbb{K}) \\ &= \sum_{i=0}^n P_i \sum_{k=i}^n Q_{k-i} R_{n-k} \quad (\text{intersion de sommes}) \end{aligned}$$

Par soucis de simplicité, pour l'associativité du produit et la distributivité du produit sur la somme, on n'introduit pas de nouvelle lettre et on adopte des notations transparentes : $(PQ)_n$ est le coefficient d'ordre n de PQ etc.

$$\begin{aligned}
&= \sum_{i=0}^n P_i \sum_{j=0}^{n-i} Q_j R_{n-i-j} \quad (j = k - i) \\
&= \sum_{i=0}^n P_i (QR)_{n-i} \\
&= (P(QR))_n
\end{aligned}$$

c'est-à-dire que le produit est associatif.

- Avec les mêmes notations que ci-dessus :

$$\begin{aligned}
(P(Q + R))_n &= \sum_{k=0}^n P_k (Q + R)_{n-k} \\
&= \sum_{k=0}^n P_k (Q_{n-k} + R_{n-k}) \\
&= \sum_{k=0}^n (P_k Q_{n-k} + P_k R_{n-k}) \quad (\text{le produit est distributif sur la somme dans } \mathbb{K}) \\
&= \sum_{k=0}^n P_k Q_{n-k} + \sum_{k=0}^n P_k R_{n-k} \\
&= (PQ)_n + (PR)_n
\end{aligned}$$

On justifie a posteriori le bien-fondé de la notation P^n vue au paragraphe I.2.

□

et on conclut comme précédemment que le produit est distributif à gauche (donc distributif car commutatif) par rapport à la somme.

- L'intégrité sera prouvée au paragraphe II.2.

Remarque : Toutes les propriétés qui font de $\mathbb{K}[X]$ un anneau permettent de travailler comme sur \mathbb{Z} , \mathbb{R} ou \mathbb{C} (sauf la division pour ces deux derniers). Pour s'en rendre compte, il suffit d'écrire P et Q sous la forme plus intuitive suivante :

$$P = a_0 + a_1X + \cdots + a_nX^n \quad \text{et} \quad Q = b_0 + b_1X + \cdots + b_mX^m$$

Dès lors, en utilisant la distributivité du produit par rapport à la somme :

$$\begin{aligned}
P \times Q &= (a_n \times b_m)X^{n+m} + (a_n \times b_{m-1} + a_{n-1} \times b_m)X^{n+m-1} \\
&\quad + (a_n \times b_{m-2} + a_{n-1} \times b_{m-1} + a_{n-2} \times b_m)X^{n+m-2} + \cdots + a_0 \times b_0
\end{aligned}$$

On peut facilement prouver que l'expression ci-dessus est celle qui est obtenue avec la définition du produit donnée au paragraphe I.2. Par exemple, le terme de degré $n + m - 1$ est égal à

$$\sum_{k=0}^{n+m-1} a_k b_{n+m-1-k}$$

et on prouve comme au paragraphe I.2 que tous les termes sauf ceux d'indices n et $n - 1$ sont nuls si bien que ce coefficient est bien égal à $a_{n-1}b_m + a_nb_{m-1}$.

Morale de l'histoire : On écrira en général un polynôme sous la forme

$$P = \sum_{k=0}^n a_k X^k = a_n X^n + \cdots + a_1 X + a_0$$

Sans perdre de vue qu'un polynôme n'est pas une fonction, ce n'est qu'une façon plus pratique d'écrire la suite presque nulle $(a_0, \dots, a_n, 0, 0 \dots)$.

et on pourra sommer et multiplier comme dans un anneau commutatif quelconque (par exemple, comme dans \mathbb{Z}), y compris appliquer les identités remarquables et le binôme de Newton. Finalement, malgré une définition qui pourrait faire un peu peur, travailler avec des polynômes est en fait extrêmement simple !

Exemples :

- Dans $\mathbb{C}[X]$, posons $P = 4X^3 + X^2 + 1$ et $Q = 3X^2 - X + 5$. Alors :

$$P + Q = 4x^3 + 4X^2 - X + 6 \quad \text{et} \quad P \times Q = 12X^5 - X^4 + 4X^3 + 8X^2 - X + 6$$

De plus :

$$\begin{aligned} P^2 &= (4X^3)^2 + (X^2)^2 + 1^2 + 2 \times 4X^3 \times X^2 + 2 \times 4X^3 \times 1 + 2 \times X^2 \times 1 \\ &= 16X^6 + 8X^5 + X^4 + 8X^3 + 2X^2 + 1 \end{aligned}$$

- Donnons un exemple dans un corps différent de \mathbb{R} ou \mathbb{C} : posons $P = X^2 + X + 1 \in \mathbb{K}[X]$ où $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$. Alors $P + P = 0$ et

$$P^2 = X^4 + X^2 + 1$$

En effet, on peut soit développer avec les doubles produits en se souvenant que, dans $\mathbb{Z}/2\mathbb{Z}$, $2 = 0$, ou se souvenir de son cours d'arithmétique : quand on travaille modulo 2 (ou plus généralement modulo p premier), $(a + b)^2 = a^2 + b^2$ modulo 2 (plus généralement $(a + b)^p = a^p + b^p$ modulo p).

Rappelons que dans $\mathbb{Z}/2\mathbb{Z}$, $1 + 1 = 0$.

I.6 Polynômes à coefficients dans un anneau (\pm HP)

I.6.a Cas général (HP⁻)

Dans la démonstration du théorème ci-dessus, nous n'avons pas utilisé les inversibles de \mathbb{K} pour la loi \times , nous n'avons utilisé que la structure d'anneau (intègre commutatif) :

- L'existence de 0 i.e. d'un neutre pour l'addition, la commutativité, l'associativité de la somme et l'existence d'un symétrique. En clair : la structure de groupe abélien pour la loi $+$.
- L'associativité et la commutativité du produit.
- L'existence d'un élément neutre pour le produit.
- La distributivité du produit sur la somme.
- L'intégrité (même si le fait que $\mathbb{K}[X]$ est un anneau intègre ne sera prouvé qu'au paragraphe II.2).

Dès lors, rien ne nous empêche de recommencer avec un anneau (intègre commutatif) A à la place du corps \mathbb{K} , tout ce qui précède sera encore valable. On se donne dans ce paragraphe un anneau A commutatif et intègre (qu'on pourra identifier à \mathbb{Z} pour se faire une idée si on en ressent le besoin).

Définition. Un polynôme (à coefficients dans A) est une suite presque nulle à valeurs dans A . Si $(a_n)_{n \in \mathbb{N}}$ est un polynôme (donc une suite presque nulle) et si $k \in \mathbb{N}$, on dit que a_k est son coefficient d'indice k ou d'ordre k .

Remarque : Tout ce qui précède (mais pas tout ce qui suit) est encore valable en remplaçant \mathbb{K} par A :

- Il y a unicité des coefficients.
- On peut définir une somme, un produit par un scalaire, et un produit de la même façon. Idem pour les puissances.

Attention, tout ce qui suit ne sera pas forcément valable ! En particulier, toute la partie arithmétique des polynômes n'est pas valable sur un anneau. Nous préciserons à chaque fois ce qui reste valable et ce qui ne l'est pas.

- On définit X de la même façon, et on a le même résultat concernant les X^n , ce qui permet de noter les polynômes de la même façon.
- On note $A[X]$ l'ensemble des polynômes à coefficients dans A , et c'est encore un anneau intègre commutatif.

Remarque : L'étude des polynômes à coefficients dans un anneau n'est pas la même que celle pour les polynômes à coefficients dans un corps et est intéressante en elle-même (ce n'est pas pour rien qu'elle est hors programme), nous n'en parlons ici que pour pouvoir considérer des éléments de $\mathbb{Z}[X]$ sans nous poser de questions (ce qui arrive souvent dans les sujets ou exercices de concours) : ce sont des polynômes comme les autres, ils sont simplement à coefficients dans \mathbb{Z} , et $\mathbb{Z}[X]$ est aussi un anneau commutatif et intègre.

Exemple : $X^3 + X + 1 \in \mathbb{Z}[X]$.

I.6.b Polynômes à plusieurs indéterminées (HP⁺)

On vient de voir qu'on peut définir des polynômes à coefficients dans un anneau A de la même façon que des polynômes à coefficients dans un corps \mathbb{K} . Puisque $\mathbb{K}[X]$ est un anneau, on peut donc définir des polynômes à coefficients dans $\mathbb{K}[X]$! D'où (encore) l'intérêt de la définition d'un polynôme comme une suite presque nulle : un polynôme à coefficients dans $\mathbb{K}[X]$ est simplement une suite presque nulle d'éléments de $\mathbb{K}[X]$, par exemple :

$$(X^2 + 1, X, 1, 2X, X^3 + 1, 2, 0, 0, \dots)$$

est un polynôme à coefficients dans $\mathbb{K}[X]$. Mais comment les écrire sous forme plus simple ? Comment généraliser la notation des polynômes vue au paragraphe I.3 puisque X est déjà pris ?

Il suffit de se souvenir (cf. paragraphe I.3) que l'indéterminée est muette, qu'on peut parfois l'appeler Y , T (ou même « truc ») etc. L'ensemble des polynômes à coefficients dans A est alors noté $A[Y]$, $A[T]$ etc. mais il faut bien comprendre que c'est le même ensemble : qu'on note X, Y ou T le polynôme $(0, 1, 0, \dots)$, cela ne change rien, c'est toujours l'ensemble des suites presque nulles à coefficients dans A . Dès lors, il suffit de noter (par exemple) Y le polynôme $(0, 1, 0, \dots)$ et le tour est joué. Le polynôme ci-dessus est donc égal à

$$(X^2 + 1) \times 1 + X \times Y + 2X \times Y^2 + (X^3 + 1) \times Y^3 + 2 \times Y^4$$

L'ensemble de ces polynômes est donc noté $A[Y]$ mais comme $A = \mathbb{K}[X]$, on le note également $\mathbb{K}[X][Y]$ ou plus simplement $\mathbb{K}[X, Y]$ et on l'appelle l'anneau (car A est un anneau donc $A[Y]$ est un anneau, et cet anneau est intègre si A l'est) des polynômes à deux indéterminées. Même si cela fait un peu peur, il faut juste se rendre compte que c'est l'ensemble des éléments qui s'écrivent comme une combinaison linéaire de puissances de X et de Y , par exemple :

$$Y^2 + 3X^5 + 2X^2Y + X^3Y^2 - 5XY^4 \in \mathbb{K}[X, Y]$$

Bon, c'est hors programme donc on s'arrête là, mais il ne faut pas en avoir peur si on en rencontre dans un sujet : ce sont des polynômes comme les autres, simplement l'indéterminée est notée Y (ce qui revient au même : penser à « truc ») et les coefficients sont eux-mêmes des polynômes. Le polynôme ci-dessus peut s'écrire simplement sous la forme $a_0 + a_1Y + a_2Y^2 + a_4Y^4$ avec $a_0 = 3X^5$, $a_1 = 2X^2$, $a_2 = 1 + X^3$ et $a_4 = -5X$. On peut évidemment généraliser à n indéterminées et parler de l'anneau $\mathbb{K}[X_1, \dots, X_n]$ des polynômes en n indéterminées à coefficients dans \mathbb{K} , qui est donc l'ensemble des polynômes s'écrivant comme combinaison linéaire de termes de la forme $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ avec $i_1, \dots, i_n \in \mathbb{N}$.

II Degré d'un polynôme

Dans la suite du cours, on abandonne la notation $P = (a_n)_{n \in \mathbb{N}}$ et on notera les polynômes sous la forme d'une somme (finie ou faussement infinie) de termes de la forme $a_k X^k$.

⚠ Ne généralisez pas trop vite l'implication « A anneau $\Rightarrow A[X]$ anneau » en « \mathbb{K} corps $\Rightarrow \mathbb{K}[X]$ corps ». Même si \mathbb{K} est un corps, $\mathbb{K}[X]$ n'est pas un corps, la plupart des éléments de $\mathbb{K}[X]$ ne sont pas inversibles (cf. paragraphe III.1). Il faut ajouter une division, mais comment définir une division pour les suites ? Nous en parlerons (un peu) dans le chapitre 20.

De plus, nous verrons dans le chapitre 20 que $\mathbb{K}(X)$ est un corps : on peut donc construire des polynômes à coefficients dans $\mathbb{K}(X)$ de la même façon que des polynômes à coefficients dans \mathbb{K} . C'est déjà tombé dans des sujets de concours (par exemple ENS MPI 2023) : il faut donc déjà en avoir entendu parler, et voir ça comme des polynômes comme les autres.

On peut même prendre des polynômes à coefficients dans un anneau A : on définit de même l'anneau $\mathbb{Z}[X_1, \dots, X_n]$, qui est donc un anneau commutatif intègre.

II.1 Définition, premiers exemples



Définition. Soit P un polynôme non nul.

- On appelle degré de P , noté $\deg(P)$, le plus grand entier n_0 tel que le coefficient de X^{n_0} soit non nul.
- Ce coefficient est appelé le coefficient dominant de P .
- Enfin, P est dit unitaire si son coefficient dominant est égal à 1.


Par convention, le polynôme nul est de degré $-\infty$.

Tous les résultats de cette partie sont encore valables avec des polynômes à coefficients dans un anneau intègre commutatif (en particulier pour les polynômes à coefficients dans \mathbb{Z}).

Remarques :

- Le degré d'un polynôme $P = \sum_{k=0}^n a_k X^k$ non nul est bien défini, c'est-à-dire que l'ensemble $\{k \in \mathbb{N} \mid a_k \neq 0\}$ admet un plus grand élément. En effet, il est non vide car le polynôme est non nul donc admet un coefficient non nul, et il est fini puisque (par définition d'un polynôme) P n'admet qu'un nombre fini de coefficients non nuls.
-  Par définition, un coefficient dominant est donc non nul ! On ne parle également de coefficient dominant que pour un polynôme non nul, cela n'a pas de sens de parler du coefficient dominant du polynôme nul. Cependant (voir ci-dessus), parler du degré du polynôme nul a un sens.
- Attention, sans indication contraire, quand on écrit P sous la forme $P = \sum_{k=0}^n a_k X^k$, a priori a_n peut être nul. Par exemple, quand on manipulera des polynômes de degré **inférieur ou égal à** n , on les écrira sous cette forme mais ils ne seront pas forcément de degré **égal à** n donc a_n pourra être nul (plus fort : le polynôme nul peut s'écrire sous cette forme, avec tous les a_k sont nuls). Lorsqu'on voudra écrire P sous cette forme avec $n = \deg(P)$ et donc a_n le coefficient dominant de P , il ne faudra pas oublier de le préciser.
-  Le polynôme nul est le seul polynôme de degré strictement négatif : si, au cours d'une démonstration, on arrive à $\deg(P) < 0$, alors on peut conclure que $P = 0$. Voir par exemple la démonstration du théorème de division euclidienne (cf. partie III).

Exemples :

- $2X^5 + X - 5$ est de degré 5 et de coefficient dominant égal à 2.
- $X^{1789} + 19X^{10} + 2$ est unitaire de degré 1789.
- Un polynôme constant non nul est de degré 0. Ainsi, quand on voudra parler du degré d'un polynôme constant, il faudra séparer les cas selon si le polynôme est nul ou non.
- Un polynôme est non constant si et seulement s'il a un degré supérieur ou égal à 1, et constant si et seulement s'il a un degré inférieur ou égal à 0 (0 si le polynôme est non nul, et $-\infty$ s'il est nul).
-  Le degré peut ne pas sauter aux yeux. Par exemple, ce n'est qu'en développant qu'on réalise que $P = (X + 1)^4 - (X - 1)^4$ est de degré 3 et de coefficient dominant égal à 8.

II.2 Degré d'une somme, d'un produit, d'une composée

On adjoint à \mathbb{N} un élément noté $-\infty$ qui n'appartient pas à \mathbb{N} .

Définition. On prolonge la relation d'ordre \leq sur $\mathbb{N} \cup \{-\infty\}$ en posant :

$$-\infty \leq -\infty \quad \text{et} \quad \forall x \in \mathbb{N}, \quad -\infty < x$$

On fait comme dans le chapitre 12 quand on a créé \mathbb{R} , mais ici on n'ajoute pas d'élément noté $+\infty$ et on ne crée pas une nouvelle notation pour l'ensemble $\mathbb{N} \cup \{+\infty\}$.

Définition. On prolonge l'addition usuelle de \mathbb{N} sur $\mathbb{N} \cup \{-\infty\}$ en posant :

$$\forall x \in \mathbb{N} \cup \{-\infty\}, \quad (-\infty) + x = -\infty$$

Théorème. Soit $(P, Q) \in \mathbb{K}[X]^2$. Alors $\deg(P \times Q) = \deg(P) + \deg(Q)$.

DÉMONSTRATION. Supposons P et Q non nuls, de degrés respectifs n et m (appartenant à \mathbb{N} , donc) et de coefficients dominants respectifs a_n et b_m . Le résultat découle alors immédiatement de l'expression de $P \times Q$ (celle avec $a_n \times b_m$) donnée en I.5.

Si P ou Q est nul : supposons sans perte de généralité que $P = 0$ si bien que $\deg(P) + \deg(Q) = -\infty$ (que Q soit nul ou non : $-\infty$ est absorbant) et $P \times Q = 0$ donc $\deg(P \times Q) = -\infty$.

Remarque : C'est pour cela qu'on a défini le degré du polynôme nul comme étant égal à $-\infty$: c'est un élément absorbant, et donc il n'est pas nécessaire de distinguer les cas selon que l'un des deux est nul ou non.

Théorème. Soient P et Q appartenant à $\mathbb{K}[X]$ non tous nuls. Alors $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$. De plus, si P et Q sont non nuls, il y a égalité si et seulement si $\deg(P) \neq \deg(Q)$ ou $[\deg(P) = \deg(Q)$ et les coefficients dominants de P et Q ne sont pas opposés].

Remarque : En d'autres termes, le degré d'une somme est égal au maximum des degrés quand les termes dominants ne se compensent pas : soit les polynômes ne sont pas de même degré, soit ils sont de même degré mais les coefficients ne se compensent pas, c'est-à-dire qu'ils ne sont pas opposés. En tout cas, que les termes dominants se compensent ou pas, on ne peut pas « créer de nouveaux degrés » donc le degré d'une somme est toujours inférieur ou égal au maximum des degrés. C'est la même idée pour la différence.

DÉMONSTRATION. Si P ou Q est nul : supposons sans perte de généralité que $P = 0$ si bien que $P + Q = Q$ et $\deg(Q) \geq \deg(P)$ (que Q soit nul ou non) donc $\deg(P + Q) = \max(\deg(P), \deg(Q))$. De plus, alors $\deg(P) + \deg(Q) = -\infty$ (que Q soit nul ou non) et $P \times Q = 0$ donc $\deg(P \times Q) = -\infty$.

Supposons P et Q non nuls, de degrés respectifs n et m (appartenant à \mathbb{N} , donc) de coefficients dominants respectifs a_n et b_m . Le résultat (l'inégalité et le cas d'égalité) découle alors immédiatement de l'expression de $P + Q$ (comme somme finie) donnée en I.4.

Remarque : Retenons aussi que le coefficient dominant d'un produit de polynômes non nuls est le produit des coefficients dominants. Pour la somme, avec les notations des paragraphes I.4 et I.5, si P est de degré n et Q de degré m :

- Si $n > m$ (respectivement $n < m$), le coefficient dominant de $P + Q$ est a_n (respectivement b_m).
- Si $n = m$ et $a_n \neq -b_m$, le coefficient dominant de $P + Q$ est $a_n + b_m$.
- Si $n = m$ et $a_n = -b_m$, on ne peut rien conclure en toute généralité.

On en déduit que $\mathbb{K}[X]$ est un anneau intègre. En effet, avec les notations précédentes, $P \times Q$ est de degré $n + m$ de coefficient dominant $a_n \times b_m \neq 0$ donc est non nul : un produit de polynômes non nul est non nul, l'anneau est bien intègre. En particulier :

Corollaire. Tout élément non nul de $\mathbb{K}[X]$ est régulier, c'est-à-dire que si P est un polynôme non nul et si Q et R sont deux polynômes tels que $PQ = PR$ alors $Q = R$.

Exemple : Si $P \times (X + 1) = Q \times (X + 1)$ alors $P = Q$. Attention à ne pas écrire d'horreur : un polynôme n'est pas un nombre ou une fonction, n'écrivez pas : « si $X \neq -1$ alors $P = Q$ » ! Tout ce qu'il faut vérifier c'est si le polynôme par lequel on simplifie est nul ou non, ici ce n'est pas le cas donc on peut simplifier.

Contrairement au chapitre 12 avec \mathbb{R} , le fait qu'il n'y ait pas $+\infty$ simplifie beaucoup les choses, et en particulier évite les formes indéterminées.

Le cas où P ou Q est nul est trivial : la somme est alors égale à l'autre polynôme et il y a encore égalité. Nous ne le mettons pas dans l'énoncé pour ne pas l'alourdir avec un cas évident qui se produit somme toute assez peu.

Même si le polynôme admet des racines donc si la fonction polynôme associée s'annule, voir la suite.

Corollaire.

- Soit $(P, Q) \in \mathbb{K}[X]^2$. $\deg(P-Q) \leq \max(\deg(P), \deg(Q))$ avec égalité si et seulement si $\deg(P) \neq \deg(Q)$ ou $\deg(P) = \deg(Q)$ et les coefficients dominants de P et Q ne sont pas égaux.
- Le degré d'une somme de polynômes de degrés distincts est égal au maximum des degrés.
- Soit $P \in \mathbb{K}[X]$ et soit $\lambda \in \mathbb{K}$. Alors $\deg(\lambda P) \leq \deg(P)$, avec égalité si et seulement si $\lambda \neq 0$.

DÉMONSTRATION. Le premier point se démontre en appliquant le théorème à P et Q . Le second se démontre par récurrence (laissée en exercice) sur le nombre de polynômes. Enfin, le dernier découle du fait que $\deg(\lambda P) = \deg(\lambda) + \deg(P)$. \square

Définition. Soit $(P, Q) \in \mathbb{K}[X]^2$. Si $P = a_n X^n + \dots + a_1 X + a_0$, on définit le polynôme composé $P \circ Q$ par : $P \circ Q = a_n Q^n + \dots + a_1 Q + a_0$.

Exemple : Si $P = 2X^1 - 1$ et $Q = 3X^3 + X + 1$ alors

$$\begin{aligned} P \circ Q &= 2(3X^3 + X + 1)^2 - 1 \\ &= 2(9X^6 + X^2 + 1 + 6X^4 + 6X^3 + 2X) - 1 \\ &= 18X^6 + 12X^4 + 12X^3 + 2X^2 + 4X + 1 \end{aligned}$$

Proposition. Soit $(P, Q) \in \mathbb{K}[X]^2$ avec P et Q non constants. Alors : $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

DÉMONSTRATION. Notons $P = a_n X^n + \dots + a_1 X + a_0$ avec $a_n \neq 0$ (n est donc le degré de P et a_n son coefficient dominant). Tout d'abord,

$$\deg(Q^2) = \deg(Q \times Q) = \deg(Q) + \deg(Q) = 2 \deg(Q)$$

Par une récurrence immédiate, pour tout $k \in \mathbb{N}$, $\deg(Q^k) = k \times \deg(Q)$. Puisque $a_n \neq 0$, alors $\deg(a_n Q^n) = \deg(Q^n) = n \deg(Q)$ et, si $k \leq n-1$,

$$\deg(a_k Q^k) \leq \deg(Q^k) = k \deg(Q) < n \deg(Q) \quad \square$$

car $\deg(Q) \neq 0$ puisque Q n'est pas constant. Par conséquent, $P \circ Q$ est la somme d'un polynôme de degré $n \times \deg(Q)$ et de polynômes ayant un degré strictement inférieur. Il en découle que $\deg(P \circ Q) = n \times \deg(Q)$. En d'autres termes, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

II.3 $\mathbb{K}_n[X]$

Définition. Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients réels de degré inférieur ou égal à n .

Exemple : $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants.

Proposition. Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est stable par somme et par multiplication par un scalaire.

DÉMONSTRATION. • Soient $P \in \mathbb{K}_n[X]$ et $\lambda \in \mathbb{K}$. Alors $\deg(\lambda P) \leq \deg(P) \leq n$ donc $\lambda P \in \mathbb{K}_n[X]$: $\mathbb{K}_n[X]$ est stable par multiplication par un scalaire.

- Soit $(P, Q) \in \mathbb{K}_n[X]^2$. Alors $\deg(P+Q) \leq \max(\deg(P), \deg(Q)) \leq n$: $P+Q \in \mathbb{K}_n[X]$ donc $\mathbb{K}_n[X]$ est stable par somme.

Et on rappelle que $\deg(\lambda) \leq 0$.

On trouve aussi la notation $P(Q)$. On a évidemment $P(X) = P$. On trouve donc également la notation $P(X)$ pour désigner le polynôme P .

Si P est constant, alors $P \circ Q$ est constant et son degré est le même que celui de P , et si Q est constant, le degré de $P \circ Q$ dépend de si Q est racine (cf. V.1) de P ou non.



Attention, pas de degré égal à n !




Attention, $\mathbb{K}_n[X]$ n'est pas stable par produit (sauf si $n = 0$). Par exemple, $X \in \mathbb{K}_1[X]$, $X+1 \in \mathbb{K}_1[X]$ mais $X(X+1) \notin \mathbb{K}_1[X]$.

Remarques :

- En particulier, $\mathbb{K}_n[X]$ est un sous-groupe de $\mathbb{K}[X]$ et en particulier est un groupe (mais pas un sous-anneau si $n \geq 1$ puisqu'il n'est pas stable par produit).
- On montre aisément que la fonction $\varphi : \mathbb{K}_0[X] \rightarrow \mathbb{K}$ qui au polynôme constant $(\lambda, 0, \dots)$ associe la constante λ est un isomorphisme de groupes. Par conséquent (ce qui se voit très bien), $\mathbb{K}_0[X]$ est un groupe isomorphe à \mathbb{K} . C'est même un isomorphisme de corps : \leadsto

EXERCICE.

-  L'ensemble des polynômes de degré n n'est stable ni par somme, ni par multiplication par un scalaire. En effet, $X^n - X^n$ n'est pas de degré n , et $0.X^n$ ne l'est pas non plus. C'est la raison pour laquelle on s'intéresse à $\mathbb{K}_n[X]$ plutôt qu'à l'ensemble des polynômes de degré n .

La multiplication par un scalaire en fait même un \mathbb{K} -espace vectoriel : cf. second chapitre 28.

III Arithmétique des polynômes

III.1 Arithmétique « élémentaire » i.e. sans division euclidienne

Définition. Soient A et B deux polynômes. On dit que B divise A s'il existe $Q \in \mathbb{K}[X]$ tel que $A = B \times Q$. On dit alors que A est un multiple de B et que B est un diviseur de A .

Notation : Si B divise A , on note $B \mid A$. Dans le cas contraire, on note $B \nmid A$.

Remarque : Le polynôme nul est un multiple de tous les polynômes car, pour tout $P \in \mathbb{K}[X]$, $0 = 0 \times P$. Cependant, le seul multiple du polynôme nul est le polynôme nul lui-même.

Exemple : $X^3 + X = X(X^2 + 1)$ donc $X^2 + 1$ divise $X^3 + X$.

Proposition. Soient A et B deux polynômes. Si B divise A et si $A \neq 0$ alors $\deg(B) \leq \deg(A)$.

DÉMONSTRATION. En effet, il existe alors Q non nul tel que $A = BQ$, si bien que $\deg(A) = \deg(Q) + \deg(B)$. Or, Q est non nul donc $\deg(Q) \geq 0$ ce qui permet de conclure.

Proposition. Les polynômes inversibles de $\mathbb{K}[X]$ sont exactement les polynômes constants non nuls.

DÉMONSTRATION. Soit $P \in \mathbb{K}[X]$ inversible et soit $Q \in \mathbb{K}[X]$ l'inverse de P . Alors $PQ = 1$ donc $\deg(P) + \deg(Q) = 0$ donc (un degré est soit égal à $-\infty$ soit un entier positif) $\deg(P) = \deg(Q) = 0$ c'est-à-dire que P est constant non nul. Réciproquement, un polynôme constant non nul est inversible car si P est constant égal à $\lambda \neq 0$, en notant Q le polynôme constant égal à $1/\lambda$, on a bien $PQ = 1$ donc P est inversible.

Définition. Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que A et B sont associés si $A \mid B$ et $B \mid A$.

Proposition. Soit $(A, B) \in \mathbb{K}[X]^2$. Alors A et B sont associés si et seulement si on passe de A à B par une multiplication par un polynôme inversible c'est-à-dire un polynôme constant non nul.

DÉMONSTRATION. Supposons que $A \mid B$ et $B \mid A$.

Si $A = 0$ alors B est un multiple de 0 donc $B = 0$ si bien que $A = B = 1 \times B$. De même si $B = 0$.

Par contre, les polynômes constants non nuls divisent tous les polynômes car, si $\lambda \neq 0$ et $P \in \mathbb{K}[X]$ alors $P = \lambda \times \left(\frac{1}{\lambda} \times P\right)$.

Rappelons que le seul polynôme de degré strictement négatif est le polynôme nul.

Dans le cas où on travaille sur un anneau, les seuls polynômes inversibles sont les polynômes constants dont la valeur est un inversible de l'anneau A . Par exemple, les seuls inversibles de $\mathbb{Z}[X]$ sont les polynômes constants égaux à ± 1 .

Si A et B sont non nuls alors, d'après ce qui précède, $\deg(A) \leq \deg(B)$ et $\deg(B) \leq \deg(A)$ donc $\deg(A) = \deg(B)$. Or, $B \mid A$ donc il existe Q tel que $A = BQ$ si bien que $\deg(A) = \deg(B) + \deg(Q)$ donc $\deg(Q) = 0$: Q est constant non nul.

La réciproque est immédiate.

Proposition. Soit $(A, B) \in \mathbb{K}[X]^2$ et soit $P \in \mathbb{K}[X]$. Si A est un multiple de B alors PA est un multiple de PB .

DÉMONSTRATION. Par hypothèse, il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$ donc $PA = Q \times PB$.

Proposition. Soient $B \in \mathbb{K}[X]$, $n \geq 1$ et $A_1, \dots, A_n, C_1, \dots, C_n$ des polynômes. Si $B \mid A_i$ pour tout $i \in \llbracket 1; n \rrbracket$, alors $B \mid A_1C_1 + \dots + A_nC_n$.

DÉMONSTRATION. Pour tout $i \in \llbracket 1; n \rrbracket$, il existe Q_i tel que $A_i = Q_i \times B$. Dès lors,

$$A_1C_1 + \dots + A_nC_n = \underbrace{(C_1Q_1 + \dots + C_nQ_n)}_{\in \mathbb{K}[X]} \times B$$

ce qui permet de conclure. □

Proposition. Soit $(A, B, C) \in \mathbb{K}[X]^3$. Si $C \mid B$ et $B \mid A$ alors $C \mid A$.

DÉMONSTRATION.

\rightsquigarrow EXERCICE.

Proposition. Soit $(A, B, C, D) \in \mathbb{K}[X]^4$. Si $B \mid A$ et $D \mid C$ alors $B \times D \mid A \times C$.

DÉMONSTRATION. Il existe $(Q_1, Q_2) \in \mathbb{K}[X]^2$ tel que $A = Q_1 \times B$ et $C = Q_2 \times D$, si bien que $AC = (Q_1Q_2) \times BD$ ce qui permet de conclure.

Corollaire. Soit $(A, B) \in \mathbb{K}[X]^2$. Si $B \mid A$ alors, pour tout $n \in \mathbb{N}$, $B^n \mid A^n$.

DÉMONSTRATION. Par récurrence :

\rightsquigarrow EXERCICE.

On a envie de poursuivre encore plus loin l'analogie avec l'arithmétique sur \mathbb{Z} , mais pour cela, on a besoin du théorème de la division euclidienne. Par chance, il est encore possible de définir une division euclidienne sur l'anneau $\mathbb{K}[X]$ (on dit donc que $\mathbb{K}[X]$ est un anneau euclidien, mais c'est une autre histoire).

III.2 Division euclidienne

La suite de cette partie n'est valable que lorsqu'on se place sur un corps, c'est-à-dire lorsqu'on s'intéresse à des polynômes à coefficients dans un corps \mathbb{K} , pas sur un anneau, c'est-à-dire que ce qui suit n'est plus valable pour des polynômes à valeurs dans un anneau A .

Théorème (théorème de division euclidienne.). Soit $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = B \times Q + R$ et $\deg(R) < \deg(B)$. On appelle Q le quotient de la division euclidienne de A par B , et R est le reste.

Exemple : Faisons la division euclidienne de $A = 5X^4 - 2X^3 + 16X^2 - X - 1$ par $B = 2X^2 + 3$. On la pose comme la division euclidienne dans \mathbb{Z} :

$$\begin{array}{r|l} 5X^4 - 2X^3 + 16X^2 - X - 1 & 2X^2 + 3 \\ - (5X^4 & + 15X^2/2) \\ \hline & - 2X^3 + 17X^2/2 - X - 1 \\ - & (- 2X^3 & - 3X) \\ \hline & 17X^2/2 + 2X - 1 \\ & - (17X^2/2 & + 51/4) \\ \hline & 2X - 55/4 \end{array}$$

Le théorème ci-dessous est évidemment à rapprocher de la division euclidienne sur \mathbb{Z} . Nous l'avons énoncé (pour les fonctions polynomiales) dans le chapitre 9.

Ce théorème n'est plus valable sur un anneau car on divise (plusieurs fois) par le coefficient dominant de B , ce qui n'est pas forcément possible sur un anneau. Cependant, si le coefficient dominant de B divise tous les coefficients de A ou (plus simple) si B est unitaire, alors ce théorème est encore valable sur un anneau : cf. exercice 67.

Ainsi,

$$\underbrace{5X^5 - 2X^3 + 16X^2 - X - 1}_A = \underbrace{(2X^2 + 3)}_B \times \underbrace{\left(\frac{5}{2}X^2 - X + \frac{17}{4}\right)}_Q + \underbrace{2X - \frac{55}{4}}_R$$

DÉMONSTRATION. Montrons d'abord l'existence puis l'unicité.

Existence : Par récurrence sur le degré de A .

- Pour tout $n \geq 0$, notons H_n la proposition

$$\ll \forall A \in \mathbb{K}_n[X], \exists (Q, R) \in \mathbb{K}[X]^2, A = BQ + R \text{ avec } \deg(R) < \deg(B) \gg.$$

- Soit $A \in \mathbb{K}_0[X]$. Le polynôme A est donc constant, disons égal à $\alpha \in \mathbb{K}$.

- ★ Si B est constant (non nul), disons égal à $\beta \in \mathbb{R}$, alors $A = \beta \times \left(\frac{\alpha}{\beta}\right) + 0$.
Posons $Q = \alpha/\beta$ et $R = 0$. On a bien $A = BQ + R$ avec $\deg(R) = -\infty < 0 = \deg(B)$.
- ★ Si B n'est pas constant, alors $A = B \times 0 + A$. On pose $Q = 0$ et $R = A$. On a bien $A = BQ + R$ avec $\deg(R) \leq 0 < \deg(B)$ (car B n'est pas constant).

Dans tous les cas, H_0 est vraie.

- Soit $n \in \mathbb{N}$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Soit donc $A \in \mathbb{K}_{n+1}[X]$.
 - ★ Si $\deg(A) \leq n$, alors $A \in \mathbb{K}_n[X]$. Par hypothèse de récurrence, il existe Q et R tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.
 - ★ On suppose à présent que $\deg(A) = n + 1$. Notons a_{n+1} le coefficient dominant (non nul) de A , p le degré de B , et b_p le coefficient dominant (non nul) de B .
Si $n + 1 < p$, on écrit $A = B \times 0 + A$ et on conclut de même que dans l'initialisation. Supposons enfin $n + 1 \geq p$, et posons

$$\tilde{A} = A - B \times \left(\frac{a_{n+1}}{b_p}\right) X^{n+1-p}.$$

Comme \tilde{A} est la différence de deux polynômes de même degré $n + 1$ et de même coefficient dominant a_{n+1} , on a $\deg(\tilde{A}) < n + 1$ (cf. paragraphe II.2). En d'autres termes, $\tilde{A} \in \mathbb{K}_n[X]$. Par hypothèse de récurrence, il existe \tilde{Q} et \tilde{R} (attention, la notation Q' est réservée au polynôme dérivé de Q , et il ne faut pas confondre ici \tilde{Q} avec la fonction polynomiale associée à Q qu'on notera également \tilde{Q} dans le paragraphe IV) tels que $\tilde{A} = B\tilde{Q} + \tilde{R}$ et $\deg(\tilde{R}) < \deg B$. Il en découle (en remplaçant \tilde{A} par son expression) que

$$\begin{aligned} A &= B \times \frac{a_{n+1}}{b_p} X^{n+1-p} + B\tilde{Q} + \tilde{R} \\ &= B \times \left(\frac{a_{n+1}}{b_p} X^{n+1-p} + \tilde{Q}\right) + \tilde{R} \end{aligned}$$

Posons $Q = \frac{a_{n+1}}{b_p} X^{n+1-p} + \tilde{Q}$ et $R = \tilde{R}$. On a bien $A = BQ + R$ avec $\deg(R) = \deg(\tilde{R}) < \deg(B)$: H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$.



Méthode : on multiplie B par le terme nécessaire pour que les termes dominants soient les mêmes, on soustrait, et on recommence. Par exemple, on multiplie B par $5X^2/2$ au départ, car $2X^2 \times 5X^2/2 = 5X^4$, qui est le terme dominant de A . Ensuite, on multiplie B par $-X$ car $2X^2 \times -X = -2X^3$, ce qui est le terme dominant du polynôme obtenu après différence, et ainsi de suite. On s'arrête quand on obtient un polynôme de degré inférieur strictement au degré de B .



On a donc

$$\begin{aligned} A &= a_{n+1}X^{n+1} + \dots \\ \text{et } B &= b_pX^p + \dots \end{aligned}$$



Comme dans l'exemple ci-dessus : on multiplie B par ce qu'il faut pour que le terme dominant soit le même que celui de A (il faut multiplier b_pX^p par $(a_{n+1}/b_p)X^{n+1-p}$ pour obtenir $a_{n+1}X^{n+1}$), on soustrait, et on recommence, c'est-à-dire qu'on applique l'hypothèse de récurrence : la preuve n'est rien de plus que la formalisation de la méthode utilisée dans l'exemple !

D'où l'existence.

Unicité : Soient (Q_1, R_1) et (Q_2, R_2) deux couples qui conviennent. Alors $A = BQ_1 + R_1 = BQ_2 + R_2$. Ainsi $B(Q_1 - Q_2) = R_2 - R_1$ et donc :

$$\begin{aligned}\deg(R_2 - R_1) &= \deg(B(Q_1 - Q_2)) \\ &= \deg(B) + \deg(Q_1 - Q_2)\end{aligned}$$

Or, $\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) < \deg(B)$ donc $\deg(Q_1 - Q_2) < 0$. Comme le seul polynôme de degré strictement négatif est le polynôme nul, on a $Q_1 - Q_2 = 0$ c'est-à-dire que $Q_1 = Q_2$. Enfin, $R_2 - R_1 = B(Q_1 - Q_2) = 0$ donc $R_1 = R_2$. D'où l'unicité. \square

Remarque : Comme sur \mathbb{Z} , si A et B sont deux polynômes avec $B \neq 0$, alors $B \mid A$ si et seulement si le reste dans la division euclidienne de A par B est nul (la démonstration est analogue).


III.3 \mathbb{Z} et $\mathbb{K}[X]$, même combat (enfin, presque)

L'existence d'une division euclidienne permet de faire de l'arithmétique sur $\mathbb{K}[X]$ de la même façon que sur \mathbb{Z} . Par conséquent, certains résultats ci-dessous dont la preuve est analogue à celle vue dans le chapitre 6 ne seront pas redémontrés. Cependant, attention tout de même : certaines choses changent, mais nous le dirons le moment venu.

III.3.a PGCDs

Définition. Soient A et B deux polynômes non tous nuls. Tout diviseur commun à A et à B de degré maximal est appelé un PGCD de A et de B .

Remarques :

- Il existe en effet des diviseurs communs à A et B ayant un degré maximal car A et B sont non tous nuls. Supposons (raisonnement analogue dans l'autre cas) que $B \neq 0$. Alors tout diviseur D de B vérifie $\deg(D) \leq \deg(B)$: en d'autres termes, l'ensemble $E = \{\deg(D) \in \mathbb{N} \mid D \text{ divise } A \text{ et } D \text{ divise } B\}$ est majoré par $\deg(B)$. Puisque cet ensemble est non vide (il contient 0 puisque le polynôme constant égal à 1 divise A et B donc son degré, 0, appartient à E), c'est une partie non vide majorée de \mathbb{N} donc admet un plus grand élément.
-  Grosse différence avec les entiers : on dit un PGCD et non pas le PGCD puisqu'il peut y en avoir plusieurs. Rectification : il y en a plusieurs, et même une infinité (lorsque \mathbb{K} est infini ce qui est le cas lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$), voir ci-dessous.
- Là aussi, un moyen simple de prouver qu'un polynôme D est un PGCD de A et de B consiste à montrer que D divise A et B et que tout diviseur commun à A et B a un degré inférieur ou égal à celui de D .
- Là aussi, le PGCD est commutatif (il est aussi associatif, cf. paragraphe II.3.g).
- Là aussi, si $B \neq 0$, alors B est un PGCD de 0 et de B .
- Là aussi, le degré d'un PGCD de A et de B est inférieur ou égal à $\min(\deg(A), \deg(B))$ avec égalité si et seulement si l'un des deux divise l'autre.

Il est temps de se poser la question suivante : si A et B sont non tous nuls, quel lien y a-t-il entre tous les PGCD de A et de B ?

III.3.b Algorithme d'Euclide

L'algorithme d'Euclide est toujours valable pour les polynômes, mais attention : il donne un PGCD.

Exemple :

En particulier, on a $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$.

Comparez avec votre cours d'arithmétique : le plan est (presque) le même !

Parler d'un polynôme plus grand qu'un autre n'a pas vraiment de sens : c'est pour cela qu'on définit un PGCD comme un polynôme ayant un **degré** supérieur ou égal au degré de tous les autres diviseurs communs. Attention : il n'y a pas unicité du PGCD !

Nous ne démontrons pas ces résultats, la preuve est analogue à celle pour les entiers.

La démonstration est analogue mais il faut remplacer le PGCD par les PGCD, et il termine car la suite des degrés est strictement décroissante.

$$\begin{array}{r|l} 2X^3 - 8X^2 + 10X - 4 & X^2 - 5X + 6 \\ - & \dots \\ \hline & 8X - 16 \end{array}$$

$$\begin{array}{r|l} X^2 - 5X + 6 & 8X - 16 \\ - & \dots \\ \hline & 0 \end{array}$$

Un PGCD de $2X^3 - 8X^2 + 10X - 4$ et de $X^2 - 5X + 6$ est donc $8X - 16$.

À présent, nous pouvons donner le lien entre les différents PGCD de deux polynômes A et B .

Théorème. Soient A et B non tous nuls. Soit D un PGCD de A et de B . Alors les PGCD de A et de B sont exactement tous les polynômes associés à D . En particulier :

- Si D est un PGCD de A et B , les autres PGCD sont exactement les λD où $\lambda \in \mathbb{K}^*$.
- Parmi tous les PGCD de A et B , un seul est unitaire : on le note $A \wedge B$.


DÉMONSTRATION. Commençons par un lemme.

Lemme. Soit R un polynôme non nul. Alors les PGCD de 0 et R sont exactement les polynômes associés à R .

Démontrons ce lemme. Les polynômes associés à R divisent R et tout polynôme divise 0 donc sont des diviseurs communs à R et 0 de degré $\deg(R)$. Or, un diviseur commun à 0 et R est de degré inférieur à $\deg(R)$ donc ces polynômes sont des diviseurs communs de degré maximal donc sont des PGCD.

Réciproquement, soit D un PGCD de R et 0. On déduit de ce qui précède que $\deg(D) = \deg(R)$. Or, D divise R et D et R ont le même degré donc le quotient est de degré 0 donc est constant non nul : les deux polynômes sont associés : le lemme est démontré.

Revenons au théorème. Notons $(R_1, \dots, R_n, 0)$ les restes de l'algorithme d'Euclide entre A et B , avec $R_n \neq 0$ (si bien que R_n est un PGCD de A et B). Or, les PGCD de A et B sont les PGCD de R_n et 0 qui sont tous les polynômes associés à R_n . En particulier, les PGCD de A et B sont associés.

Remarque :  L'algorithme d'Euclide donne un PGCD de A et B mais pas forcément $A \wedge B$: voir l'exemple ci-dessus, l'algorithme d'Euclide renvoie $8X - 16$ alors que $A \wedge B = X - 2$, l'unique polynôme proportionnel à $8X - 16$ qui soit unitaire. Tout ce qu'on peut dire est que l'algorithme d'Euclide renvoie un multiple de $A \wedge B$, pour obtenir $A \wedge B$, il suffit de diviser par le coefficient dominant.

En d'autres termes, $A \wedge B$ n'est pas le PGCD de A et B puisqu'il n'y a plus unicité du PGCD mais l'unique PGCD unitaire de A et B , c'est-à-dire leur unique diviseur commun de degré maximal qui soit unitaire.

III.3.c Polynômes premiers entre eux

Définition. Soient A et B deux polynômes non nuls. On dit que A et B sont premiers entre eux si $A \wedge B = 1$.

Remarques :

- Puisque tous les PGCD sont associés, deux polynômes sont premiers entre eux si et seulement si leurs PGCD sont les polynômes constants non nuls, si et seulement si leurs seuls diviseurs communs sont les polynômes constants non nuls.
- Si $A \mid B$ et si A n'est pas constant alors A et B ne sont pas premiers entre eux.
- Attention, comme pour les entiers, si aucun des deux ne divise l'autre, cela ne signifie pas qu'ils soient premiers entre eux.

Exemple : Soient λ et μ deux éléments de \mathbb{K} distincts. Alors $X - \lambda$ et $X - \mu$ sont premiers entre eux. En effet :

$$\begin{array}{r|l} X - \lambda & X - \mu \\ - (X - \mu) & 1 \\ \hline \mu - \lambda & \end{array} \qquad \begin{array}{r|l} X - \mu & \mu - \lambda \\ - (X - \mu) & \frac{X - \mu}{\mu - \lambda} \\ \hline 0 & \end{array}$$

Dès lors, le polynôme constant égal à $\lambda - \mu$ est un PGCD de $X - \lambda$ et $X - \mu$ donc ils sont premiers entre eux. Plus généralement, deux polynômes de degré 1 sont premiers entre eux si et seulement s'ils ne sont pas proportionnels : \rightsquigarrow EXERCICE.

Plus généralement (cf. paragraphe III.3.h), si n et m sont des entiers non nuls, $(X - \lambda)^n$ et $(X - \mu)^m$ sont premiers entre eux si et seulement si $\lambda \neq \mu$.

III.3.d Algorithme d'Euclide étendu et relation de Bézout

L'algorithme d'Euclide étendu est encore valable pour des polynômes (tout en gardant en tête qu'il faut parler d'un PGCD et pas du PGCD). Le théorème de Bézout est encore valable pour des polynômes :

Théorème (Théorème de Bézout). Soient A et B appartenant à $\mathbb{K}[X]$ non tous nuls.

- Il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = A \wedge B$.
- Plus généralement, si $P \in \mathbb{K}[X]$, il existe $(U, V) \in \mathbb{Z}^2$ tel que $AU + BV = P$ si et seulement si P est un multiple de $A \wedge B$.
- En particulier, A et B sont premiers entre eux si et seulement s'il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.

Ou, ce qui revient au même, si et seulement si P est divisible par $A \wedge B$.

Remarques :

- Comme pour les entiers, il n'y a pas unicité de U et V (lorsqu'il y a existence).
- Comme pour les entiers, si A est premier avec P et si B est premier avec P alors AB est premier avec P .
- Comme pour les entiers, un polynôme divise A et B si et seulement s'il divise leurs PGCD (ou, ce qui revient au même, un de leur PGCD ou $A \wedge B$).
- Comme pour les entiers, en divisant deux polynômes par un de leurs PGCD, on obtient des polynômes premiers entre eux.

Exemple : Donnons une PGCD de $X^{12} - 1$ et de $X^8 - 1$ ainsi qu'une relation de Bézout entre ces deux polynômes.

On peut montrer (cf. exercice 64) que $(X^a - 1) \wedge (X^b - 1) = X^{a \wedge b} - 1$.

$$\begin{array}{r|l} X^{12} - 1 & X^8 - 1 \\ - (X^8 - X^4) & X^4 \\ \hline X^4 - 1 & \end{array} \qquad \begin{array}{r|l} X^8 - 1 & X^4 - 1 \\ - (X^8 - X^4) & X^4 \\ \hline X^4 - 1 & \end{array} \qquad \begin{array}{r|l} X^4 - 1 & X^4 - 1 \\ - (X^4 - 1) & X^4 \\ \hline 0 & \end{array}$$

et $X^4 - 1 = X^{12} - 1 - X^4(X^8 - 1)$.


III.3.e Théorème de Gauß

Le théorème de Gauß est encore valable pour les polynômes. Son corollaire aussi, c'est-à-dire que si A et B sont premiers entre eux et divisent P , alors AB divise P .

III.3.f PPCMs

Définition. Soient A et B deux polynômes non nuls. Tout multiple commun à A et à B de degré minimal est appelé un PPCM de A et de B .

Remarques :


- Il existe en effet des diviseurs communs à A et B ayant un degré minimal. L'ensemble $E = \{\deg(D) \in \mathbb{N} \mid A \text{ divise } D \text{ et } B \text{ divise } D\}$ est non vide (il contient $\deg(AB)$ puisque le polynôme AB est divisible par A et par B donc son degré appartient à E), c'est une partie non vide de \mathbb{N} donc admet un plus petit élément.
-  Là aussi, il y a plusieurs PPCM.
- Là aussi, un moyen simple de prouver qu'un polynôme D est un PPCM de A et de B consiste à montrer que D est divisible par A et par B et que tout multiple commun à A et B a un degré supérieur ou égal à celui de D .
- Là aussi, le PPCM est commutatif.
- Là aussi, le degré d'un PPCM de A et de B est supérieur ou égal à $\max(\deg(A), \deg(B))$ avec égalité si et seulement si l'un des deux divise l'autre.
- Là aussi, un polynôme est un multiple commun à A et B si et seulement si c'est un multiple d'un PPCM.

On en déduit le lien entre les PPCM de A et B .

Théorème. Soient A et B non nuls. Soit M un PPCM de A et de B . Alors les PPCM de A et de B sont exactement tous les polynômes associés à M . En particulier :

- Si M est un PPCM de A et B , les autres PPCM sont exactement les λM où $\lambda \in \mathbb{K}^*$.
- Parmi tous les PPCM de A et B , un seul est unitaire : on le note $A \vee B$.

DÉMONSTRATION. D'après ce qui précède, deux PPCM de A et de B sont multiples l'un de l'autre donc sont associés.

Remarque :  On n'a plus $(A \wedge B) \times (A \vee B) = AB!!!$ Il faut bien comprendre que les PGCD et PPCM sont définis à une constante près ! Pour bien se rendre compte que ce n'est pas forcément égal, il suffit de voir que le membre de gauche est unitaire mais que celui de droite n'a aucune raison de l'être. Cependant, si on note a_n le coefficient dominant de A et b_m celui de B , alors on peut montrer que $AB = a_n \times b_m \times (A \wedge B) \times (A \vee B)$ mais cette relation est moins utile avec des polynômes qu'avec des entiers et donc on se contentera de la mettre en remarque.

En d'autres termes, $A \vee B$ n'est pas le PPCM de A et B puisqu'il n'y a plus unicité du PPCM mais l'unique PPCM unitaire de A et B , c'est-à-dire leur unique multiple commun de degré minimal qui soit unitaire.

III.3.g Extension à plus de deux polynômes

Comme pour les entiers, tous les résultats précédents peuvent aisément se généraliser à plus de deux polynômes.

Définition. Soient $n \geq 2$ et $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$ des polynômes non tous nuls. Tout diviseur commun à A_1, \dots, A_n et à B de degré maximal est appelé un PGCD de A_1, \dots, A_n .


Remarques :

- Là aussi, il existe un degré maximal pour les diviseurs communs à A_1, \dots, A_n donc les PGCD sont bien définis.
- Les diviseurs communs à A_1, \dots, A_n sont tous associés, et donc il existe un unique PGCD unitaire, que l'on note $A_1 \wedge \dots \wedge A_n$.
- Là aussi, le PGCD est associatif.

- Les polynômes A_1, \dots, A_n sont premiers entre eux **dans leur ensemble** » si $A_1 \wedge \dots \wedge A_n = 1$ c'est-à-dire si leurs seuls diviseurs communs sont les polynômes constants non nuls.
- Les A_i sont premiers entre eux deux à deux si, pour tous $i \neq j$, A_i et A_j sont premiers entre eux.
- Là aussi,

Premiers entre eux deux à deux \Rightarrow Premiers entre eux dans leur ensemble

mais la réciproque est fausse.

- Le théorème de Bézout est encore vrai pour n polynômes.
- Si A_1, \dots, A_n sont premiers avec un polynôme P , alors leur produit l'est également.
- Un polynôme divise $A_1 \wedge \dots \wedge A_n$ si et seulement s'il divise tous les A_i .
- Si $D = A_1 \wedge \dots \wedge A_n$ alors les A_i/D sont premiers entre eux **dans leur ensemble** ».
-  Si A_1, \dots, A_n sont premiers entre eux **deux à deux** » et divisent un polynôme P alors leur produit divise P .
- On pourrait aussi parler du PPCM de n polynômes, mais c'est HP, pas très utile en pratique, et totalement analogue au cas des entiers : on zappe.

III.3.h Polynômes irréductibles

Définition. Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible si P n'est pas inversible et ne peut pas s'écrire comme produit de deux polynômes non inversibles.

Remarque : Les inversibles de $\mathbb{K}[X]$ étant exactement les polynômes constants non nuls, un polynôme est irréductible si et seulement s'il ne peut pas s'écrire sous la forme de deux polynômes non constants. Dès lors, si on raisonne par l'absurde et qu'on veut prouver qu'un polynôme est irréductible, on suppose qu'on peut l'écrire sous la forme $A \times B$ avec A et B non constants donc avec $1 \leq \deg(A), \deg(B) \leq n - 1$ où n est le degré de P .

Exemple : Un polynôme de degré 1 est irréductible.

Remarque : Les polynômes irréductibles jouent le rôle des nombres premiers sur \mathbb{Z} .

Remarque : Bien que cela dépasse le cadre du programme, disons un mot au sujet des polynômes irréductibles quand on travaille sur un anneau. Un polynôme est irréductible lorsqu'il ne peut pas s'écrire comme produit de deux polynômes non inversibles. Or, les polynômes constants ne sont pas forcément inversibles, seuls les polynômes constants égaux à un élément inversible de A le sont : par conséquent, dans un anneau, la situation est légèrement différente. Par exemple, sur \mathbb{Z} , un polynôme est irréductible lorsque la seule façon de l'écrire sous forme d'un produit est de l'écrire sous la forme AB avec A ou B égaux à ± 1 . Par exemple, sur \mathbb{Z} , $2X$ n'est pas irréductible !

On prouve de façon analogue à \mathbb{Z} le théorème suivant (non valable sur un anneau quelconque) :

Théorème (Décomposition en produit de facteurs irréductibles). Soit $P \in \mathbb{K}[X]$. Il existe $r \geq 1$, P_1, \dots, P_r irréductibles distincts et $\alpha_1, \dots, \alpha_r$ supérieurs ou égaux à 1 tels que :


$$P = P_1^{\alpha_1} \times \dots \times P_r^{\alpha_r}$$

De plus, cette écriture est unique (à l'ordre près des termes et à multiplication par un facteur inversible près).

Remarque : Même si on ne définit pas de valuation p -adique dans ce chapitre, on peut tout de même prouver les résultats suivants :

Lorsque $\mathbb{K} = \mathbb{C}$, ce sont les seuls (cf. paragraphe VII.3.a). Sur \mathbb{R} , il faut rajouter les polynômes de degré 2 de discriminant strictement négatif (cf. paragraphe VII.4.a).

Il arrive parfois de devoir prouver qu'un polynôme est irréductible sur \mathbb{Z} , mais alors la définition est rappelée, pas de panique. Néanmoins, il peut être utile d'en avoir déjà entendu parler.

 Attention (cf. paragraphe VII), le fait qu'un polynôme soit irréductible ou non dépend de \mathbb{K} donc la décomposition en produit de facteurs irréductibles également.

- le produit des facteurs premiers apparaissant à la fois dans la décomposition de A et dans celle de B , mis à la puissance qui est **la plus petite des deux**, est un PGCD de A et de B .
- le produit de tous les facteurs premiers apparaissant dans la décomposition de a ou dans celle de b , mis à la puissance qui est **la plus grande des deux**, est un PPCM de A et de B .
- A et B sont premiers entre eux si et seulement si leurs décomposition en facteurs irréductible n'ont aucun terme commun (sauf des éléments inversibles i.e. constants non nuls), c'est-à-dire si A et B n'ont aucun facteur irréductible commun.
- Soient k_1 et k_2 supérieurs ou égaux à 1. Alors : $A \wedge B = 1 \iff A^{k_1} \wedge B^{k_2} = 1$.
- un polynôme en divise un autre si et seulement si ses facteurs irréductibles apparaissent chez l'autre à une puissance plus grande. C'est l'équivalent de la CNS de divisibilité avec les valuations p -adiques pour les entiers.

En particulier, si $n \in \mathbb{N}^*$:

$$A \wedge B = 1 \iff A^n \wedge B^n = 1$$

Exemples :

- Dans $\mathbb{C}[X]$, si $A = (X-1)(X-2)^2(X-3)^3$ et $B = (X-2)(X-3)^2(X-4)^4$, alors un PGCD de A et de B est $(X-2)(X-3)^2$ et un PPCM est $(X-1)(X-2)^2(X-3)^3(X-4)^4$.
- Si $\alpha \neq \beta$, $X-\alpha$ et $X-\beta$ sont premiers entre eux (cf. paragraphe III.3.c) donc, pour tous n et m supérieurs ou égaux à 1, $(X-\alpha)^n$ et $(X-\beta)^m$ également car n'ont aucun facteur irréductible commun.

IV Fonction polynomiale associée à un polynôme

On l'a assez répété : les polynômes ne sont pas des fonctions mais des suites presque nulles. Cependant, on a tout fait pour pousser au maximum l'analogie entre les polynômes et les fonctions polynomiales (à commencer par l'écriture d'un polynôme avec des X). Il est temps d'exhiber le lien étroit qui existe entre polynômes et fonctions polynomiales.


Pour insister sur la différence entre polynômes et fonctions polynomiales, on parle parfois de polynômes formels, pour signifier que seuls comptent les coefficients.

Définition. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$. On appelle fonction polynomiale (ou fonction polynôme) associée à P la fonction


$$\tilde{P} : \begin{cases} \mathbb{K} & \rightarrow & \mathbb{K} \\ x & \mapsto & \sum_{k=0}^n a_k x^k \end{cases}$$

Définition. Soit $P \in \mathbb{K}[X]$ et soit $x \in \mathbb{K}$. L'évaluation de P en x est l'élément de \mathbb{K} défini par $\tilde{P}(x)$. Pour simplifier les notations, on désigne souvent cette évaluation plus simplement par $P(x)$.

On rappelle que, par convention, $x^0 = 1$.

Remarque :  Quand on veut calculer $P(1)$, on ne dit pas « Soit $X = 1$ » ou « Posons $X = 1$ » (rappelons que X n'est pas un nombre) mais « Évaluons P en 1 » ou « calculons $P(1)$ ».

Exemple : Sur $\mathbb{C}[X]$, si $P = X^2 + X + 1$ alors $P(j) = P(j^2) = 0$: on dit que j et j^2 sont racines de P , cf. paragraphe V.1.

 Mais attention à ne pas franchir le pas et à écrire que $P = \tilde{P}$: un polynôme n'est pas une fonction !

Activité : algorithme de Hörner On souhaite implémenter sur une machine un algorithme prenant en entrée un polynôme $P = \sum_{k=0}^n a_k X^k$ (i.e. un vecteur, un tableau, une matrice etc. contenant ses coefficients a_n, \dots, a_0) et un élément x et qui renvoie $P(x)$.

- Méthode naïve : on calcule x^2, \dots, x^n puis $a_1x, a_2x^2, \dots, a_nx^n$ et enfin $P(x) = \sum_{k=0}^n a_kx^k$. Cette méthode nécessite $2n - 1$ multiplications et n additions.
- méthode de Hörner : il suffit de voir que

$$P = a_0 + X \times (a_1 + X \times (a_2 + X \times (a_3 + \dots + X \times (a_n) \dots)))$$

Sur un exemple, cela donne :

$$3 + 4X + 5X^2 - X^3 + 10X^4 = 3 + X(4 + X(5 + X(-1 + X \times 10)))$$

Cette fois, si on veut calculer $P(2)$, il faut faire la multiplication $2 \times a_n$, puis ajouter a_{n-1} , puis multiplier par 2 et ajouter a_{n-2} , et ainsi de suite, ce qui donne n multiplications et n additions, soit $2n$ opérations élémentaires, dont seulement n multiplications (rappelons qu'elles coûtent plus cher que les additions), ce qui est quand même mieux !

Théorème. La fonction

$$\varphi : \begin{cases} \mathbb{K}[X] & \rightarrow \mathbb{K}^{\mathbb{K}} \\ P & \mapsto \tilde{P} \end{cases}$$

est un morphisme d'anneaux injectif. On pourra donc parfois identifier polynômes et fonctions polynomiales (tout en gardant à l'esprit qu'un polynôme n'est pas une fonction polynomiale).

En particulier, le polynôme nul est le seul antécédent de la fonction nulle, c'est-à-dire que le polynôme nul est le seul qui s'annule en tout élément de \mathbb{K} .

DÉMONSTRATION. Le fait que φ soit un morphisme d'anneaux est immédiat. Nous prouverons qu'il est injectif dans le paragraphe V.2.

Remarque : Ce théorème est faux en général sur un corps quelconque. Par exemple, si $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ et si $P = X^2 + X$ alors $P(0) = P(1) = 0$ donc la fonction polynomiale associée à P est la fonction nulle alors que P n'est pas le polynôme nul (ses coefficients ne sont pas tous nuls, c'est la suite presque nulle $(0, 1, 1, 0, 0, \dots)$). Plus généralement, sur un corps fini \mathbb{K} dont les éléments sont notés x_1, \dots, x_n , φ n'est pas injective car le polynôme $P = (X - x_1) \times \dots \times (X - x_n)$ n'est pas le polynôme nul (il est unitaire de degré n) mais est nul en tout élément de \mathbb{K} donc sa fonction polynomiale associée est la fonction nulle : il n'y a pas injectivité de φ , deux polynômes différents peuvent avoir la même fonction polynomiale associée, on ne peut pas identifier polynôme et fonction polynomiale.

Une condition nécessaire pour que cela soit possible est donc que \mathbb{K} soit infini. Nous montrerons au paragraphe V.2 que c'est également une condition suffisante.

V Racines d'un polynôme

V.1 Définition

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

Exemples :

- 1 est racine de $P = X^3 - X^2 + X - 1$ car $P(1) = 1 - 1 + 1 - 1 = 0$.
- Si on se place sur \mathbb{C} , i et $-i$ sont racines de $X^2 + 1$. Cependant, si on se place sur \mathbb{R} , $P = X^2 + 1$ n'a aucune racine. En particulier, le fait qu'un polynôme admette ou non des racines dépend du corps sur lequel on se place.
- Tout élément de \mathbb{K} est racine du polynôme nul. En particulier, lorsque \mathbb{K} est infini, alors le polynôme nul admet une infinité de racines, et on verra dans le paragraphe V.2 que c'est le seul.

On dit aussi que α est un zéro de P .

Remarques :

- ⚠ On rappelle que X n'est pas un élément de \mathbb{K} . Ainsi, quand on voudra donner l'image d'un élément α par un polynôme P , on dira « Évaluons P en α » ou simplement « $P(\alpha) = \dots$ » mais jamais « Posons $X = \alpha$ ». De la même façon, si on cherche les racines de P , on n'écrira jamais d'égalité du type « $X^2 + X = 0 \iff X = 0$ ou $X = -1$ ». On écrira plutôt : « Soit $x \in \mathbb{K}$. $x^2 + x = 0 \iff x = 0$ ou $x = -1$ ».
- ⚠ Cas particuliers importants : 0 est racine de P si et seulement si son terme constant est nul, et 1 est racine de P si et seulement si la somme de ses coefficients est nulle (voir le premier exemple ci-dessus). En effet, si $P = \sum_{k=0}^n a_k X^k$, alors $P(0) = a_0$ (rappelons que $X^0 = 1$) et $P(1) = \sum_{k=0}^n a_k$. Cela peut être utile pour trouver des racines évidentes rapidement.

V.2 Lien entre degré et nombre de racines

Proposition. Soit $P \in \mathbb{K}[X]$ et soit $\alpha \in \mathbb{K}$. α est racine de P si et seulement si $X - \alpha$ divise P .

DÉMONSTRATION. Notons $B = X - \alpha$. B n'est pas le polynôme nul donc, d'après le théorème de division euclidienne, il existe un unique couple de polynômes Q et R tels que $P = BQ + R$ et $\deg(R) < \deg(B) = 1$. Par conséquent, $\deg(R) \leq 0$: R est constant, disons égal à $\beta \in \mathbb{K}$. Ainsi, $P = (X - \alpha) \times Q + \beta$. En particulier, $P(\alpha) = \beta$ (car $X - \alpha$ est nul en α). Alors :

Il découle également de la démonstration que le reste de la division de P par $(X - \alpha)$ est $P(\alpha)$.

$$B \text{ divise } P \iff R = 0$$

$$\iff \beta = 0$$

$$\iff P(\alpha) = 0$$

$$\iff \alpha \text{ est racine de } P$$

□

Proposition. Soient $P \in \mathbb{K}[X]$, $n \geq 1$ et $(\alpha_1, \dots, \alpha_n)$ des éléments de \mathbb{K} deux à deux distincts. Si $\alpha_1, \dots, \alpha_n$ sont des racines de P , alors P est divisible par $\prod_{j=1}^n (X - \alpha_j)$.

DÉMONSTRATION. Pour tout $j \in \llbracket 1; n \rrbracket$, α_j est racine de P donc $X - \alpha_j$ divise P . Les α_j étant distincts, les $X - \alpha_j$ sont premiers entre eux deux à deux (cf. paragraphe III.3.c) donc leur produit divise P (cf. paragraphe III.3.g).

Corollaire. Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$ de degré inférieur ou égal à n . Si P admet au moins $n + 1$ racines distinctes, alors P est le polynôme nul.

DÉMONSTRATION. Notons ces racines $\alpha_1, \dots, \alpha_{n+1}$. D'après la proposition précédente, il existe Q tel que $P = Q \times \prod_{k=1}^{n+1} (X - \alpha_k)$. Par conséquent,

$$\deg(P) = \deg(Q) + \deg\left(\prod_{k=1}^{n+1} (X - \alpha_k)\right) = \deg(Q) + n + 1.$$

Or, $\deg(P) \leq n$: on en déduit que $\deg(Q) < 0$ donc que Q est le polynôme nul, ce qui permet de conclure. □

⚠ Pour montrer qu'un tel produit divise P , il suffit donc de prouver que $P(\alpha_1) = \dots = P(\alpha_n) = 0$. Par exemple, pour montrer que $X(X+1)$ divise P , il suffit de prouver que $P(0) = P(-1) = 0$.

En d'autres termes, $P \in \mathbb{K}_n[X]$.

En d'autres termes, un polynôme **non nul** ne peut pas avoir un nombre de racines distinctes strictement plus grand que son degré. On verra dans le paragraphe V.4 que c'est encore vrai quand on ne suppose plus les racines distinctes, c'est-à-dire quand on les compte avec multiplicité.

Corollaire. Soit $P \in \mathbb{K}[X]$. Si P admet une infinité de racines distinctes, alors P est le polynôme nul.

Remarque : Ce corollaire est extrêmement important car on ne connaît pas toujours le degré des polynômes que l'on manipule. Bon, il n'a d'intérêt que lorsque \mathbb{K} est infini, mais puisqu'on se place en général sur \mathbb{R} ou sur \mathbb{C} (ce qui est le cadre officiel du programme), ce sera le cas.

Remarque : Prouvons que l'application φ du paragraphe IV est injective lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Puisque c'est un morphisme d'anneaux, il suffit de prouver que son noyau est réduit au polynôme nul. Or, si $P \in \ker(\varphi)$, alors $\tilde{P} = 0$ donc $\tilde{P}(x) = 0$ pour tout $x \in \mathbb{K}$ donc $P(x) = 0$ pour tout $x \in \mathbb{K}$: P a une infinité de racine (car \mathbb{K} est infini) donc est le polynôme nul. On voit même que seul compte le fait que \mathbb{K} soit infini : ce résultat est donc toujours vrai sur un corps infini quelconque (mais pas sur un corps fini, comme on l'a vu au paragraphe IV).

V.3 Conséquence : condition d'égalité de deux polynômes, rigidité des polynômes

De façon générale, deux fonctions f et g définies sur un même ensemble E sont égales si elles coïncident en tout élément de E , c'est-à-dire si $f(x) = g(x)$ pour tout élément x de E . On va voir que cette condition peut être considérablement affaiblie quand f et g sont des polynômes.

Proposition. Soit $(P, Q) \in \mathbb{K}[X]^2$.

- Si P et Q sont de degré inférieur ou égal à n et coïncident en au moins $n + 1$ points (distincts), alors $P = Q$.
- Si P et Q coïncident en une infinité de points (distincts) alors $P = Q$.

DÉMONSTRATION. • Si P et Q sont de degré inférieur ou égal à n et coïncident en au moins $n + 1$ points alors $P - Q$ a au moins $n + 1$ racines distinctes donc $P - Q$ est le polynôme nul, c'est-à-dire que $P = Q$.

• Si P et Q coïncident en une infinité de points alors $P - Q$ a une infinité de racines donc est le polynôme nul, c'est-à-dire que $P = Q$. \square

Remarques :

- Comme ci-dessus, le deuxième point de la proposition est très utile en pratique car on ne connaît pas toujours le degré des polynômes que l'on manipule.
- On a enfin prouvé le résultat utilisé dans de nombreux chapitres : si deux fonctions polynomiales coïncident en une infinité de points, alors elles ont les mêmes coefficients. En effet, cela signifie que les polynômes associés coïncident en une infinité de points donc sont égaux (donc ont les mêmes coefficients).

Application : Un polynôme réel périodique est constant.

Soit $P \in \mathbb{R}[X]$ un polynôme périodique. Soit $T \in \mathbb{R}^*$ tel que, pour tout $x \in \mathbb{R}$, $P(x + T) = P(x)$. Alors, en particulier (en prenant $x = 0$), $P(T) = P(0)$ puis, en prenant $x = T$, $P(2T) = P(T) = P(0)$. Par une récurrence immédiate, $P(nT) = P(0)$ pour tout $n \in \mathbb{N}$. En particulier, le polynôme P et le polynôme constant égal à $P(0)$ coïncident en tous les nT donc en une infinité de points : ils sont par conséquent égaux. En particulier, P est constant.

V.4 Racines multiples

Le polynôme $X^2(X - 1)$ n'admet que deux racines distinctes : 0 et 1. Cependant, intuitivement, nous avons envie de compter 0 « deux fois » et 1 « une seule fois ». On veut définir rigoureusement cette notion de comptage de racines.



Le corollaire ci-dessus est très important et est très utile en pratique, car nous ne savons pas en général le degré des polynômes que nous manipulons. Un moyen simple d'avoir un nombre de racines strictement supérieur au degré (si celui-ci est inconnu) est d'en avoir une infinité ! Par conséquent, quand on veut montrer qu'un polynôme est nul, on cherche en général à montrer qu'il admet une infinité de racines.



Les polynômes sont donc des objets extrêmement rigides : il suffit de connaître un polynôme de degré n en $n + 1$ points pour caractériser totalement ce polynôme !

Définition. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $n \geq 1$. On dit que α est racine de P de multiplicité n ou d'ordre n si $(X - \alpha)^n$ divise P et si $(X - \alpha)^{n+1}$ ne divise pas P .

Remarques :

- Si α est racine de multiplicité 1, on dit que α est une racine simple de P . Si α est racine de multiplicité 2, on dit que α est une racine double de P , etc.
- Si α est racine de multiplicité strictement supérieure à 1, on dit que α est une racine multiple de P .
- Par convention, si α n'est pas racine de P , on dit que α est racine de P de multiplicité nulle.
- Si α_1 de multiplicité m_1 , α_2 de multiplicité m_2 , ..., α_q de multiplicité m_q sont les seules racines de P , on dit que P admet $m_1 + \dots + m_q$ racines, comptées avec multiplicité.

Nous verrons dans le paragraphe VI.4 une caractérisation de la multiplicité d'une racine grâce aux dérivées successives de P .

Exemple : 0 est racine double et 1 est racine simple de $X^2(X - 1)$. On dit que $X^2(X - 1)$ admet trois racines, comptées avec multiplicité.

Proposition. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $n \geq 1$. α est racine de P de multiplicité n si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^n \times Q$ et tel que $Q(\alpha) \neq 0$.

DÉMONSTRATION. Supposons que α soit racine de P de multiplicité n . Alors $(X - \alpha)^n$ divise P donc il existe Q tel que $P = (X - \alpha)^n Q$. Si α est racine de Q alors $X - \alpha$ divise Q donc il existe R tel que $Q = (X - \alpha) \times R$ si bien que $P = (X - \alpha)^{n+1} \times R$: $(X - \alpha)^{n+1}$ divise P ce qui est absurde puisque α est racine de multiplicité n : on en déduit que $Q(\alpha) \neq 0$.

Réciproquement, si P s'écrit sous cette forme, alors $(X - \alpha)^n$ divise P : α est racine de multiplicité au moins n . Si α est racine de multiplicité au moins $n + 1$, alors $(X - \alpha)^{n+1}$ divise P : il existe R tel que $P = (X - \alpha)^{n+1} R = (X - \alpha)^n Q$. Dès lors $(\mathbb{K}[X]$ est un anneau intègre : tout polynôme non nul est régulier), $Q = (X - \alpha)R$ donc α est racine de Q ce qui est absurde : la multiplicité de n est bien égale à n .

Théorème. Soit $P \in \mathbb{K}[X]$. Soient $(\alpha_1, \dots, \alpha_q) \in \mathbb{K}^q$ deux à deux distincts, racines de P de multiplicités respectives m_1, \dots, m_q . Alors $(X - \alpha_1)^{m_1} \times \dots \times (X - \alpha_q)^{m_q}$ divise P .

DÉMONSTRATION. Vient du fait (cf. paragraphe III) que les $(X - \alpha_i)^{m_i}$ sont premiers entre eux deux à deux.

Corollaire. Soit $n \in \mathbb{N}$. Soit $P \in \mathbb{K}[X]$.

- Si P est de degré n , alors P admet au plus n racines comptées avec multiplicité.
- Si P est de degré inférieur ou égal à n et admet au moins $n + 1$ racines, comptées avec multiplicité, alors P est le polynôme nul.

En d'autres termes, un polynôme non nul admet un nombre de racines comptées avec multiplicité inférieur ou égal à son degré.

DÉMONSTRATION. Il suffit d'utiliser le fait que si B divise A et si A est non nul, alors $\deg(B) \leq \deg(A)$. \square

VI Dérivée formelle d'un polynôme

VI.1 Définition

Définition. Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. On appelle polynôme dérivé ou dérivée formelle

On note parfois



$$P' = \sum_{k=0}^{+\infty} k a_k X^{k-1}$$

Pour $k = 0$, le fait ...

du polynôme P le polynôme noté P' ou $D(P)$ défini par :

$$P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$$

Remarques :

- Si on note $P = \sum_{k=0}^n a_k X^k$, alors $P' = \sum_{k=1}^n k a_k X^{k-1}$.
- On définit de même la dérivée seconde etc. d'un polynôme. On note la dérivée seconde P'' ou $D^2(P)$, et si $n \in \mathbb{N}$, on note $P^{(n)}$ ou $D^n(P)$ la dérivée n -ième de P .
-   Cela n'a rien à voir avec un quelconque taux d'accroissement ou une quelconque limite (ce qui n'est pas aisé à définir dans un corps quelconque). Rappelons une dernière fois qu'un polynôme est une suite presque nulle, et si on note $P = (\underbrace{a_0}_0, \underbrace{a_1}_1, \underbrace{a_2}_2, \dots, \underbrace{a_n}_n, 0, 0, \dots)$, alors on **définit** le polynôme dérivé de P par :

$$P' = (\underbrace{a_1}_0, \underbrace{2a_2}_1, \underbrace{3a_3}_2, \dots, \underbrace{na_{n-1}}_{n-1}, 0, 0, 0, \dots)$$

C'est une définition purement arbitraire qui n'a aucun rapport a priori avec la dérivée d'une fonction définie sur \mathbb{R} (et donc qui existe sur tout corps \mathbb{K} alors qu'on ne peut dériver que des fonctions de la variable réelle : comment par exemple définir une notion de limite sur un corps fini ?). En particulier, la dérivée d'un polynôme (à ne pas confondre avec la dérivée d'une **fonction** polynôme) existe toujours et il n'est pas nécessaire de justifier son existence. L'inconvénient est qu'a priori, il n'y a aucune raison pour que la dérivée d'un polynôme vérifie les mêmes propriétés que la dérivée d'une fonction. C'est ce que nous allons démontrer dans la suite.

- Par contre, lorsque $\mathbb{K} = \mathbb{R}$, les deux définitions coïncident. Plus précisément, si on note \tilde{P} la fonction polynomiale associée à P , alors $\tilde{P}' = \tilde{P}'$, c'est-à-dire que la fonction associée à P' est la dérivée de la fonction associée à P , et on pourra parfois identifier les deux sur \mathbb{R} (car, sur \mathbb{R} ou \mathbb{C} on peut parfois identifier polynômes et fonctions polynomiales). C'est pour cela qu'on définit le polynôme formel P' de cette façon, et qu'on le note de la même façon que la dérivée. Mais attention : cela n'est possible que sur \mathbb{R} .

VI.2 Opérations sur les polynômes dérivés

Proposition. La dérivation formelle est un opérateur linéaire, c'est-à-dire que pour tous polynômes P et Q et tous scalaires λ et μ , $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.

DÉMONSTRATION. Soient $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Notons $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q =$

$\sum_{k=0}^{+\infty} b_k X^k$. D'une part :

$$P' = \sum_{k=1}^{+\infty} k a_k X^{k-1} \quad \text{et} \quad Q' = \sum_{k=1}^{+\infty} k b_k X^{k-1}$$

si bien que

$$\lambda P' + \mu Q' = \sum_{k=1}^{+\infty} k(\lambda a_k + \mu b_k) X^{k-1}$$

... que X^{-1} ne soit pas défini est compensé par le fait qu'on le multiplie par $k = 0$ donc le terme $k a_k X^{k-1}$ est nul par convention.

On privilégiera pour l'instant la notation $P^{(n)}$, la notation D^n prendra tout son sens au chapitre 29.

C'est même un bel échec de type de dire qu'un polynôme est continu, dérivable ou \mathcal{C}^∞ (alors que ça a du sens pour une fonction polynôme) : un polynôme n'est pas une fonction ! Bon, on le dira parfois, mais uniquement parce que sur un corps infini (en particulier sur \mathbb{R} ou \mathbb{C}), on peut parfois identifier polynôme et fonction polynomiale associée, cf. paragraphe IV.

et d'autre part, $\lambda P + \mu Q = \sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) X^k$ si bien que

$$(\lambda P + \mu Q)' = \sum_{k=1}^{+\infty} k(\lambda a_k + \mu b_k) X^{k-1}$$

□

On généralise aisément par récurrence à une combinaison linéaire d'un nombre quelconque (fini) de polynômes.

Proposition (admise provisoirement). Soit $(P, Q) \in \mathbb{K}[X]^2$. Alors $(PQ)' = P'Q + PQ'$.

Nous le démontrerons dans le chapitre 29.

Proposition (Formule de Leibniz). Soit $(P, Q) \in \mathbb{K}[X]^2$. Soit $n \in \mathbb{N}$. Alors :

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

DÉMONSTRATION. Analogue à la démonstration faite dans le chapitre 14.

VI.3 Degré d'un polynôme dérivé

Proposition. Soit $P \in \mathbb{K}[X]$. Si P est constant, alors $P' = 0$, et si P n'est pas constant, alors $\deg(P') = \deg(P) - 1$.



Ainsi, quand on voudra donner le degré d'un polynôme dérivé, il faudra faire deux cas. Comme pour la somme des termes d'une suite géométrique : quel est le degré d'un polynôme dérivé ? Ça dépend !

DÉMONSTRATION. Si P est constant alors on a évidemment $P' = 0$. Sinon, en notant $n \geq 1$ le degré de P , on a $P = \sum_{k=0}^n a_k X^k$ avec $a_n \neq 0$ donc

$$P' = \sum_{k=1}^n k a_k X^{k-1}$$

□

et puisque $n a_n \neq 0$, P' est bien de degré $n - 1$.

Remarque : Ce résultat n'est vrai que sur un corps de caractéristique nulle, il est faux sur un corps quelconque. Par exemple, sur $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, la dérivée de $P = X^2$ est $P' = 2X = 0$ car, sur $\mathbb{Z}/2\mathbb{Z}$, $2 = 0$. D'où la nécessité de travailler sur un corps de caractéristique nulle, ce qui sera le cas en pratique car on ne travaillera que sur \mathbb{R} ou \mathbb{C} .



Sur un corps quelconque, le résultat précédent n'est valable que si la caractéristique du corps ne divise pas le degré. Mais bon : HP++.

Corollaire. Soit $P \in \mathbb{K}[X]$. Alors $P' = 0$ si et seulement si P est constant.

On peut généraliser le résultat précédent :

Proposition. Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors $P^{(n+1)} = 0$ si et seulement si $\deg(P) \leq n$.



Pas égal à n mais inférieur ou égal à n !

DÉMONSTRATION. Si $P = \sum_{k=0}^{+\infty} a_k X^k$, par une récurrence immédiate, pour tout $n \in \mathbb{N}$,

$$P^{(n+1)} = \sum_{k=n+1}^{+\infty} k(k-1) \cdots (k-n) a_k X^{k-n-1}$$

□

et ce polynôme est nul si et seulement si tous ses coefficients sont nuls si et seulement si $a_k = 0$ pour tout $k \geq n+1$ si et seulement si $\deg(P) \leq n$.

VI.4 Formule de Taylor et caractérisation de la multiplicité d'une racine

Proposition (Formule de Taylor pour les polynômes (admise provisoirement)).

Soit $P \in \mathbb{K}[X]$ et soit $\alpha \in \mathbb{K}$. Alors

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha) \times (X - \alpha)^k}{k!}$$

En particulier, si P est de degré n , alors

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

Ce résultat n'est valable que sur un corps de caractéristique nulle, il n'est pas valable sur un corps quelconque. Nous le démontrerons dans le chapitre 29, ainsi que le résultat suivant.

Théorème (Admis provisoirement). Soit $n \in \mathbb{N}^*$. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P de multiplicité n si et seulement si

$$P(\alpha) = P'(\alpha) = \dots = P^{(n-1)}(\alpha) = 0 \quad \text{et} \quad P^{(n)}(\alpha) \neq 0.$$

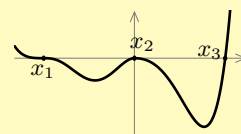
En particulier, α est racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

La multiplicité d'une racine α est donc l'ordre de la première dérivée non nulle en α .

Remarque : Par contraposée : α est racine multiple si et seulement si $P(\alpha) = P'(\alpha) = 0$. Les racines multiples sont donc celles en lesquelles la dérivée s'annule. Géométriquement, ce sont celles en lesquelles le graphe (de la fonction polynomiale associée) admet une tangente horizontale.

Corollaire. Soit $n \in \mathbb{N}^*$. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P . Alors α est racine de P de multiplicité n si et seulement si α est racine de P' de multiplicité $n - 1$.

Par exemple, si P est le polynôme réel dont le graphe (enfin, le graphe de la fonction polynôme associée) est donné ci-dessous.



alors x_1 et x_2 sont des racines multiples, et x_3 est une racine simple. Plus précisément, puisque le polynôme change de signe en x_1 , alors sa multiplicité est impaire, donc supérieure ou égale à 3 car x_1 est racine multiple. De même, la multiplicité de x_2 est paire.

VII Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$

VII.1 Polynômes scindés

Définition. Soit $P \in \mathbb{K}[X]$ non constant. P est scindé s'il peut s'écrire comme un produit de polynômes de degré 1.

Remarques :

- En d'autres termes, un polynôme P de degré $n \geq 1$ est scindé s'il existe $a \in \mathbb{K}^*$ (le coefficient dominant) et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ (ses racines, pas forcément distinctes mais comptées avec multiplicité) tels que

$$P = a(X - \alpha_1) \times \dots \times (X - \alpha_n)$$

- Quand une telle écriture est possible, elle est parfois plus intéressante que l'écriture classique (sous forme de somme) car on connaît alors les racines du polynôme et car on connaît le signe de la fonction polynomiale associée (quand on se place sur \mathbb{R}).
- P est scindé sur \mathbb{K} si et seulement s'il possède un nombre de racines (comptées avec multiplicité) égal à son degré.
- Parfois, on veut que les racines soient distinctes. On regroupe alors les racines égales, ce qui donne

$$P = a(X - \beta_1)^{m_1} \times \dots \times (X - \beta_q)^{m_q}$$

où les β_i sont les racines distinctes de P de multiplicités m_1, \dots, m_q . On a alors $\deg(P) = m_1 + \dots + m_q$.

Chaque écriture a ses avantages et ses inconvénients : l'une est plus simple pour voir le degré, l'autre permet plus facilement de compter les racines distinctes.


Exemples :

- $3X^3 - 6X^2 + 3X = 3X(X-1)^2$ est scindé.
- $X^2 + 1$ n'admet pas de racine réelle donc n'est pas scindé sur \mathbb{R} .
- $X^2 + 1 = (X-i)(X+i)$ est scindé sur \mathbb{C} .
- De même, $X^2 + X + 1$ n'est pas scindé sur \mathbb{R} car n'admet pas de racine réelle, mais il est scindé sur \mathbb{C} puisque $X^2 + X + 1 = (X-j)(X-j^2)$. On voit que le fait qu'un polynôme soit scindé ou non dépend du corps \mathbb{K} sur lequel on se place.

Ces deux polynômes reviennent très souvent dans les exercices : il est utile de connaître leur factorisation sur \mathbb{C} .

Remarque : Pour écrire un polynôme sous forme scindée (quand c'est possible!), il faut connaître :

- ses racines.
- leur multiplicité.
- le coefficient dominant.

 Ne pas oublier le coefficient dominant ou les multiplicités! En effet, si on prend l'exemple de $P = 3X^3 - 6X^2 + 3X$ ci-dessus, alors ses seules racines sont 0 et 1, et si on oublie les multiplicités ou le coefficient dominant, on peut écrire que $P = X(X-1)$, ce qui est évidemment faux!

VII.2 Relations coefficients-racines

Rappelons que si on a $P = aX^2 + bX + c$ un polynôme de degré 2 (donc avec $a \neq 0$), si P est scindé, c'est-à-dire si P admet deux racines x_1 et x_2 (éventuellement égales), alors $P = a(X-x_1)(X-x_2)$ si bien que $P = a(X^2 - (x_1+x_2)X + x_1x_2)$. Dès lors,

$$c = ax_1x_2 \quad \text{et} \quad b = -a(x_1+x_2)$$

En d'autres termes, on peut exprimer les coefficients de P en fonction des racines (et du coefficient dominant). On cherche à généraliser cette notion dans le cas d'un polynôme scindé de degré quelconque.

Regardons ce qui se passe dans le cas d'un polynôme de degré 3. Soit $P = aX^3 + bX^2 + cX + d$ un polynôme de degré 3 (avec donc $a \neq 0$) et on suppose que P est scindé sur \mathbb{K} , c'est-à-dire qu'il existe $(x_1, x_2, x_3) \in \mathbb{K}^3$ tel que $P = a(X-x_1)(X-x_2)(X-x_3)$. En développant, on trouve :

$$P = a(X^3 - (x_1+x_2+x_3)X^2 + (x_1x_2+x_2x_3+x_1x_3)X - x_1x_2x_3)$$

si bien que

$$b = -(x_1+x_2+x_3)a, c = (x_1x_2+x_2x_3+x_1x_3)a \quad \text{et} \quad d = -(x_1x_2x_3)a$$

Là aussi on peut exprimer les coefficients à l'aide des racines et du coefficient dominant. Pour un polynôme scindé de degré n , on a besoin d'introduire de nouvelles notations.

Définition. Soient $n \geq 1$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ et $k \in \llbracket 1; n \rrbracket$. On appelle fonction symétrique élémentaire d'ordre k en x_1, \dots, x_n la somme

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

Remarques :

- Pour faire simple : on prend tous les choix possibles de k indices parmi $1, \dots, n$ i.e. on prend tous les choix possibles de k éléments parmi x_1, \dots, x_n et on somme.

La somme contient donc $\binom{n}{k}$ termes.

- Par exemple, si $n = 4$ et $k = 2$, alors

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

- On les appelle symétriques car, si on intervertit deux x_k , la somme reste la même (échangez x_2 et x_4 ci-dessus par exemple pour vous en convaincre).
- Les formules pour $k = 1$ et $k = n$ doivent être sues sur le bout des doigts :

$$\sigma_1(x_1, \dots, x_n) = x_1 + \dots + x_n \quad \text{et} \quad \sigma_n(x_1, \dots, x_n) = x_1 \times \dots \times x_n$$

Les autres doivent être retrouvées facilement dans un cas explicite (comme ci-dessus).

Il est temps de généraliser les résultats précédents à un polynôme SCINDÉ de degré quelconque.

Théorème (Relations coefficients-racines ou formules de Viète). Soit $n \geq 1$ et soit $P = \sum_{k=0}^n a_k X^k$ un polynôme de degré n (avec donc $a_n \neq 0$ son coefficient dominant) scindé de racines (pas forcément distinctes) x_1, \dots, x_n . Alors, pour tout $k \in \llbracket 1; n \rrbracket$,

$$a_{n-k} = (-1)^k \times a_n \times \sigma_k$$

c'est-à-dire que :

$$P = a_n(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n \sigma_n)$$

Nous montrerons dans le paragraphe VII.3.a que tout polynôme complexe est scindé : ce théorème est donc valable pour tout polynôme complexe (non constant).

On a écrit σ_k au lieu de $\sigma_k(x_1, \dots, x_n)$ par souci de simplification.

Remarques :

- On fera bien attention : on trouve σ_k dans le terme à la puissance $n - k$. On fera également attention à la puissance de -1 .
- Par conséquent, on peut retrouver les coefficients quand on connaît les racines. Malheureusement, le contraire est faux : on ne peut pas (à partir du degré 5) trouver les racines à partir des coefficients (et c'est bien dommage).

DÉMONSTRATION. Il suffit de développer l'écriture $P = a_n(X - x_1) \cdots (X - x_n)$: quand on développe, il faut prendre un terme par parenthèse, et on obtient du X^{n-k} en prenant $n - k$ fois X et k termes de la forme $-x_i$ donc cela donne un terme de la forme $(-x_{i_1}) \times \dots \times (-x_{i_k}) = (-1)^k x_{i_1} \cdots x_{i_k}$ avec $i_1 < \dots < i_k$, et pour avoir le coefficient final, il suffit de tous les prendre, donc de sommer, ce qui donne $(-1)^k \times \sigma_k$, qu'on multiplie finalement par a_n .

Corollaire (Relations coefficients racines ou formules de Viète). Avec les mêmes notations que ci-dessus, pour tout $k \in \llbracket 1; n \rrbracket$, $\sigma_k = (-1)^{n-k} \times \frac{a_{n-k}}{a_n}$. En particulier :

$$\sum_{i=1}^n x_i = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \prod_{i=1}^n x_i = (-1)^n \frac{a_0}{a_n}$$

Ce résultat est une simple réécriture du théorème précédent et donc est également appelé formules de Viète. Il donne en particulier la valeur de la somme et du produit des racines d'un polynôme scindé en fonction de ses coefficients, ce qui est remarquable car on ne sait pas en général trouver ces racines !

VII.3 Dans $\mathbb{C}[X]$

VII.3.a Factorisation sur \mathbb{C}

Théorème (théorème de d'Alembert-Gauß (admis)). Soit $P \in \mathbb{C}[X]$ non constant. Alors P admet une racine complexe.

Remarques :

- Quand on dit « une » racine complexe, il faut bien sûr comprendre « au moins une ».
- Ce théorème est appelé en anglais « fundamental theorem of algebra » : c'est dire son importance !
- Si \mathbb{K} est un corps quelconque, on dit qu'il est algébriquement clos si tout polynôme à coefficients dans \mathbb{K} admet une racine dans \mathbb{K} . Ainsi, le théorème de d'Alembert-Gauß affirme que \mathbb{C} est algébriquement clos. \mathbb{R} et \mathbb{Q} ne sont pas algébriquement clos car $X^2 + 1$ n'admet aucune racine dans ces corps. On peut montrer qu'un corps algébriquement clos est forcément infini (cf. exercice 81) mais, comme on vient de le voir, la réciproque est fausse.

Corollaire. Les irréductibles de \mathbb{C} sont exactement les polynômes de degré 1.

DÉMONSTRATION. On sait déjà que les polynômes de degré 1 sont irréductibles. Réciproquement, soit $P \in \mathbb{C}[X]$ irréductible (donc non constant). D'après le théorème de d'Alembert-Gauß, P admet une racine complexe qu'on note α donc est divisible par $X - \alpha$ si bien qu'il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - \alpha) \times Q$. Si Q n'est pas constant, alors P s'écrit comme le produit de deux polynômes non constants donc n'est pas irréductible, ce qui est absurde. Dès lors, Q est constant (non nul car P est non nul) si bien que P est de degré 1.

Par conséquent, sur \mathbb{C} , la situation est extrêmement simple :

Corollaire (Factorisation d'un polynôme sur \mathbb{C}). Soit $P \in \mathbb{C}[X]$ non constant. Alors P est scindé c'est-à-dire qu'il existe $a \in \mathbb{C}^*$ (le coefficient dominant) et $(\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ (les racines, pas forcément distinctes) tels que

$$P = a(X - \alpha_1) \times \dots \times (X - \alpha_n)$$

De plus, cette écriture est unique à l'ordre près des termes.

DÉMONSTRATION. P admet une décomposition en produit de facteurs irréductibles et les polynômes irréductibles de \mathbb{C} sont exactement les polynômes de degré 1. De plus, cette écriture est unique à l'ordre près des termes, et à multiplication par une constante non nulle près, mais puisqu'ici on impose que les polynômes soient unitaires, la constante devant les $X - \alpha_k$ est forcément égale au coefficient dominant de P : il y a bien unicité.

Remarque : En particulier, les relations coefficients racines vues au paragraphe précédent sont toujours valables sur \mathbb{C} .

Corollaire. Soit $P \in \mathbb{C}[X]$ et soit $n \in \mathbb{N}$. Si P est de degré n , alors P admet exactement n racines complexes (comptées avec multiplicité).

Corollaire. Soient A et B deux polynômes non nuls. Alors B divise A si et seulement si toutes les racines de B sont racines de A , avec une multiplicité plus petite que celle de A .

DÉMONSTRATION. cf. paragraphe III.3.h : un polynôme en divise un autre si et seulement si ses facteurs irréductibles apparaissent chez l'autre à une puissance plus grande.

Donnons enfin une CNS simple pour que deux polynômes complexes soient premiers entre eux.

On pourrait également prouver ce résultat par récurrence sur le degré de n , exo.

Si P est écrit sous forme scindée, on dit qu'il est écrit sous forme factorisée (puisque cette écriture est sa factorisation en produit de facteurs irréductibles).

C'est-à-dire que la multiplicité des racines de A est plus grande que pour B .

Proposition. Deux polynômes complexes non tous nuls sont premiers entre eux si et seulement s'ils n'ont aucune racine complexe commune.

DÉMONSTRATION. Soient A et B deux polynômes complexes non tous nuls. Prouvons (ce qui revient exactement au même) que A et B ne sont pas premiers entre eux si et seulement s'ils ont une racine complexe commune.

Si A et B ont une racine complexe commune alors ils sont tous les deux divisibles par $X - \alpha$ donc ils ne sont pas premiers entre eux (ils ont un diviseur commun non constant).

Réciproquement, supposons qu'ils ne soient pas premiers entre eux et notons D un PGCD de A et de B . Puisque A et B ne sont pas premiers entre eux, D n'est pas constant donc, d'après le théorème de d'Alembert-Gauß, D admet une racine complexe notée α . Or, D divise A et B donc il existe Q et R tels que $A = DQ$ et $B = DR$ si bien que α est racine de A et B : A et B ont bien une racine complexe commune, d'où le résultat.

Exemple : On retrouve le fait que si α et β sont deux complexes distincts et si n et m sont deux entiers supérieurs ou égaux à 1, alors $(X - \alpha)^n$ et $(X - \beta)^m$ sont premiers entre eux puisqu'ils n'ont aucune racine complexe commune.

Remarque : Dans le cas d'un corps \mathbb{K} quelconque (et en particulier sur \mathbb{R}), il est faux de dire que deux éléments de $\mathbb{K}[X]$ sont premiers entre eux si et seulement s'ils n'ont aucune racine commune dans \mathbb{K} . Par exemple, si $A = B = X^2 + 1$ dans $\mathbb{R}[X]$, ces polynômes sont égaux donc ne sont pas premiers entre eux, pourtant ils n'ont aucune racine réelle donc aucune racine réelle commune !

Cependant, la proposition précédente peut aussi nous aider sur \mathbb{R} puisque \mathbb{R} est inclus dans \mathbb{C} :

Corollaire. Deux polynômes réels non tous nuls sont premiers entre eux si et seulement s'ils n'ont aucune racine COMPLEXE commune.

VII.3.b Exemples

- Factoriser sur \mathbb{C} le polynôme $P = X^n - 1$.

Rappel : il faut les racines, leur multiplicité, le coefficient dominant. Cherchons donc les racines de P . Soit $z \in \mathbb{C}$.

$$P(z) = 0 \iff z^n = 1$$

$$\iff z \text{ est une racine } n\text{-ième de l'unité}$$

$$\iff \exists k \in \llbracket 0; n-1 \rrbracket, z = e^{2ik\pi/n}$$

Dès lors, les racines de P sont exactement les $e^{2ik\pi/n}$ où $k \in \llbracket 0; n-1 \rrbracket$. On a n racines, le polynôme est de degré n donc admet n racines avec multiplicité : ces racines sont donc forcément simples, et puisque P est unitaire, on a :

$$P = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n})$$

- Factorisons (sur \mathbb{C}) le polynôme $P = (X + i)^n - (X - i)^n$.

Soit $z \in \mathbb{C}$. i n'est pas solution (car $(2i)^n \neq 0$) : on peut donc supposer $z \neq i$.



Ne jamais écrire $X = e^{2ik\pi/n}$ ou toute autre horreur du même genre, cf. paragraphe I.3.



Ne pas oublier les multiplicités ni le coefficient dominant ! Si on se contente de donner les racines, le raisonnement est incomplet, cf. paragraphe VII.1.

$$P(z) = 0 \iff (z+i)^n = (z-i)^n$$

$$\iff \left(\frac{z+i}{z-i}\right)^n = 1$$

$$\iff \frac{z+i}{z-i} \text{ est une racine } n\text{-ième de l'unité.}$$

$$\iff \exists k \in \llbracket 0; n-1 \rrbracket, \quad \frac{z+i}{z-i} = e^{2ik\pi/n}$$

$$\iff \exists k \in \llbracket 0; n-1 \rrbracket, \quad z+i = (z-i)e^{2ik\pi/n}$$

$$\iff \exists k \in \llbracket 0; n-1 \rrbracket, \quad z(1 - e^{2ik\pi/n}) = i \times (-1 - e^{2ik\pi/n})$$

Si $k = 0$, alors le membre de gauche vaut 0 et celui de droite vaut 0 : $k = 0$ n'est pas solution. On peut donc supposer $k \neq 0$ si bien que $1 - e^{2ik\pi/n} \neq 0$.

$$P(z) = 0 \iff \exists k \in \llbracket 1; n-1 \rrbracket, \quad z(1 - e^{2ik\pi/n}) = i \times (-1 - e^{2ik\pi/n})$$

$$\iff \exists k \in \llbracket 1; n-1 \rrbracket, \quad z = i \times \frac{-1 - e^{2ik\pi/n}}{1 - e^{2ik\pi/n}}$$

$$\iff \exists k \in \llbracket 1; n-1 \rrbracket, \quad z = i \times \frac{e^{ik\pi/n} \times (-e^{-ik\pi/n} - e^{ik\pi/n})}{e^{ik\pi/n} \times (e^{-ik\pi/n} - e^{ik\pi/n})}$$

$$\iff \exists k \in \llbracket 1; n-1 \rrbracket, \quad z = i \times \frac{-2i \sin(k\pi/n)}{2 \cos(k\pi/n)}$$

$$\iff \exists k \in \llbracket 1; n-1 \rrbracket, \quad z = \frac{\sin(k\pi/n)}{\cos(k\pi/n)}$$

On a $n-1$ racines. Cherchons le degré de P et son coefficient dominant. D'après le binôme de Newton :

$$\begin{aligned} P &= \sum_{k=0}^n \binom{n}{k} X^k i^{n-k} - \sum_{k=0}^n \binom{n}{k} X^k (-i)^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} (i^{n-k} - (-i)^{n-k}) X^k \end{aligned}$$

★ Le coefficient devant X^n est

$$\binom{n}{n} (i^0 - (-i)^0) = 0$$

★ Le coefficient devant X^{n-1} est

$$\binom{n}{n-1} (i^1 - (-i)^1) = 2ni$$

Dès lors, P est de degré $n-1$ et de coefficient dominant $2ni$. Puisqu'on a trouvé $n-1$ racines, elles sont forcément simples. En conclusion :

$$P = 2ni \prod_{k=1}^n \left(X - \frac{\sin(k\pi/n)}{\cos(k\pi/n)} \right)$$

VII.4 Dans $\mathbb{R}[X]$

VII.4.a Factorisation sur \mathbb{R}

On cherche le degré de P , c'est-à-dire la plus grande puissance avec un coefficient non nul. On part donc de la plus grande puissance possible, n , et on cherche si le coefficient est non nul : si oui, on s'arrête, sinon, on descend, jusqu'à obtenir un coefficient non nul : la puissance correspondante sera alors le degré et le coefficient en question sera le coefficient dominant.

Proposition. Soit $P \in \mathbb{R}[X]$ et soit $\alpha \in \mathbb{C}$ racine de P . Alors $\bar{\alpha}$ est racine de P de même multiplicité que α .



Même si α est complexe, P est à coefficients réels !

DÉMONSTRATION. Notons $P = \sum_{k=0}^n a_k X^k$. α est racine de P donc $P(\alpha) = 0$ donc $\overline{P(\alpha)} = 0$, c'est-à-dire :

$$\overline{\sum_{k=0}^n a_k \alpha^k} = 0$$

Or, les a_k sont des réels, si bien que $\sum_{k=0}^n a_k \bar{\alpha}^k = 0$, c'est-à-dire que $P(\bar{\alpha}) = 0$. Par conséquent, $\bar{\alpha}$ est racine de P . On vient donc de prouver l'implication :

$$\alpha \text{ racine de } P \Rightarrow \bar{\alpha} \text{ racine de } P \quad \square$$

En appliquant ce résultat à $\bar{\alpha}$ à la place de α (penser à « truc »), il vient que si $\bar{\alpha}$ est racine de P , c'est aussi le cas de $\bar{\bar{\alpha}} = \alpha$: l'implication ci-dessus est donc une équivalence. Enfin, le polynôme P étant quelconque, on en déduit les équivalences suivantes :

- $P'(\alpha) = 0 \iff P'(\bar{\alpha}) = 0$.
- $P''(\alpha) = 0 \iff P''(\bar{\alpha}) = 0$.
- Plus généralement, pour tout k , $P^{(k)}(\alpha) = 0 \iff P^{(k)}(\bar{\alpha}) = 0$.

ce qui permet de conclure avec le théorème du paragraphe VI.4 reliant multiplicité d'une racine et dérivées successives.

Exemple :

- $1 + i$ et $1 - i$ sont racines de $X^2 - 2X + 2$.
- Raisonnement classique : si P est un polynôme réel et si $\alpha \in \mathbb{C}$, alors α est racine de P si et seulement si $\bar{\alpha}$ est racine de P , et si et seulement si (si $\alpha \neq \bar{\alpha}$ i.e. si α n'est pas réel) P est divisible par $(X - \alpha)(X - \bar{\alpha})$. Par exemple, si $P \in \mathbb{R}[X]$, si i est racine de P alors $-i$ également et P est divisible par $(X - i)(X + i) = X^2 + 1$ (réciproque immédiate). De même, si j est racine de P alors j^2 aussi et P est alors divisible par $(X - j)(X - j^2) = X^2 + X + 1$.

Théorème (Factorisation d'un polynôme sur \mathbb{R}). Soit $P \in \mathbb{R}[X]$. Alors P peut s'écrire comme un produit de polynômes de degré 1 et de polynômes de degré 2 de discriminant strictement négatif.

Exemple : $X^4 - 2X^3 + 2X^2 - 2X + 1 = (X - 1)^2(X^2 + 1)$.

DÉMONSTRATION. Soit $P \in \mathbb{R}[X]$. Alors $P \in \mathbb{C}[X]$. D'après le paragraphe précédent, P est scindé sur \mathbb{C} : il existe $a \in \mathbb{R}^*$ (son coefficient dominant : il est donc réel) et $(\alpha_1, \dots, \alpha_q) \in \mathbb{C}^q$ distincts (les racines, qui sont donc complexes) de multiplicités respectives m_1, \dots, m_q tels que

$$P = a(X - \alpha_1)^{m_1} \times \dots \times (X - \alpha_q)^{m_q}$$

Quitte à changer l'ordre des racines, on suppose que $\alpha_1, \dots, \alpha_r$ sont réelles et que $\alpha_{r+1}, \dots, \alpha_q$ sont complexes non réelles. Or, d'après la proposition précédente, si $\beta \in \mathbb{C}$ alors $\bar{\beta}$ est racine avec la même multiplicité. Encore une fois, quitte à changer l'ordre des racines, on suppose que :

$$\alpha_{r+2} = \overline{\alpha_{r+1}}, \alpha_{r+4} = \overline{\alpha_{r+3}}, \dots, \alpha_q = \overline{\alpha_{q-1}}$$

On note $\beta_1 = \alpha_{r+1}$, de multiplicité n_1 , $\beta_2 = \alpha_{r+3}$, de multiplicité n_2 , et ainsi de suite jusqu'à $\beta_s = \alpha_{q-1}$, de multiplicité n_s . En d'autres termes :

$$P = a(X - \alpha_1)^{m_1} \times \cdots \times (X - \alpha_r)^{m_r} (X - \beta_1)^{n_1} \times (X - \overline{\beta_1})^{n_1} \times \cdots \times (X - \beta_s)^{n_s} \times (X - \overline{\beta_s})^{n_s}$$

Or, pour tout $k \in \llbracket 1; s \rrbracket$,

$$(X - \beta_k) \times (X - \overline{\beta_k}) = X^2 - 2\operatorname{Re}(\beta_k)X + |\beta_k|^2$$

qui est un polynôme de degré 2 à coefficients réels de discriminant strictement négatif (inutile de le calculer : ses racines ne sont pas réelles, son discriminant ne peut pas être positif!). Notons $Q_k = (X - \beta_k) \times (X - \overline{\beta_k})$. Finalement,

$$P = a(X - \alpha_1)^{m_1} \times \cdots \times (X - \alpha_r)^{m_r} \times Q_1^{n_1} \times \cdots \times Q_s^{n_s} \quad \square$$

Inutile de calculer un discriminant si on sait que le polynôme n'admet pas de racine le discriminant sera automatiquement strictement négatif!


Corollaire. Les irréductibles de \mathbb{R} sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif, et l'écriture de P comme produit de polynômes de degré 1 et de degré 2 de discriminant strictement négatif est sa décomposition en produit de facteurs irréductibles (et donc est unique à l'ordre près des termes et à multiplication par un réel non nul près).

DÉMONSTRATION. Soit $P \in \mathbb{R}[X]$.

- Si $\deg(P) = 1$ alors P est irréductible.
- Supposons que P soit de degré 2 de discriminant strictement négatif. Si P peut s'écrire comme produit de deux polynômes non constants, puisque $\deg(P) = 2$, alors P est le produit de deux polynômes de degré 1, en particulier P a au moins une racine réelle, ce qui est absurde : P est irréductible.

Montrons à présent qu'il n'y a pas d'autre polynôme irréductible.

- Si $\deg(P) = 2$ avec un discriminant positif (ou nul), alors P est scindé sur \mathbb{R} donc n'est pas irréductible.
- Si $\deg(P) \geq 3$ alors P s'écrit comme produit de polynômes de degré 1 ou de degré 2 de discriminant strictement négatif donc n'est pas irréductible.

Remarque :  « irréductible \neq ne pas avoir de racine » ! Un polynôme irréductible a une définition bien précise, tout comme la décomposition en produit de facteurs irréductibles. Ce n'est pas parce qu'un polynôme n'a pas de racine réelle qu'il ne peut pas se décomposer ! Par exemple, $X^4 + 1$ n'a aucune racine réelle mais n'est pas irréductible car est de degré 4, cf. paragraphe suivant pour sa décomposition en produit de facteurs irréductibles.

Il est tout de même remarquable que les irréductibles de \mathbb{R} ou de \mathbb{C} soient aussi simples. Dans un corps \mathbb{K} quelconque, ce n'est pas forcément la même chose : par exemple, sur un corps fini ou même sur \mathbb{Q} , il existe des polynômes irréductibles de degré quelconque !

VII.4.b Exemples

- Factoriser sur \mathbb{R} le polynôme $P = X^5 + X^4 - X^2 - X$.

On commence par chercher des racines évidentes $(0, \pm 1, \pm 2)$. On remarque que 0, 1 et -1 sont racines évidentes : P est donc divisible par $X(X - 1)(X + 1) = X^3 - X$. On pourrait effectuer la division euclidienne de P par $X^3 - X$ (et cela marcherait très bien, exo) mais nous allons voir une autre méthode. Puisque $X^3 - X$ divise P , il existe $Q \in \mathbb{R}[X]$ tel que $P = (X^3 - X) \times Q$. Comme P est de degré 5 et $X^3 - X$ de degré 3, on a $\deg(Q) = 2$: il existe $(a, b, c) \in \mathbb{R}^2$ tels que $P = (X^3 - X) \times (aX^2 + bX + c)$. En développant, il vient :

$$P = aX^5 + bX^4 + (c - a)X^3 - bX^2 - cX$$

Par unicité des coefficients d'un polynôme, on trouve $-c = -1$ donc $c = 1$, $-b = -1$ donc $b = 1$ et $a = 1$ (et $c - a = 0$ ce qui est cohérent avec les valeurs $a = c = 1$). Dès lors, $P = (X^3 - X)(X^2 + X + 1)$. Or, le discriminant de $X^2 + X + 1$ vaut -3 : on ne peut pas aller plus loin. En conclusion, la forme factorisée de P est $P = X(X - 1)(X + 1)(X^2 + X + 1)$.

- Factoriser sur \mathbb{R} le polynôme $P = 2X^4 - 4X^3 - 4X^2 + 6X + 4$.

On vérifie que -1 et 2 sont racines évidentes : P est divisible par $(X+1)(X-2) = X^2 - X - 2$. Comme $\deg(P) = 4$ et $X^2 - X - 2$ est de degré 2, il existe $(a, b, c) \in \mathbb{R}^3$ tels que $P = (X^2 - X - 2)(aX^2 + bX + c)$ (on pourrait aussi faire la division euclidienne). De même, on trouve $a = 2, b = c = -2$ si bien que $P = (X+1)(X-2)(2X^2 - 2X - 2)$. Le discriminant de $2X^2 - 2X - 2$ vaut $20 > 0$: il admet donc deux racines simples

$$\frac{2 \pm \sqrt{20}}{4} = \frac{2 \pm 2\sqrt{5}}{4} = \frac{1 \pm \sqrt{5}}{2}.$$

Ainsi (ne pas oublier le coefficient dominant !), d'après le paragraphe précédent,

$$2X^2 - 2X - 2 = 2 \left(X - \frac{1 - \sqrt{5}}{2} \right) \left(X - \frac{1 + \sqrt{5}}{2} \right)$$

En conclusion, la forme factorisée de P est :

$$P = 2(X+1)(X-2) \left(X - \frac{1 - \sqrt{5}}{2} \right) \left(X - \frac{1 + \sqrt{5}}{2} \right).$$

- Factoriser sur \mathbb{R} le polynôme $X^4 + 1$.

$$\begin{aligned} X^4 + 1 &= (X^2 + 1)^2 - 2X^2 \\ &= (X^2 + 1)^2 - (X\sqrt{2})^2 \\ &= (X^2 + 1 - X\sqrt{2}) \times (X^2 + 1 + X\sqrt{2}) \end{aligned}$$

Remarque : Cependant, ce n'est pas toujours aussi simple. Factoriser un polynôme en général est difficile. Dans le cas général, la démonstration du théorème ci-dessus nous fournit un moyen « simple » de factoriser un polynôme réel :

- Trouver les racines complexes et leur multiplicité (i.e. factoriser sur \mathbb{C}).
- Mettre à part les racines réelles.
- Regrouper les racines conjuguées.

Faisons comme si nous n'avions pas vu l'astuce ci-dessus et appliquons la méthode ci-dessus pour redonner la factorisation de $P = X^4 + 1$ sur \mathbb{R} . Commençons par donner les racines complexes. Soit $z \in \mathbb{C}$. $P(z) = 0 \iff z^4 = -1$. Or, $-1 = e^{i\pi}$ donc (cf. chapitre 7) les racines quatrièmes de -1 sont

$$e^{i\pi/4}, e^{i(\frac{\pi}{4} + \frac{2\pi}{4})} = e^{3i\pi/4}, e^{i(\frac{\pi}{4} + \frac{4\pi}{4})} = e^{5i\pi/4} \quad \text{et} \quad e^{i(\frac{\pi}{4} + \frac{6\pi}{4})} = e^{7i\pi/4}$$

On a quatre racines distinctes et $\deg(P) = 4$ donc elles sont simples. De plus, P est unitaire donc on obtient la factorisation suivante (sur \mathbb{C}) :

$$P = (X - e^{i\pi/4}) (X - e^{3i\pi/4}) (X - e^{5i\pi/4}) (X - e^{7i\pi/4})$$

Sur \mathbb{R} , regroupons les racines conjuguées. On a $e^{7i\pi/4} = e^{-i\pi/4} = \overline{e^{i\pi/4}}$ et $e^{5i\pi/4} = e^{-3i\pi/4} = \overline{e^{3i\pi/4}}$. Par conséquent :

$$\begin{aligned} P &= (X - e^{i\pi/4}) (X - \overline{e^{i\pi/4}}) (X - e^{3i\pi/4}) (X - \overline{e^{3i\pi/4}}) \\ &= (X^2 - (e^{i\pi/4} + e^{-i\pi/4})X + 1) \times (X^2 - (e^{3i\pi/4} + e^{-3i\pi/4})X + 1) \\ &= (X^2 - 2X \cos(\pi/4) + 1) \times (X^2 - 2X \cos(3\pi/4) + 1) \\ &= (X^2 - X\sqrt{2} + 1) \times (X^2 + X\sqrt{2} + 1) \end{aligned}$$

Inutile de calculer les discriminants : le polynôme n'a pas de racine réelle, ils sont forcément strictement négatifs.

Simple en théorie : en général, on ne sait pas trouver les racines complexes, donc on ne sait pas factoriser un polynôme dans le cas général.

On peut l'affirmer directement mais si on veut le prouver :

$$\begin{aligned} e^{7i\pi/4} &= e^{\frac{8i\pi}{4} - \frac{i\pi}{4}} \\ &= e^{2i\pi - \frac{i\pi}{4}} \\ &= e^{-i\pi/4} \\ &= \overline{e^{i\pi/4}} \end{aligned}$$

et idem pour l'autre. Cela se voit très bien sur le dessin page suivante :

et on retrouve bien sûr la même chose (il y a unicité!).

Donnons un dernier exemple pour la route : factorisons sur \mathbb{R} le polynôme $P = X^{2n} - 1$.
Commençons par le factoriser sur \mathbb{C} : d'après le paragraphe VII.3.b (en remplaçant n par $2n$), sa factorisation sur \mathbb{C} est :

$$P = \prod_{k=0}^{2n-1} (X - e^{ik\pi/n})$$

Cherchons, parmi les racines, lesquelles sont réelles. Soit donc $k \in \llbracket 0; 2n-1 \rrbracket$.

$$e^{ik\pi/n} \in \mathbb{R} \iff k\pi/n \equiv 0[\pi]$$

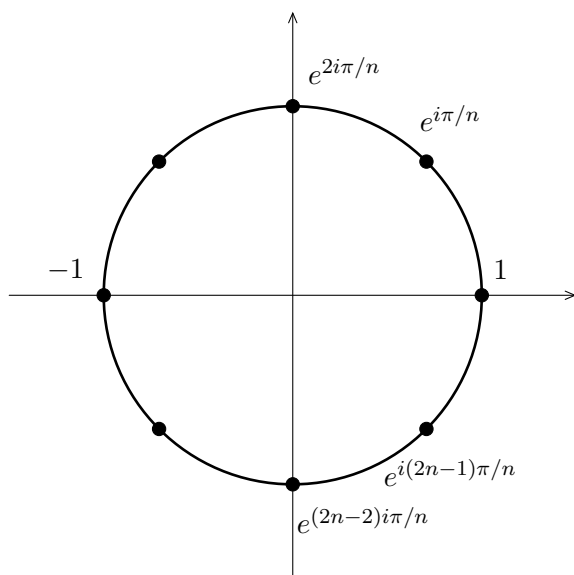
$$\iff k \equiv 0[n]$$

$$\iff k \text{ est un multiple de } n$$

Par conséquent, les seules racines réelles sont obtenues pour $k = 0$ et $k = n$ et sont égales respectivement à 1 et -1 (ce qu'on savait déjà : ce sont les seules solutions réelles de l'équation $z^{2n} = 1$). Dès lors :

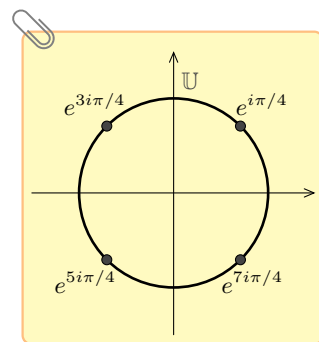
$$P = (X - 1)(X + 1) \prod_{k=1}^{n-1} (X - e^{ik\pi/n}) \times \prod_{k=n+1}^{2n-1} (X - e^{ik\pi/n})$$

Parmi les racines complexes, cherchons lesquelles sont conjuguées : faisons un dessin.



Le conjugué de $e^{ik\pi/n}$ étant $e^{i(2n-k)\pi/n}$, faisons le changement d'indice $p = 2n - k$ dans le deuxième produit :

$$\begin{aligned} P &= (X - 1)(X + 1) \prod_{k=1}^{n-1} (X - e^{ik\pi/n}) \times \prod_{p=1}^{n-1} \left(X - e^{i\frac{(2n-p)\pi}{n}} \right) \\ &= (X - 1)(X + 1) \prod_{k=1}^{n-1} (X - e^{ik\pi/n}) \times \left(X - e^{i\left(2\pi - \frac{k\pi}{n}\right)} \right) \\ &= (X - 1)(X + 1) \prod_{k=1}^{n-1} (X - e^{ik\pi/n}) \times (X - e^{-ik\pi/n}) \\ &= (X - 1)(X + 1) \prod_{k=1}^{n-1} (X^2 - 2\cos(k\pi/n)X + 1) \end{aligned}$$



VIII Activité - Expressions polynomiales en quelque-chose (oui, c'est flou...)

L'idée sous-jacente est assez simple : on peut évaluer un polynôme en tout et n'importe quoi. Par exemple, si $P = a_n X^n + \dots + a_1 X + a_0$, alors $P(2) = a_n \times 2^n + \dots + a_1 \times 2 + a_0$, mais on peut évaluer P en des quantités plus générales. Par exemple, si $P \in \mathbb{R}[X]$, alors, pour tout $x \in \mathbb{R}$,

$$P(\cos(x)) = a_n \times \cos^n(x) + \dots + a_1 \times \cos(x) + a_0.$$

Nous ferons plutôt le cheminement inverse : si on a une quantité de ce type (une combinaison linéaire de puissances), on peut le voir comme l'image par un certain polynôme. Par exemple, $2\cos^2(x) - 1 = T_2(\cos(x))$ où $T_2 = 2X^2 - 1$. On dit que $2\cos^2(x) - 1$ est polynomiale en $\cos(x)$, c'est-à-dire que c'est l'image de $\cos(x)$ par un certain polynôme. De la même façon, si $x \neq 0$, alors

$$\frac{-6}{x^4} + \frac{4}{x^6} = P_2\left(\frac{1}{x}\right)$$

où $P_2 = -6X^4 + 4X^6$: on dit que la quantité ci-dessus est polynomiale en $1/x$. Plus généralement, donnons une définition (vague ! mais intuitive) :

Définition (vague). On dit qu'une quantité est polynomiale en truc si cette quantité s'exprime comme somme, produit, combinaison linéaire de puissances positives de truc.

Donnons deux exemples très classiques de cette idée générale.

Exemple : Reprenons la fonction étudiée dans le chapitre 14 :

$$g : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} e^{-1/x^2} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{cases}$$

Montrer que, pour tout $n \in \mathbb{N}$, il existe $P_n \in \mathbb{R}[X]$ dont on précisera le degré tel que :

$$\forall x \neq 0, \quad g^{(n)}(x) = P_n\left(\frac{1}{x}\right) \times e^{-1/x^2}$$

En déduire que g est \mathcal{C}^∞ sur \mathbb{R} .

Disons tout de suite que g est \mathcal{C}^∞ sur \mathbb{R}^* car composée de la fonction $x \mapsto -1/x^2$ qui est \mathcal{C}^∞ sur \mathbb{R}^* et de la fonction \exp qui est \mathcal{C}^∞ sur \mathbb{R} . On va raisonner par récurrence pour l'existence et le degré de P_n , mais il faut d'abord conjecturer son degré : regardons pour cela ce qui se passe pour les petites valeurs de n . Soit $x \in \mathbb{R}^*$.

- $g(x) = e^{-1/x^2}$, donc $P_0 = 1$ (de degré 0) convient.
- $g'(x) = \frac{2}{x^3} \times e^{-1/x^2}$. Ainsi, $P_1 = 2X^3$, de degré 3, convient.
- On a :

$$\begin{aligned} g''(x) &= \left(\frac{-6}{x^4} + \frac{2}{x^3} \times \frac{2}{x^3} \right) \times e^{-1/x^2} \\ &= \left(\frac{-6}{x^4} + \frac{4}{x^6} \right) \times e^{-1/x^2} \end{aligned}$$

Finalement, si on pose $P_2 = -6X^4 + 4X^6$ (de degré 6), alors on a bien $g''(x) = P_2(1/x) \times e^{-1/x^2}$.

Les cas particuliers précédents semblent justifier la récurrence ci-dessous :

- Si $n \in \mathbb{N}$, notons H_n : « il existe $P_n \in \mathbb{R}[X]$ de degré $3n$ tel que, pour tout $x \neq 0$, $g^{(n)}(x) = P_n\left(\frac{1}{x}\right) \times e^{-1/x^2}$ ».

Pour donner une définition générale, vu que nous allons l'utiliser pour des matrices, des réels, et même des coefficients d'une matrice (nous dirons par exemple que le déterminant d'une matrice est polynomial en les coefficients, cf. chapitre 33), il faudrait se placer sur un anneau général et même introduire des polynômes à plusieurs indéterminées, alors que l'idée générale est assez simple.

g admet deux points d'inflexion, en $\pm\sqrt{2/3}$.

- D'après ce qui précède, H_0, H_1, H_2 sont vraies.
- Soit $n \geq 2$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $P_n \in \mathbb{R}[X]$ de degré $3n$ tel que, pour tout $x \neq 0$, $g^{(n)}(x) = P_n\left(\frac{1}{x}\right) \times e^{-1/x^2}$. Soit $x \neq 0$.

$$\begin{aligned} g^{(n+1)}(x) &= (g^{(n)})'(x) \\ &= \left(-\frac{1}{x^2} \times P_n' \left(\frac{1}{x}\right) + P_n \left(\frac{1}{x}\right) \times \frac{2}{x^3}\right) e^{-1/x^2} \end{aligned}$$

Posons $P_{n+1} = -X^2 P_n' + 2X^3 P_n$. Alors on a bien :

$$\forall x \neq 0, \quad g^{(n+1)}(x) = P_{n+1} \left(\frac{1}{x}\right) e^{-1/x^2}.$$

De plus, par hypothèse de récurrence, $\deg(P_n) = 3n$ donc $\deg(P_n') = 3n - 1$ donc $\deg(-X^2 P_n') = 3n + 1$. De plus, $\deg(2X^3 P_n) = 3n + 3$. On somme deux polynômes de degré distinct donc

$$\begin{aligned} \deg(P_{n+1}) &= \max(\deg(-X^2 P_n'), \deg(2X^3 P_n)) \\ &= 3n + 3 \\ &= 3(n + 1) \end{aligned}$$

Finalement, H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$.

Montrons à présent que g est \mathcal{C}^∞ . Encore une fois, raisonnons par récurrence et montrons que g est \mathcal{C}^n pour tout $n \geq 1$.

- Si $n \geq 1$, notons H_n : « g est de classe \mathcal{C}^n ».
- H_1 est vraie d'après le chapitre 14.
- Soit $n \geq 1$. Supposons H_n vraie et montrons que H_{n+1} est vraie. D'après ce qui précède, il existe $P_{n+1} \in \mathbb{R}[X]$ tel que, pour tout $x \neq 0$,

$$g^{(n+1)}(x) = P_{n+1} \left(\frac{1}{x}\right) e^{-1/x^2}.$$

Or, $y = 1/x^2 \xrightarrow{x \rightarrow 0} +\infty$ et, pour tout $k \in \mathbb{N}$, $y^{k/2} e^{-y} \xrightarrow{y \rightarrow +\infty} 0$ par croissances comparées. Par composition de limites,

$$y^{k/2} e^{-y} = \left| \frac{1}{x^k} \right| e^{-1/x^2} \xrightarrow{x \rightarrow 0} 0 \quad \text{donc} \quad \frac{1}{x^k} e^{-1/x^2} \xrightarrow{x \rightarrow 0} 0.$$

Or, $P_{n+1}(1/x)e^{-1/x^2}$ est une combinaison linéaire (finie) de tels termes, donc une combinaison linéaire de termes qui tendent vers 0. Ainsi, $g^{(n+1)}(x) \xrightarrow{x \rightarrow 0} 0$. De plus, g est \mathcal{C}^{n+1} sur \mathbb{R}^* et, par hypothèse de récurrence, g est \mathcal{C}^n c'est-à-dire que $g^{(n)}$ est \mathcal{C}^1 sur \mathbb{R}^* et continue sur \mathbb{R} . D'après le théorème de la limite de la dérivée (cf. chapitre 14) à $g^{(n)}$, $g^{(n)}$ est \mathcal{C}^1 sur \mathbb{R} (et sa dérivée est nulle en 0), donc g est \mathcal{C}^{n+1} et $g^{(n+1)}(0) = 0$: H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 1$.

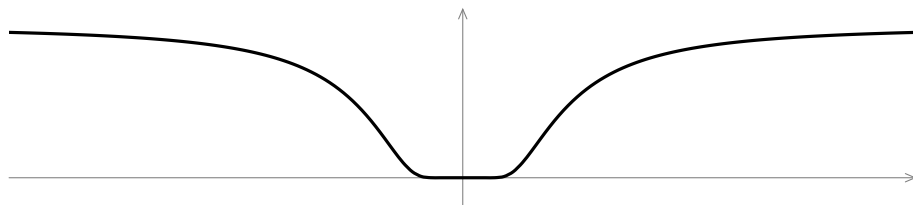
On peut même montrer l'unicité du polynôme P_n . En effet, supposons qu'il existe un autre polynôme Q_n qui convient. Alors, pour tout $x \neq 0$, $e^{-1/x^2} \neq 0$ donc $P_n(1/x) = Q_n(1/x)$. En d'autres termes, P_n et Q_n coïncident en tout réel de la forme $1/x$, donc sur l'image de la fonction inverse. Or, l'image de la fonction inverse est \mathbb{R}^* donc P_n et Q_n coïncident sur \mathbb{R}^* qui est infini donc $P_n = Q_n$.

On a identifié ci-dessus P_n à la fonction polynomiale associée et on a dérivé comme une fonction composée classique et c'est ce qu'on fera en pratique.

Le degré de P_{n+1} n'importe pas ici.

Attention, x peut être positif ou négatif, donc $y^{k/2} = \sqrt{y^k} = \sqrt{1/x^{2k}} = |1/x^k|$.

Dès lors, g est de classe \mathcal{C}^∞ et, pour tout $n \in \mathbb{N}$, $g^{(n)}(0) = 0$. Ci-dessous le graphe de g :



Exemple : Les polynômes de Tchebychev (enfin !)

Soit $x \in \mathbb{R}$. On sait que $\cos(2x) = 2\cos^2(x) - 1$ et $\cos(3x) = 4\cos^3(x) - 3\cos(x)$: $\cos(2x)$ et $\cos(3x)$ sont polynomiaux en $\cos(x)$. Plus précisément, si on pose $T_2 = 2X^2 - 1$ et $T_3 = 4X^3 - 3X$, alors $T_2(\cos(x)) = \cos(2x)$ et $T_3(\cos(x)) = \cos(3x)$. On veut généraliser ce résultat.

Montrons plus généralement le résultat suivant :

$$\forall n \geq 0, \exists! T_n \in \mathbb{R}[X], \forall \theta \in \mathbb{R}, \cos(n\theta) = T_n(\cos(\theta))$$

Existence : par récurrence sur \mathbb{N} .

- Si $n \geq 0$, notons H_n : « il existe $T_n \in \mathbb{R}[X]$ tel que, pour tout $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$ ».
- Si $n = 0$: pour tout $\theta \in \mathbb{R}$, $\cos(0 \times \theta) = 1$ donc $T_0 = 1$ convient : H_0 est vraie.
- Si $n = 1$: pour tout $\theta \in \mathbb{R}$, $\cos(1 \times \theta) = \cos(\theta)$ donc $T_1 = X$ convient : H_1 est vraie.
- On a vu que H_2 et H_3 sont vraies avec $T_2 = 2X^2 - 1$ et $T_3 = 4X^3 - 3X$.
- Soit $n \geq 3$. Supposons H_n et H_{n-1} vraies et prouvons que H_{n+1} est vraie. Soit $\theta \in \mathbb{R}$.

$$\begin{aligned} \cos((n+1)\theta) &= \cos(n\theta)\cos(\theta) - \sin(n\theta)\sin(\theta) \\ &= \cos(n\theta)\cos(\theta) - \frac{1}{2}[\cos((n-1)\theta) - \cos((n+1)\theta)] \end{aligned}$$

Dès lors,

$$\frac{1}{2} \times \cos((n+1)\theta) = \cos(n\theta)\cos(\theta) - \frac{1}{2} \times \cos((n-1)\theta)$$

Finalement :

$$\cos((n+1)\theta) = 2\cos(\theta)\cos(n\theta) - \cos((n-1)\theta)$$

Par hypothèse de récurrence, il existe T_n et T_{n-1} appartenant à $\mathbb{R}[X]$ tels que

$$\cos((n+1)\theta) = 2\cos(\theta)T_n(\cos(\theta)) - T_{n-1}(\cos(\theta))$$

Posons $T_{n+1} = 2XT_n - T_{n-1}$. Alors $\cos((n+1)\theta) = T_{n+1}(\cos(\theta))$: H_{n+1} convient.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$. D'où l'existence.

Unicité : Soit $n \geq 0$. Si Q_n convient, alors pour tout $\theta \in \mathbb{R}$, $T_n(\cos(\theta)) = Q_n(\cos(\theta))$ si bien que T_n et Q_n coïncident en tout réel de la forme $\cos(\theta)$ donc sur $[-1; 1]$ qui est infini. Or, deux polynômes qui coïncident en une infinité de points sont égaux. D'où l'unicité.

Remarque : Les T_n sont appelés polynômes de Tchebychev. Ci-dessous les graphes de T_1 , T_2 , T_3 , T_4 , T_7 et T_{10} .

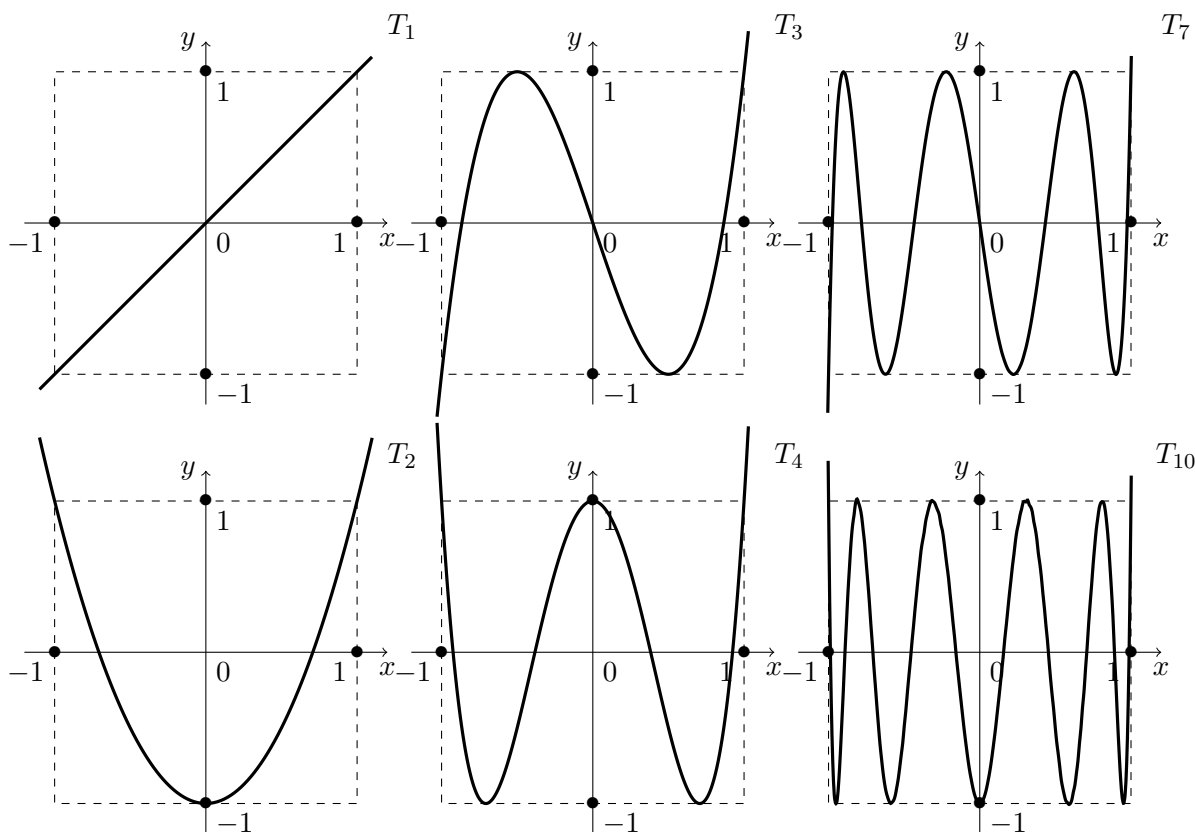
Cela signifie que toutes les dérivées de g sont nulles en 0 : géométriquement parlant, cela signifie que g est « super plate » en 0, c'est-à-dire qu'elle tend très vite vers 0 en 0. Attention cependant, malgré cela et le graphe ci-contre, cela ne signifie pas que g soit nulle sur un voisinage de 0 ! En effet, g n'est nulle qu'en 0 ! Cependant, elle tend tellement vite vers 0 qu'on a l'impression qu'elle est nulle sur un voisinage de 0 (mais ce n'est qu'une impression).

On a vu dans le chapitre 7 que $\cos(nx)$ est polynomial en $\cos(x)$ et on a même une expression explicite, mais cette expression est très peu maniable, ne serait-ce que pour donner le degré et le coefficient dominant.

Ainsi,

$$\begin{aligned} T_4 &= 2XT_3 - T_2 \\ &= 8X^4 - 8X^2 + 1 \end{aligned}$$

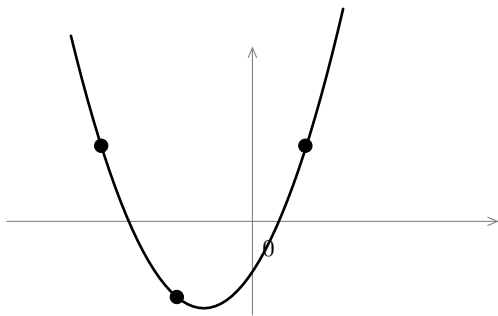
En d'autres termes, pour tout $\theta \in \mathbb{R}$, $\cos(4\theta) = 8\cos^4(\theta) - 8\cos^2(\theta) + 1$.



IX Un dernier pour la route : les polynômes d'interpolation de Lagrange

On s'intéresse au problème suivant : on fixe un entier $n \geq 1$, on dispose de a_1, \dots, a_n des éléments DISTINCTS de \mathbb{K} , de b_1, \dots, b_n des éléments de \mathbb{K} (pas forcément distincts), et on cherche un polynôme $P \in \mathbb{K}[X]$ tel que pour tout $k \in \llbracket 1; n \rrbracket$, $P(a_k) = b_k$.

Interprétation géométrique : on cherche un polynôme P tel que la courbe de la fonction polynomiale associée à P passe par les points (d'abscisses distinctes mais pas forcément d'ordonnées distinctes) de coordonnées $(a_1, b_1), \dots, (a_n, b_n)$.



- Première étape : soit $k \in \llbracket 1; n \rrbracket$. Trouver un polynôme L_k tel que $L_k(a_k) \neq 0$ et $L_k(a_i) = 0$ si $i \neq k$.

$L_k = (X - a_1)(X - a_2) \cdots (X - a_{k-1})(X - a_{k+1}) \cdots (X - a_n)$ convient. Sous forme condensée : $L_k = \prod_{i \neq k} (X - a_i)$.

- Deuxième étape : soit $k \in \llbracket 1; n \rrbracket$. Trouver un polynôme Λ_k tel que $\Lambda_k(a_k) = 1$ et $\Lambda_k(a_i) = 0$ si $i \neq k$.

Il suffit de prendre $\Lambda_k = L_k / L_k(a_k)$, c'est-à-dire :

$$\Lambda_k = \frac{(X - a_1)(X - a_2) \cdots (X - a_{k-1})(X - a_{k+1}) \cdots (X - a_n)}{(a_k - a_1)(a_k - a_2) \cdots (a_k - a_{k-1})(a_k - a_{k+1}) \cdots (a_k - a_n)}$$

convient. Sous forme condensée :

$$\Lambda_k = \prod_{i \neq k} \frac{(X - a_i)}{(a_k - a_i)}$$

D'où la nécessité de prendre les abscisses distinctes.

- Troisième étape : soit $k \in \llbracket 1; n \rrbracket$. Trouver un polynôme P_k tel que $P_k(a_k) = b_k$ et $P_k(a_i) = 0$ si $i \neq k$.

Il suffit de prendre $P_k = b_k \times \Lambda_k$ c'est-à-dire :

$$P_k = b_k \times \prod_{i \neq k} \frac{(X - a_i)}{(a_k - a_i)} = b_k \times \frac{(X - a_1)(X - a_2) \cdots (X - a_{k-1})(X - a_{k+1}) \cdots (X - a_n)}{(a_k - a_1)(a_k - a_2) \cdots (a_k - a_{k-1})(a_k - a_{k+1}) \cdots (a_k - a_n)}$$

- Quatrième étape : conclure.

$P = \sum_{k=1}^n P_k$ convient. En effet, pour tout $i \in \llbracket 1; n \rrbracket$,

$$\begin{aligned} P(a_i) &= \underbrace{P_i(a_i)}_{=b_i} + \sum_{k \neq i} \underbrace{P_k(a_i)}_{=0} \\ &= b_i \end{aligned}$$

De façon explicite :

$$P_k = \sum_{k=1}^n b_k \times \prod_{i \neq k} \frac{(X - a_i)}{(a_k - a_i)}$$

Exemple : Trouver $P \in \mathbb{R}[X]$ tel que $P(1) = -5$, $P(2) = 1$ et $P(3) = -2$.

$$P = -5 \times \frac{(X - 2)(X - 3)}{(1 - 2)(1 - 3)} + 1 \times \frac{(X - 1)(X - 3)}{(2 - 1)(2 - 3)} - 2 \times \frac{(X - 1)(X - 2)}{(3 - 1)(3 - 2)} \text{ convient.}$$

Théorème. Avec les notations précédentes, P est l'unique polynôme à coefficients dans \mathbb{K} de degré inférieur ou égal à $n - 1$ tel que $P(a_k) = b_k$ pour tout $k \in \llbracket 1; n \rrbracket$. P est appelé le polynôme d'interpolation de Lagrange passant par les points $(a_1, b_1), \dots, (a_n, b_n)$.

DÉMONSTRATION.

- Tout d'abord, P envoie bien les a_k sur les b_k et est bien à coefficients dans \mathbb{K} car ses coefficients sont obtenus en effectuant des produits, des sommes et des quotients d'éléments de \mathbb{K} . De plus, P est combinaison linéaire de polynômes de degré inférieur ou égal à $n - 1$ donc est de degré inférieur ou égal à $n - 1$. D'où l'existence.
- Soit $Q \in \mathbb{K}_{n-1}[X]$ un polynôme qui convient. Alors P et Q coïncident en au moins n points distincts (les a_k) mais sont de degré inférieur ou égal à $n - 1$ donc sont égaux : d'où l'unicité.

Remarque : Si $n = 2$, on retrouve le résultat connu : par deux points d'abscisses distinctes passe une unique droite non verticale donc le graphe d'une unique fonction affine. Pour $n = 3$, on vient de prouver qu'il existe une unique fonction polynomiale de degré inférieur ou égal à 2 (pas forcément égal !) dont le graphe passe par ces trois points.

Que se passe-t-il si on n'impose plus la condition sur le degré ? Alors il n'y a plus unicité, mais on peut donner la forme générale des polynômes solutions.

Le degré n'est pas forcément égal à $n - 1$! Par exemple, si tous les points ont la même ordonnée, alors P est constant donc de degré inférieur ou égal à 0.

Nous prouverons l'existence et l'unicité dans le chapitre 30 avec des arguments d'algèbre linéaire. La méthode du chapitre 30 pourra sembler plus simple, mais elle aura le gros défaut de ne pas être constructive !

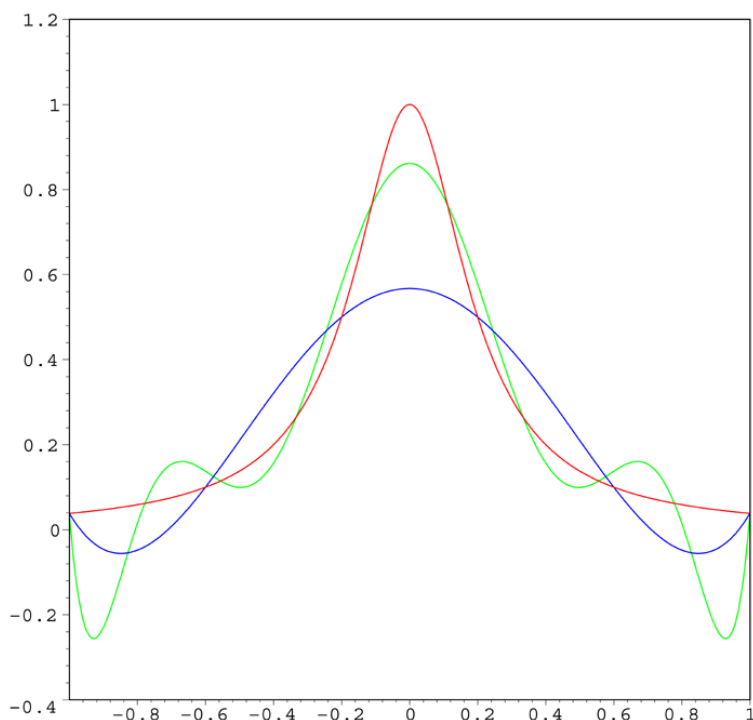
Proposition. Avec les mêmes notations que ci-dessus, un polynôme Q vérifie $Q(a_1) = b_1, \dots, Q(a_n) = b_n$ si et seulement P est le reste de la division euclidienne de Q par $(X - a_1) \dots (X - a_n)$, si et seulement s'il existe $A \in \mathbb{K}[X]$ tel que

$$Q = A \times (X - a_1) \cdots (X - a_n) + P$$

Nous dirons au chapitre 36 que l'ensemble des solutions est un espace affine.

DÉMONSTRATION. Un polynôme de cette forme est évidemment solution. Réciproquement, si Q convient, alors a_1, \dots, a_n sont des racines distinctes de $Q - P$ (car, pour tout i , $Q(a_i) = P(a_i) = b_i$) donc $Q - P$ est divisible par $(X - a_1) \cdots (X - a_n)$ ce qui permet de conclure.

Remarque : On peut également se poser une question suivante : si on a une fonction inconnue f dont on connaît certaines valeurs, le polynôme d'interpolation de Lagrange passant par ces points est-il une « bonne » approximation de f ? Plus vague, tu meurs... Tout dépend déjà de ce qu'on entend par « bonne approximation ». Disons juste ceci : ce n'est pas parce qu'on augmente le nombre de points qu'on a une meilleure approximation, comme on le voit sur l'exemple ci-dessous (merci Wikipédia) : la courbe bleue (qui oscille peu) est la fonction, la courbe rouge (avec le pic le plus haut) est le polynôme de Lagrange obtenu avec 5 points et la fonction verte (qui oscille beaucoup) est le polynôme de Lagrange obtenu avec 9 points.



Si on augmente le nombre de points, d'accord, le polynôme de Lagrange coïncide avec la fonction en plus de points, mais entre deux points successifs, le polynôme est incontrôlable et peut osciller très fortement, et même s'éloigner de plus en plus de la fonction ! Ce phénomène est appelé phénomène de Runge. On peut parfois l'éviter en choisissant les points d'une façon précise (il y a un rapport avec les polynômes de Tchebychev d'ailleurs), mais là, on commence à aller trop loin dans un domaine (parfois) intéressant appelé l'analyse numérique...