Chapitre 21

Polynômes

Mais tous les résultats de ce chapitre (sauf quelques uns et, alors, nous le mentionnerons explicitement) sont valables pour un corps $\mathbb{K}$ quelconque.

Dans ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

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

1) Construction de $\mathbb{K}[X]$

a) Retour sur les fonctions polynomiales

Plusieurs fois cette année, nous avons rencontré les fonctions polynomiales. On dit qu'une fonction f de $\mathbb{K}$ dans $\mathbb{K}$ est polynomiale s'il existe $n \in \mathbb{N}$ et $a_0, \dots, a_n$ des éléments de $\mathbb{K}$ (pas forcément non nuls, ni même tous non nuls) tels que

$$\forall x \in \mathbb{K}, \qquad f(x) = \sum_{k=0}^{n} a_k x^k.$$

On peut ajouter autant de terme nul que l'on veut à cette somme. La notion de degré (lorsque f n'est pas la fonction polynomiale nulle) permet de présenter une somme avec un nombre optimal de terme. Nous en reparlerons plus tard.

En général, pour connaître une fonction de $\mathbb{K}^{\mathbb{K}}$, il faut connaître la valeur qu'elle prend en chaque élément de $\mathbb{K}$. Dans le cas des fonctions polynomiales, il suffit de connaître ses coefficients, c'est-à-dire un nombre fini d'informations. Soyons précis :

- Les coefficients d'une fonction polynomiale sont uniques. Montrons-le en deux temps.
  - ⋆ Pour tout $n \in \mathbb{N}$, posons

    $H(n)$: « Pour tout $(c_0, \dots, c_n) \in \mathbb{K}^{n+1}$, si $\sum_{k=0}^{n} c_k x^k = 0$ pour tout $x \in \mathbb{C}$, alors $c_0 = \dots = c_n = 0$ » .

    Il est immédiat que $H(0)$ est vrai. Soit $n \in \mathbb{N}$. Supposons que $H(n)$ est vraie. Donnons-nous $c_0, \dots, c_{n+1}$ dans $\mathbb{K}$ tels que $f : x \longmapsto \sum_{k=0}^{n} c_k x^k = 0$ est la fonction nulle. Alors, pour tout $x \in \mathbb{K}$

    $$0 = 2^{n+1} f(x) - f(2x) = \sum_{k=0}^{n} (2^{n+1} - 2^k) c_k x^k.$$

    Cette différence est faite pour faire disparaître le terme en x^{n+1}.

    Par hypothèse de récurrence, pour tout $k \in [\![0\,;n]\!]$, $(2^{n+1} - 2^k)c_k = 0$ et donc $c_k = 0$. Il s'ensuit que $f : x \longmapsto c_{n+1} x^{n+1}$. Puisque $0 = f(1) = c_{n+1}$, on conclut que $H(n+1)$ est vraie. Ainsi, par récurrence, pour tout $n \in \mathbb{N}$, $H(n)$ est vraie. On vient de montrer que les coefficients de la fonction polynomiale nulle sont uniques : ils sont tous nuls.
  - ⋆ On se donne $\lambda \in \mathbb{K}$, $n \in \mathbb{N}$, $p \in \mathbb{N}$, $(a_0, \dots, a_n) \in \mathbb{K}^n$ et $(b_0, \dots, b_p) \in \mathbb{K}^p$ tels que

    $$\forall x \in \mathbb{K}, \qquad \sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{p} b_k x^k.$$

    Quitte à poser $b_{p+1} = \dots = b_n = 0$ si $p < n$ ou $a_{n+1} = \dots = a_p = 0$ si $n < p$, supposons que $n = p$. Alors

    $$\forall x \in \mathbb{K}, \qquad \sum_{k=0}^{n} (a_k - b_k) x^k = 0.$$

    Par unicité des coefficients de la fonction nulle, pour tout $k \in [\![0\,;n]\!]$, $a_k = b_k$.

même si, dans leur écriture en terme de somme, l'une peut avoir plus de termes que l'autre mais alors les termes en plus sont nuls

Ainsi, lorsque deux fonctions polynomiales sont égales, leurs coefficients sont égaux deux à deux.

- Soient $p \in \mathbb{N}$ et $q \in \mathbb{N}$. Soient $(a_0, \dots, a_p) \in \mathbb{K}^p$ et $(b_0, \dots, b_q) \in \mathbb{K}^q$. Considérons
$$f : x \longmapsto \sum_{k=0}^{p} a_k x^k \qquad \text{et} \qquad g : x \longmapsto \sum_{k=0}^{q} b_k x^k.$$
Quitte à ajouter des termes nuls, supposons que $p = q = n$. Alors :
  - ⋆ Pour tout $x \in \mathbb{K}$, $(f+g)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$.
  - ⋆ Pour tout $x \in \mathbb{K}$, $(\lambda f)(x) = \sum_{k=0}^{n} (\lambda a_k) x^k$.
  - ⋆ Pour tout $x \in \mathbb{K}$,
$$\begin{aligned} f(x)g(x) &= (a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n)(b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 \\ &\qquad + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0) x^3 + \cdots + b_n a_n x^{2n} \end{aligned}$$
Plus précisément :
$$f(x)g(x) = \left(\sum_{k=0}^{n} a_k x^k \right) \left(\sum_{k=0}^{n} b_k x^k \right) = \sum_{k=0}^{n} \sum_{\ell=0}^{\ell} a_k b_\ell x^{k+\ell}.$$
Pour tout $k \in [\![0\,;n]\!]$, faisons le changement d'indice $j = k + \ell$ dans la somme intérieure. Alors :
$$f(x)g(x) = \sum_{k=0}^{n} \sum_{j=k}^{k+n} a_k b_{j-k} x^j = \sum_{k=0}^{n} \sum_{j=0}^{2n} a_k b_{j-k} x^j,$$
en posant $a_{n+1} = \cdots = a_{2n} = b_{n+1} = \cdots = b_{2n} = 0$. Par théorème de Fubini,
$$f(x)g(x) = \sum_{j=0}^{2n} \Bigg(\underbrace{\sum_{k=0}^{n} a_k b_{j-k}}_{=c_j} \Bigg) x^i.$$
  - ⋆ Quand $\mathbb{K} = \mathbb{R}$, f est dérivable sur $\mathbb{R}$ et, pour tout $x \in \mathbb{R}$, $f'(x) = \sum_{k=0}^{n-1} a_{k+1} x^k$.

  On constate donc que $f+g$, λf, fg et f' sont encore des fonctions polynomiales. Par ailleurs la connaissance des coefficients de f et g déterminent entièrement leurs coefficients .

Par récurrence immédiate, pour tout $k \in \mathbb{N}$, f^k est encore une fonction polynomiale et donc
$$g \circ f = \sum_{k=0}^{q} b_k f^k$$
aussi.

Ainsi, dans les fonctions polynomiales, seuls les coefficients importent et ils permettent seuls de faire toutes les opérations usuelles. Cela motive l'introduction d'un objet plus général que l'on va appeler polynôme, qui va être défini par les coefficients uniquement et qui ne sera pas une fonction. Pourquoi faire cela ? Et bien parce qu'ils seront beaucoup plus maniables que des fonctions qui ont le défaut d'exiger un domaine de définition, l'introduction de variable quand on fait des calculs avec elles, etc.

b) Suites presque nulles et définition d'un polynôme

L'entier n_0 dépend de la suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$.

Définition (suite presque nulle). *On dit qu'une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est presque nulle si ses termes sont nuls à partir d'un certain rang, c'est-à-dire s'il existe $n_0 \in \mathbb{N}$ telle que, pour tout $n \geqslant n_0$, $a_n = 0$.*

Remarque : On note souvent $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ une suite presque nulle. Cette notation sous-entend que les termes sont nuls au moins à partir du rang $n+1$ (mais ne dit pas non plus que $a_n \neq 0$).

Définition (polynôme). *On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}}$ presque nulle d'éléments dans $\mathbb{K}$. Pour tout $n \in \mathbb{N}$, on dit que a_n est le coefficient d'indice n ou d'ordre n. Le coefficient a_0 est appelé le coefficient constant.*

⚠ Vous aviez bien lu : un polynôme est une suite (qui est presque nulle) et donc ce n'est pas une fonction !

On expliquera plus tard ce que X veut dire.

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

Remarque : Puisque $\mathbb{R} \subset \mathbb{C}$, on a $\mathbb{R}[X] \subset \mathbb{C}[X]$.

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

Démonstration. Découle du fait que, deux suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ (presque nulles ou non) sont égales si et seulement si, pour tout $n \in \mathbb{N}$, $a_n = b_n$. □

Définition (polynôme constant). *Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$. On dit que P est constant si, pour tout $n \in \mathbb{N}^*$, $a_n = 0$. En d'autres termes, P est constant s'il existe $\lambda \in \mathbb{K}$ tel que $P = (\lambda, 0, 0, \dots)$.*

Dans le cas où $\lambda = 0$, c'est-à-dire P est la suite nulle, on dit que P est le polynôme nul.

Remarque : Soit $\lambda \in \mathbb{K}$. Le polynôme constant $P = (\lambda, 0, 0, \dots)$ est parfois noté $P = \widetilde{\lambda}$ pour bien insister sur le fait que P n'est pas un élément de $\mathbb{K}$ mais un polynôme (une suite presque nulle). Mais, par abus de notation et soucis de simplicité, on note tout de même $P = \lambda$ la plupart du temps.

c) Opération sur les polynômes

Cela veut dire que $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont des suites presque nulles.

Définition. *On définit sur $\mathbb{K}[X]$ deux lois de composition internes $+$ et $\times$ définies par : pour tout $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}[X]$,*

- $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$
- $P \times Q = (c_n)_{n\in\mathbb{N}}$ *où, pour tout $n \in \mathbb{N}$,*

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

On définit une loi externe sur $\mathbb{K}[X]$ par : pour tout $\lambda \in \mathbb{K}$ et $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

On définira la composition de polynômes et la dérivation formelle des polynômes dans les paragraphes I.4 et I.5 respectivement.

Remarque : Les lois $+$ et $\times$ sont bien des lois de composition internes. En effet il existe $p \in \mathbb{N}$ tel que, pour tout $n > p$, $a_n = 0$ et il existe $q \in N$ tel que, pour tout $n > q$, $b_n = 0$. Par conséquent :

- pour tout $n > \max\{p; q\}$, $a_n + b_n = 0$. Ainsi $P + Q \in \mathbb{K}[X]$.
- pour tout $n > p + q$,
  - ⋆ si $k \in [\![0\,; p]\!]$, $n - k > n - p > q$ donc $b_{n-k} = 0$
  - ⋆ si $k \in [\![p + 1\,; n]\!]$, $a_k = 0$

  si bien que

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{p} a_k \underbrace{b_{n-k}}_{=0} + \sum_{k=p+1}^{n} \underbrace{a_k}_{=0} b_{n-k} = 0$$

  donc $PQ \in \mathbb{K}[X]$.

Enfin, pour tout $n > p$, $\lambda a_n = 0$. Ainsi $\lambda P \in \mathbb{K}[X]$.

Mais ce n'est pas une LCI puisque l'on multiplie P par un élément de $\mathbb{K}$.

Théorème. *$(\mathbb{K}[X],+,\times)$ est un anneau commutatif dont l'élément neutre pour $+$ est le polynôme constant égal à 0 et dont l'élément neutre pour $\times$ est le polynôme constant égal à 1.*

Démonstration.

- Commençons par montrer que $(\mathbb{K}[X],+)$ est un sous-groupe de $(\mathbb{K}^{\mathbb{N}},+)$.
  - ⋆ Déjà $\mathbb{K}[X]$ contient la suite nulle donc n'est pas vide.
  - ⋆ Soit $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$ deux polynômes. Il existe $p\in\mathbb{N}$ tel que $a_n=0$ pour tout $n\geqslant p$ et il existe $q\in\mathbb{N}$ tel que $b_n=0$ pour tout $n\geqslant q$. Alors $P-Q=(a_n-b_n)_{n\in\mathbb{N}}\in\mathbb{K}[X]$ puisque $a_n-b_n=0$ pour tout $n\geqslant\max\{p;q\}$.

  On en déduit que $(\mathbb{K}[X],+)$ est un groupe abélien. Son élément neutre est celui de $(\mathbb{K}^{\mathbb{N}},+)$ qui est la suite nulle.
- Montrons que $\times$ est associative sur $\mathbb{K}[X]$.
- Montrons que $\times$ est commutative sur $\mathbb{K}[X]$. Soient $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}[X]$. Pour tout $n\in\mathbb{N}$,
$$(PQ)_n=\sum_{k=0}^{n}a_kb_{n-k}=\sum_{j=0}^{n}b_ja_{n-j}=(QP)_n,$$
via le changement d'indice $j=n-k$. Ainsi $PQ=QP$.
- Soit $P=(a_n)_{n\in\mathbb{N}}\in\mathbb{K}[X]$. Notons $\widetilde{1}$ le polynôme constant égale à 1. Il s'agit de $(1,0,0,\dots)$. Ainsi, pour tout $n\in\mathbb{N}$,
$$(\widetilde{1}P)_n=\sum_{k=0}^{n}(\widetilde{1})_ka_{n-k}=1a_n+0+\cdots+0=a_n.$$
Ainsi $\widetilde{1}P=P$. Par commutativité, $P\widetilde{1}=P$. Ainsi $\widetilde{1}$ est l'élément neutre pour $\times$.
- Il reste à montrer que $\times$ est distributive sur $+$. Soient $P=(a_n)_{n\in\mathbb{N}}$, $Q=(b_n)_{n\in\mathbb{N}}$ et $R=(r_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}[X]$. Pour tout $n\in\mathbb{N}$,
$$(P(Q+R))_n=\sum_{k=0}^{n}a_k(Q+R)_{n-k}=\sum_{k=0}^{n}a_k(b_{n-k}+r_{n-k})=\sum_{k=0}^{n}a_kb_{n-k}+\sum_{k=0}^{n}a_kr_{n-k}$$
et donc $(P(Q+R))_n=(PQ)_n+(PR)_n=(PQ+PR)_n$. Ainsi $P(Q+R)=PQ+PR$. Par commutativité, $\times$ est donc distributive sur $+$

Il s'ensuit que $(\mathbb{K}[X],+,\times)$ est un anneau commutatif. □

On montrera plus tard qu'il est intègre et que seuls les polynômes constants non nuls sont inversibles pour $\times$.

La loi $\times$ sur $\mathbb{K}[X]$ n'est pas la loi multiplicative de $\mathbb{K}^{\mathbb{N}}$ donc $\mathbb{K}[X]$ n'est pas un sous-anneau de $\mathbb{K}^{\mathbb{N}}$: il faut tout redémontrer).

Remarques :

- Le fait que $\mathbb{K}[X]$ soit un anneau permet de définir $P^n = \underbrace{P \times \cdots \times P}_{n \text{ fois}}$ avec toutes les propriétés qui vont avec vues dans le chapitre 17. On pose $P^0 = (1, 0, 0, \dots)$ le polynôme constant égal à 1.
- Si $P = (a_n)_{n\in\mathbb{N}}$ et $\lambda \in \mathbb{K}$ alors, en notant Q le polynôme constant égal à λ, on a $QP = \lambda P$. En effet, pour tout $n \in \mathbb{N}$,

$$(QP)_n = \sum_{k=0}^{n} Q_k P_{n-k} = \lambda a_n + 0 + \cdots + 0.$$

On en déduit alors les propriétés suivantes de la multiplication externe :

Proposition. *Soient $(\lambda, \mu) \in \mathbb{K}^2$. Soient P et Q dans $\mathbb{K}[X]$. On a :*

- $(\lambda + \mu)P = \lambda P + \mu Q$,
- $\lambda(P + Q) = \lambda P + \lambda Q$,
- $\lambda(\mu P) = (\lambda\mu)P$,
- $(\lambda P)Q = P(\lambda Q) = \lambda(PQ)$.

⇝ Démonstration laissée en exercice.

Par récurrence, on a également :

Corollaire. *Soit $k \in \mathbb{N}^*$. Soient $P_1, \dots, P_k$ dans $\mathbb{K}[X]$. Soient $\lambda_1, \dots, \lambda_k$ dans $\mathbb{K}$. Alors* $\sum_{j=0}^{k} \lambda_j P_j \in \mathbb{K}[X]$.

d) Notation polynomiale

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

Remarques :

- ⚠ Et donc X n'est pas une variable (au sens un objet donc on peut donner des valeurs) ni un élément de $\mathbb{K}$. C'est un polynôme (c'est-à-dire une suite presque nulle) **bien précis** auquel on a choisi de donner un nom particulier, dont le but est évidemment l'analogie avec les fonctions polynomiales. Insistons bien :
  - ⋆ X n'est pas un nombre !
  - ⋆ X ne soit jamais être un introduit. On ne peut pas écrire des phrases du genre « $\forall X \in \mathbb{K}$ » ou « $\forall X \in \mathbb{K}[X]$ ».
  - ⋆ Cela n'a aucun sens que d'écrire, par exemple, $X = 0$ ou $X = 1$, etc.
- On dit que X est l'indéterminée. On l'utilise (on va le voir) pour représenter les polynômes autrement que par des suites et les rapprocher des fonctions polynomiales. On pourrait l'appeler autrement et parfois on le fait (c'est-à-dire qu'on pourrait appeler l'indéterminée Y , T etc.) surtout quand on a des polynômes à plusieurs indéterminées. Mais là on sort totalement du cadre du programme.

Lemme. *Soit $P = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in \mathbb{K}[X]$. Alors*

$$XP = (0, a_0, a_1, \dots, a_n, 0, 0, \dots).$$

On n'écrit jamais P^n avec $n \in \mathbb{Z}\backslash\mathbb{N}$. puisqu'un polynôme non nul non constant n'est jamais inversible.

Par commutativité du produit, on a aussi $PQ = \lambda P$.

Les trois premiers points, le fait que $1P = P$ et le fait que $(\mathbb{K}[X], +)$ est un groupe abélien, permettront d'affirmer que $\mathbb{K}[X]$ est un espace vectoriel dans le chapitre 28.

Autrement dit, une combinaison linéaire de polynômes est un polynôme.

Autrement dit $X = (a_n)_{n\in\mathbb{N}}$ avec $a_0 = 0$, $a_1 = 1$ et, pour tout $n \geqslant 2$, $a_n = 0$.

On décale tout d'un rang et on met un 0 devant.

Démonstration.

□

Comme $X^0 = (1, 0, 0, \dots, 0)$, on obtient par récurrence que :

Proposition. *Pour tout $n \in \mathbb{N}$, $X^n = (\underset{0}{0}, \underset{1}{0}, \dots, 0, \underset{n}{1}, 0, 0, \dots)$*

Autrement dit $X^n = (a_k)_{k\in\mathbb{N}}$ avec $a_n = 1$ et, pour tout $k \in \mathbb{N}\backslash\{n\}$, $a_k = 0$.

Ainsi, lorsque $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, en notant p un entier naturel tel que, pour tout $n > p$, $a_n = 0$. On a

$$\begin{aligned} P &= (a_0, a_1, a_2, \dots, a_p, 0, 0, \dots) \\ &= a_0(1, 0, 0, \dots, 0, 0, 0, \dots) + a_1(0, 1, 0, \dots, 0, 0, 0, \dots) + a_2(0, 0, 1, \dots, 0, 0, 0, \dots) \\ &\qquad + \dots + a_p(0, 0, 0, \dots, 1, 0, 0, \dots) \\ &= a_0X^0 + a_1X + a_2X^2 + \dots + a_pX^p. \end{aligned}$$

On en déduit :

Bon je fais une petite confidence : la construction de $\mathbb{K}[X]$ est en fait hors-programme mais j'avoue que je n'ai pas trouvé comment vous présenter cet ensemble autrement. Finalement, tout ce qu'il faut retenir est que :
• $\mathbb{K}[X]$ est un ensemble qui contient des éléments qui s'écrivent sous la forme

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

les a_k étant uniquement déterminés et nuls à partir d'un certain rang. Ces objets ne sont pas des fonctions !
• X est un objet précis qui n'est pas un nombre.
• Les opérations sur les éléments de $\mathbb{K}[X]$ obéissent aux règles ci-contre et $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Proposition/Définition. *Si $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, alors*

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

cette somme ayant un sens puisqu'elle est faussement infinie (la suite étant presque nulle). Le terme a_0X^0 se note simplement a_0.

Exemples :

- *Le polynôme $(2, -1, 3, 1, 0, 0, \dots)$ se note $X^3 + 3X^2 - X + 2$.*
- *Le polynôme $(0, 0, 2, -1, 7, 0, 0 \dots)$ se note $7X^4 - X^3 + 2X^2$.*

Cette notation permet de travailler avec les trois opérations de façon plus intuitive, comme dans $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$: soient $\lambda \in \mathbb{K}$ et $P = (a_n)_{n\in\mathbb{N}}$ 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 :
- Par définition, $\lambda P = (\lambda \times a_n)_{n\in\mathbb{N}}$. Avec l'écriture ci-dessus, cela se traduit de la façon suivante :
- Par définition, $PQ = (c_n)_{n\in\mathbb{N}}$ avec, pour tout $n \in \mathbb{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Avec l'écriture ci-dessus, cela se traduit de la façon suivante :

Remarque : La plupart du temps, cette somme étant finie, nous écrirons : « soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ » ce qui signifiera : « soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et soit n tel que, pour tout $k \geqslant n+1$, $a_k = 0$ ». Les relations précédentes deviennent alors : pour tous $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$ et $Q = \sum_{k=0}^{q} b_k X^k \in \mathbb{K}[X]$

Cela ne signifie pas que $a_n \neq 0$ (il faudra attendre pour cela la notion de degré). Il ne faut pas non plus 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

On a vu dans la paragraphe I.1.c que $c_k = 0$ dès que $k > p+q$.

Le fait que $\mathbb{K}[X]$ soit intègre (comme on le verra dans un instant), alors que $\mathbb{K}^{\mathbb{K}}$ ne l'est pas, va aussi être un gros avantage.

Disons finalement que la structure d'anneau commutatif de $\mathbb{K}[X]$ permet de faire les calculs sur les éléments de $\mathbb{K}[X]$, comme si on était sur $\mathbb{K}$ ou sur $\mathbb{K}^{\mathbb{K}}$. On a une définition formelle et plus maniable mais, finalement, il y a rien de nouveau dans la pratique des opérations sur les polynômes par rapport à la pratique des opérations sur les fonctions polynomiales.

Définition (monôme). *On dit qu'un polynôme P est un monôme s'il existe $\lambda \in \mathbb{K}^*$ et $n \in \mathbb{N}$ tel que $P = \lambda X^n$.*

2) Degré d'un polynôme

a) Notion de degré

Définition. *Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{R}[X]$.*

- *Si P n'est pas le polynôme nul, alors l'entier naturel $\max\{k \in [\![0\,;n]\!] \,|\, a_k \neq 0\}$ est appelé degré de P, et noté $\deg(P)$.*
  Si $p = \deg(P)$, alors a_p est appelé le coefficient dominant de P.
  Si $a_p = 1$, alors on dit que P est unitaire.
- *Si P est le polynôme nul, alors on adopte la convention $\deg(0) = -\infty$*

Ainsi $\deg(P)$ est le plus grand indice des coefficients non nuls. Il existe car c'est le maximum d'une partie de $\mathbb{N}$ qui est majoré (car $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle) et non vide car P n'est pas le polynôme nul donc il admet au moins un coefficient non nul.

Remarques :

- La convention que le polynôme nul vaut $-\infty$ trouvera son intérêt dans le prochain paragraphe.
- Si $P \in \mathbb{R}[X]$ n'est pas le polynôme nul et si $p = \deg(P)$, alors P s'écrit de manière **unique** sous la forme $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$.

  Lorsque l'on écrit $P = \sum_{k=0}^{n} a_k X^k$, on ne peut pas conclure que P est degré n. Il faut, pour cela, impérativement préciser que $a_n \neq 0$. Sans cette information, tout ce que l'on peut conclure est que $\deg(P) \leqslant n$ (cf. paragraphe I.2.d).

- On a :
  - ⋆ $\deg(P) \in \mathbb{N}$ si et seulement si P n'est pas le polynôme nul.
  - ⋆ $\deg(P) \in \mathbb{N}^*$ si et seulement si P n'est pas constant

Le polynôme nul est le seul polynôme de degré strictement négatif. Ainsi, si au cours d'une démonstration, on tombe sur $\deg(P) < 0$, on peut tout de suite conclure que $P = 0$.

Exemples :

- $P = 2X + 3$ *est de degré* 1 *et son coefficient dominant est* 2.
- X^7 *est de degré* 7 *et unitaire.*
- $P = -3X^5 + X^2 + 9X$ *est de degré* 5 *et son coefficient dominant est* -3.
- $P = 7$ *est de degré* 0 *et son coefficient dominant est* 7.

b) Degré d'une somme et d'un produit

On fait comme dans le chapitre 14 quand on a créé $\overline{\mathbb{R}}$, 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 adjoint à* $\mathbb{N}$ *un élément noté* $-\infty$ *qui n'appartient pas à* $\mathbb{N}$. *On prolonge la relation d'ordre* $\leqslant$ *sur* $\mathbb{N} \cup \{-\infty\}$ *en posant :*

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

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

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

Contrairement au chapitre 14 avec $\overline{\mathbb{R}}$, le fait qu'il n'y ait pas $+\infty$ simplifie beaucoup les choses, et en particulier évite les formes indéterminées.

Proposition (degré d'une somme). *Soient* P *et* Q *dans* $\mathbb{K}[X]$. *Alors*

$$\deg(P+Q) \leqslant \max\{\deg(P); \deg(Q)\}$$

Plus précisément, si P *et* Q *sont non nuls, il y a égalité si et seulement si* $\deg(Q) \neq \deg(Q)$ *ou bien* $\deg(P) = \deg(Q)$ *et les coefficients dominants de* P *et* Q *ne sont pas opposés.*

Remarque : On peut même être encore plus précis : supposons que P et Q sont non nuls. Notons $p = \deg(P)$, $q = \deg(Q)$, a_p le coefficient dominant de P et b_q le coefficient dominant de Q. Alors :

- Si $p > q$, $\deg(P+Q) = p$ et le coefficient dominant de $P+Q$ est a_p.
- Si $p < q$, $\deg(P+Q) = q$ et le coefficient dominant de $P+Q$ est b_q.
- Si $p = q$ et $a_p \neq -b_p$, alors $\deg(P+Q) = p$ et le coefficient dominant est $a_p + b_q$.
- Si $p = q$ et $a_p = -b_q$, alors $\deg(P+Q) < p$ et aucune formule générale ne donne le coefficient dominant de $P+Q$.

Si $a_p + b_p = 0$, alors

$$P + Q = \sum_{k=0}^{p-1} (a_k + b_k) X^k.$$

On ne sait pas si $a_{p-1} + b_{p-1} = 0$ donc on ne peut rien conclure précisément sur le degré si ce n'est qui est inférieur strictement à p.

Démonstration. Si $P = 0$, $\deg(P+Q) = \deg(Q) \leqslant \max\{-\infty; \deg(Q)\}$. Même chose si $Q = 0$. Si $P \neq 0$ et $Q \neq 0$, cela découle de la dernière remarque du paragraphe I.1.d avec l'ajout des hypothèses que $a_p \neq 0$ et $b_q \neq 0$. Dans le cas où $p = q$, et que $a_p \neq -b_q$, on a $a_p + b_p \neq 0$ donc $\deg(P+Q) = p = \max\{\deg(P); \deg(Q)\}$. □

Proposition. *Soit* $P \in \mathbb{K}[X]$. *Soit* $\lambda \in \mathbb{K}^*$. *Alors* $\deg(\lambda P) = \deg(P)$.

Remarques :

- Bien sûr, si $\lambda = 0$, $\lambda P = 0$ est de degré $-\infty$.
- Supposons que $\lambda \in \mathbb{K}^*$ et $P \neq 0$. Notons a_p le coefficient dominant de P. Alors le coefficient dominant de λP est λa_p.

Démonstration. Si $P = 0$, alors λP et P sont nuls donc ont même degré. Si $P \neq 0$, cela découle de la dernière remarque du paragraphe I.1.d avec l'ajout des hypothèses que $a_p \neq 0$. □

Proposition. *Soient P et Q dans $\mathbb{K}[X]$. Alors $\deg(PQ) = \deg(P) + \deg(Q)$.*

Remarque : Lorsque P et Q sont non nuls, le coefficient dominant de PQ est le produit des coefficients dominants de P et de Q.

Démonstration. Si $P = 0$ ou $Q = 0$, alors $PQ = 0$ donc $\deg(PQ) = -\infty$ et $\deg(P) + \deg(Q) = -\infty$. Supposons que $P \neq 0$ et $Q \neq 0$. Avec les notations de la dernière remarque du paragraphe I.1.d, on en était à

$$PQ = \sum_{k=0}^{p+q} c_k X^k.$$

Avec l'ajout que $a_p \neq 0$ et $a_q \neq 0$,

$$c_{p+q} = \sum_{j=0}^{p+q} a_j b_{p+q-j} = \sum_{j=0}^{p-1} a_j \underbrace{b_{p+q-j}}_{=0} + a_p b_q + \sum_{j=p+1}^{p+q} \underbrace{a_j}_{=0} b_{p+q-j} = a_p b_q \neq 0.$$

Ainsi PQ est de degré $p+q$ et de coefficient dominant $a_p b_q$. □

Par récurrence, nous obtenons :

Corollaire. *Soit $k \in \mathbb{N}^*$. Soient $P_1, \dots, P_k$ dans $\mathbb{K}[X]$. On a :*

$$\deg\left(\sum_{i=1}^{k} P_i\right) \leqslant \max_{1 \leqslant i \leqslant k} \left(\deg(P_i)\right) \qquad \text{et} \qquad \deg\left(\prod_{i=1}^{k} P_i\right) = \sum_{i=1}^{k} \deg(P_i).$$

Corollaire. *Pour tous $k \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$, $\deg(P^k) = k \times \deg(P)$.*

Avec la convention que

$$k \times (-\infty) = -\infty.$$

Si $P \neq 0$ et $k \in \mathbb{N}$, on a $P^k = \widetilde{1}$ et, comme $0 = 0 \times \deg(P)$, on a encore $\deg(P^k) = k \times \deg(P)$.

Remarque : Le coefficient d'un produit d'un nombre fini de polynômes non nuls est le produit des coefficients dominants. Et donc, si $P \neq 0$, le coefficient dominant de P^k est la puissance $k^{\text{ième}}$ de celui de P.

c) Intégrité et éléments inversibles

On a vu que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

On aurait bien eu du mal à montrer cela avec des fonctions polynomiales puisque $\mathbb{K}^{\mathbb{K}}$ n'est pas intègre : deux fonctions non nulles peuvent être de produit nul (cf. chapitre 17).

Proposition (intégrité). *$\mathbb{K}[X]$ est intègre, c'est-à-dire*

$$\forall (P, Q) \in \mathbb{K}[X]^2, \qquad PQ = 0 \implies P = 0 \text{ ou } Q = 0.$$

Démonstration.

□

On ne doit surtout pas dire que X doit être différent de -1 ! Encore une fois X n'est pas le réel -1 ni même le polynôme constant égale à -1. L'objet $X + 1$ n'est pas le polynôme nul, à point c'est tout.

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

Exemple : *Si on sait que Q et R sont des polynômes tels que $(X+1)P = (X+1)Q$, alors $P = Q$ (puisque $X + 1$ n'est pas le polynôme nul).*

Proposition (éléments inversible). *Les polynômes qui sont inversibles pour le produit sont exactement les polynômes constants non nuls.*

Démonstration.

□

Remarque : Et donc $\mathbb{K}[X]$ n'est pas un corps ! En revanche il est inclus dans le corps des fractions rationnelles, noté $\mathbb{K}(X)$ et étudié dans le prochain chapitre.

d) Ensembles $\mathbb{K}_n[X]$

Pour tout $n \in \mathbb{N}$, l'ensemble des polynômes de degré exactement n n'est stable ni par somme, ni par multiplication par un scalaire (en effet $X^n - X^n$ et $0.X^n$ ne sont pas de degré n). C'est pour cela que l'on introduit l'ensemble suivant :

Si $\deg(P) = n$, alors $P \in \mathbb{K}_n[X]$ mais la réciproque est fausse. Par exemple, $X^2 + 1 \in \mathbb{K}_3[X]$ mais est de degré 2.

Définition. *Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leqslant n\}$ l'ensemble des polynômes de degré au plus n.*

Remarques :

- $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants (y compris le polynôme de nul).
- Soit $n \in \mathbb{N}^*$. On a $P \in \mathbb{K}_n[X]$ si et seulement si il existe $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$ tels que
$$P = \sum_{k=0}^{n} a_k X^k.$$
⚠ Mais, pour pouvoir conclure que $\deg(P) = n$, il faut vérifier que $a_n \neq 0$.

Proposition. *Soit $n \in \mathbb{N}$. Pour tous P et Q dans $\mathbb{K}_n[X]$ et pour tout $\lambda \in \mathbb{K}$, $P + Q \in \mathbb{K}_n[X]$ et $\lambda P \in \mathbb{K}_n[X]$.*

Démonstration. Soient $P \in \mathbb{K}_n[X]$ et $Q \in \mathbb{K}_n[X]$. Alors $\deg(P) \leqslant n$ et $\deg(Q) \leqslant n$.

- On a $\deg(P+Q) \leqslant \max\{\deg(P); \deg(Q)\} \leqslant n$ (le maximum entre deux éléments de $\mathbb{N} \cup \{-\infty\}$ inférieur à n est encore inférieur à n). Ainsi $P + Q \in \mathbb{K}_n[X]$.
- Si $\lambda \in \mathbb{K}^*$, $\deg(\lambda P) = \deg(P) \leqslant n$. Si $\lambda = 0$, $\deg(\lambda P) = -\infty \leqslant n$. Ainsi, dans les deux cas, $\lambda P \in \mathbb{K}_n[X]$. □

Corollaire. *Soit $n \in \mathbb{N}$. Soient $k \in \mathbb{N}^*$ et $P_1, \dots, P_k$ dans $\mathbb{K}_n[X]$. Soient $\lambda_1, \dots, \lambda_k$ dans $\mathbb{K}$. Alors*
$$\sum_{j=1}^{k} \lambda_j P_j \in \mathbb{K}_n[X].$$

Remarques :

- Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est non vide et, pour tous P et Q dans $\mathbb{K}_n[X]$, $P + Q \in \mathbb{K}_n[X]$ et $-Q \in \mathbb{K}_n[X]$. Ainsi $(\mathbb{K}_n[X], +)$ est un sous-groupe de $(\mathbb{K}[X], +)$. Mais $\mathbb{K}_n[X]$ n'est pas un sous-anneau lorsque $n \geqslant 1$, puisqu'alors il n'est pas stable par produit.
- $\mathbb{K}_0[X]$ est un corps isomorphe à $\mathbb{K}$, via l'isomorphisme de corps
$$\left\{ \begin{array}{ccc} \mathbb{K}_0[X] & \longrightarrow & \mathbb{K} \\ (\lambda, 0, 0, \dots) & \longmapsto & \lambda \end{array} \right.$$

⇝ Démonstration laissée en exercice.

3) Fonction polynomiale associée à un polynôme

Bien sûr, on voit le lien très fort entre polynômes (surtout avec la notation sous forme de somme) et les fonctions polynomiales. Explorons ce lien plus en détail.

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

$$\widetilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \sum_{k=0}^{n} a_k x^k \end{array} \right.$$

Pour tout $x \in \mathbb{K}$, *on dit qu'on évalue le polynôme* P *en* x *lorsqu'on calcule* $\widetilde{P}(x)$. *Pour simplifier les notations, on désigne souvent cette évaluation plus simplement par* $P(x)$.

Quand on écrit cela, n est automatiquement introduit et c'est un entier naturel et $a_0, \dots, a_n$ sont aussi automatiquement introduits et ce sont des éléments de $\mathbb{K}$.

⚠ On ne sait pas que $a_n \neq 0$ donc $\deg(P) \leqslant n$ (mais pas forcément $= n$).

Remarques :

- ⚠ On écrit souvent $P(x)$ au lieu de $\widetilde{P}(x)$ mais attention à ne pas franchir le pas et à écrire que $P = \widetilde{P}$: un polynôme n'est pas une fonction !

⚠ On ne dira jamais, par exemple, « Posons $X = 1$ » (c'est une erreur très grave : encore une fois X est un objet précis, il ne vaudra jamais 1, ni même le polynôme constant égal à 1.) mais « Évaluons en 1 ».

- Pour tout $a \in \mathbb{K}$, l'application

$$\left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K} \\ P & \longmapsto & \widetilde{P}(a) \end{array} \right.$$

  est un morphisme d'anneaux (je vous laisse le vérifier) appelé évaluation en a. Il s'agit d'une surjection mais pas d'une injection puisque, pour tout $b \in \mathbb{K}$, les polynômes $P = X - a + b$ et $Q = (X-a)^2 + b$ sont distincts et $\widetilde{P}(a) = \widetilde{Q}(a) = b$.

Exemples :

- *Si* $P = 3X^3 - 2X + 5$, *on a* $\widetilde{P}(1) = 3 - 2 + 5 = 6$.
- *Si* $P = X^2 + 1$, *on a* $\widetilde{P}(\mathrm{i}) = \mathrm{i}^2 + 1 = 0$. *On dit que* i *est une racine de* P *(cf. paragraphe III).*

Algorithme de Hörner. Comment calculer l'évaluation d'un polynôme en un élément de $\mathbb{K}$ de façon optimale ? C'est-à-dire, si on se donne $x, a_0, \dots, a_n$, comment calculer le plus simplement $\widetilde{P}(x) = \sum_{k=0}^{n} a_k x^k$?

Typiquement, quelle est la complexité d'un algorithme de calcul de $\widetilde{P}(x)$?

- *Méthode naïve :* on calcule x^2 puis x^3, etc. et enfin x^n (évidemment sans recommencer tout le calcul à chaque fois : on multiplie par x une puissance pour obtenir la puissance suivante). Ensuite, on multiplie ces différentes puissances de x par $a_0, \dots, a_n$ respectivement et enfin on ajoute le tout. Cette méthode nécessite $n - 1 + n = 2n - 1$ multiplications et n additions.
- *Méthode de Hörner :* on remarque que

$$\widetilde{P}(x) = ((\dots(((a_n x + a_{n-1})x + a_{n-2})x + a_{n-3})x + \dots + a_2)x + a_1)x + a_0.$$

  Plus précisément :

  ⋆ on commence par calculer $a_n x + a_{n-1}$,

  ⋆ on multiplie cette quantité par x et on ajoute a_{n-2}, ce qui donne

$$a_n x^2 + a_{n-1}x + a_{n-2}.$$

  ⋆ on multiplie cette dernière quantité par x et on ajoute a_{n-3}, ce qui donne

$$a_n x^3 + a_{n-1}x^2 + a_{n-2}x + a_{n-3}.$$

  ⋆ etc.

⋆ lorsqu'on a obtenu $a_n x^{n-1} + a_{n-1}x^{n-2} + a_{n-2}x^{n-3} + \cdots + a_2 x + a_1$, on multiplie enfin par x et on ajoute a_0 pour obtenir $\widetilde{P}(x)$.

Par exemple, évaluons en $x = 2$ le polynôme $P = 3X^4 - X^3 - 4X^2 + 5X - 6$. Avec la méthode de Hörner :

Cette méthode nécessite n étapes et chaque étape consiste en une multiplication et une addition. Ainsi, elle nécessite n multiplications et n additions, ce qui est quand même mieux !

Les multiplications coûtent plus cher que les additions !

Théorème. *La fonction*

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \widetilde{P} \end{array} \right.$$

est un morphisme d'anneaux injectif.

Démonstration. Le fait que φ soit un morphisme d'anneaux est immédiat. Nous prouverons qu'il est injectif dans le paragraphe III.3.b. □

Remarques :

- 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 $\mathbb{K}$.
- Par définition d'une fonction polynomiale, toute fonction polynomiale est la fonction polynomiale associée à un polynôme. Ainsi, $\varphi(\mathbb{K}[X])$ est précisément égal à l'ensemble des fonctions polynomiales et donc φ réalise une bijection de $\mathbb{K}[X]$ dans l'ensemble des fonctions polynomiales. Cela permet d'« identifier » polynômes et fonctions polynomiales (tout en gardant à l'esprit qu'un polynôme n'est pas une fonction polynomiale).
- Ce théorème fait partie des quelques théorèmes de ce chapitre qui sont faux lorsqu'on travaille sur un corps quelconque.

  Par exemple, lorsque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Les polynômes $P = X$ et $Q = X^p$ sont deux polynômes distincts (car n'ont pas le même degré) à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Pourtant le petit théorème de Fermat assure que, pour tout $x \in \mathbb{Z}$, $x^p \equiv x\,[p]$. Ainsi, pour tout $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$, $\overline{x}^p = \overline{x}$ et donc $\widetilde{Q}(\overline{x}) = \widetilde{P}(\overline{x})$. Autrement dit $\widetilde{Q} = \widetilde{P}$ et donc φ n'est pas injective.

Ce sont en fait les polynômes $\overline{1}X$ et $\overline{1}X^p$.

4) Composition de polynômes

Définissons (autrement qu'avec des fonctions polynomiales) la notion de composition de polynômes (mais de sorte qu'elle soit analogue à la composition des fonctions polynomiales) :

Définition. *Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et Q dans $\mathbb{K}[X]$. On définit le polynôme $P \circ Q$ par la relation*

$$P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k.$$

On dit que $P \circ Q$ est la composition de P par Q.

$P \circ Q$ est bien défini puisque la somme est en fait une somme finie. C'est donc une combinaison linéaire de puissances de Q. Ces dernières sont des polynômes et une combinaison linéaire de polynômes en est un.

Remarques :

- Pour tout $P \in \mathbb{K}[X]$, $P \circ X = P$.
- On retrouve aussi la notation $P(Q)$ au lieu de $P \circ Q$. Ainsi il n'est pas rare de rencontrer la notation $P(X)$... qui veut simplement dire P.

Exemple : *Si* $P = X^3 - 5X^2 - X + 1$ *et* $Q = X^2 - 1$, *alors*

$$\begin{aligned} P \circ Q &= (X^2-1)^3 - 5(X^2-1)^2 - (X^2-1) + 1 \\ &= X^6 - 3X^4 + 3X^2 - 1 - 5X^2 + 10X - 5 - X^2 - 1 + 1 \\ &= X^6 - 3X^4 - 3X^2 + 10X - 6. \end{aligned}$$

Avec la convention que, pour tout $a \in \mathbb{N}^*$,

$$(-\infty) \times a = -\infty.$$

Proposition. *Soient* P *et* Q *dans* $\mathbb{K}[X]$ *tels que* Q *n'est pas constant. Alors* $\deg(PQ) = \deg(P) \times \deg(Q)$.

Démonstration. Si $P = 0$, alors $P \circ Q = 0$. Comme Q n'est pas constant, on a $\deg(Q) \geqslant 1$ et donc $\deg(P \circ Q) = -\infty = -\infty \times \deg(Q) = \deg(P)\deg(Q)$. Supposons que $P \neq 0$. Reprenons alors les notations de la définition en notant $p = \deg(P) \in \mathbb{N}^*$.

□

$P \circ Q$ s'appelle la composé de P par Q et est noté $P \circ Q$. Pourtant ici, il s'agit d'une (autre) définition de la composition (il s'agit d'une notion de composition de suites presque finies).

Remarques :

- Supposons que Q ait pour coefficient dominant b_q (toujours en supposant que $\deg(Q) \geqslant 1$). Le coefficient dominant de $P \circ Q$ est donc celui de $a_p Q$, qui se trouve donc être $a_p b_q^p$.
- Si Q est constant égal à λ, alors $P \circ Q$ est le polynôme constant égal au nombre $\sum_{k=0}^{+\infty} a_k \lambda^k$ (somme toujours faussement infinie), qui est $\widetilde{P}(\lambda)$.

Exemple : *Déterminer tous les polynômes* P *de* $\mathbb{K}[X]$ *vérifiant* $P(X^2) = (X^2+1)P(X)$.

On conclut avec $a \in \mathbb{K}$ (au lieu de $a \in \mathbb{K}^*$) pour prendre en compte le polynôme nul qui est solution.

Comme on l'a dit dans la marge, cette définition de la composition n'est pas la même que pour les fonctions polynomiales mais, bien sûr, elle a été conçue pour être analogue :

Le $\circ$ dans $\widetilde{P \circ Q}$ est la composition formelle de polynômes. Le $\circ$ dans $\widetilde{P} \circ \widetilde{Q}$ est la composition de fonctions (polynomiales ici).

Proposition. *Soient* P *et* Q *dans* $\mathbb{K}[X]$. *Alors* $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

5) Dérivée de polynômes

a) Dérivée formelle d'un polynôme

Définissons (autrement qu'avec des fonctions polynomiales) la notion de dérivée des polynômes (mais de sorte qu'elle soit analogue aux dérivées des fonctions polynomiales) :

La dérivée d'un polynôme est un polynôme qui a toujours un sens. Cela n'a rien à voir avec une limite d'un quelconque taux d'accroissement. Il n'y a aucune notion de dérivabilité : il ne faut jamais justifier qu'un polynôme est dérivable avant de calculer sa dérivée. Le nom et la notation P' sont bien sûr choisis pour l'analogie avec les fonctions polynomiales.

Définition. *Soit* $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. *On définit le polynôme dérivé* P' *de* P *par :*

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

Remarque : Bien que X^{-1} n'ait aucun sens, on peut tolérer que $0X^{-1}$ désigne le polynôme nul et donc tolérer l'usage de la définition

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

Exemples :

- *Si* $P = 8X + 7$, *alors* $P' = 8$.
- *Si* $P = 2X^5 + 9X^4 + 7\mathrm{i}X^3 + 2X + 5\mathrm{i} - 1$, *alors* $P' = 10X^4 + 36X^3 + 21\mathrm{i}X^2 + 2$.

Proposition. *Soit* $P \in \mathbb{K}[X]$.

- *Si* P *est constant, alors* $P' = 0$ *donc* $\deg(P) = -\infty$.
- *Si* $P \in \mathbb{K}[X]$ *n'est pas constant, alors* $\deg(P') = \deg(P) - 1$.

Remarque : Si P non constant est de degré p et de coefficient dominant a_p, alors P' est de coefficient dominant pa_p.

Démonstration. Reprenons les notations de la définition. Supposons que P est constant. Alors, dans la somme $P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$ tous les termes sont nuls (car $a_k = 0$ pour tout $k \geqslant 1$). Supposons que P n'est pas constant. Notons p son degré. Alors

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

Puisque $pa_p \neq 0$, il s'ensuit que P' est de degré $p-1$ et de coefficient dominant pa_p.□

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

Proposition. *Soient* P *et* Q *dans* $\mathbb{K}[X]$. *Soient* $n \in \mathbb{N}^*$ *et* $\lambda \in \mathbb{K}$. *On a*

$$(P+Q)' = P' + Q', \quad (\lambda P)' = \lambda P', \quad (PQ)' = P'Q + QP', \quad (P^n)' = nP'P^{n-1}.$$

et $(P \circ Q)' = Q' \times (P' \circ Q)$.

Démonstration. Notons $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$.

- On a

$$(P+Q)' = \left(\sum_{k=0}^{+\infty} (a_k + b_k) X^k\right)' = \sum_{k=1}^{+\infty} k(a_k + b_k) X^{k-1} = \sum_{k=1}^{+\infty} k a_k X^{k-1} + \sum_{k=1}^{+\infty} k b_k X^{k-1}$$

donc $(P+Q)' = P' + Q'$.

Encore une fois : touts ses sommes sont en fait finies (on peut les arrêter à l'indice que l'on veut supérieur au degré) donc on peut leur appliquer toutes les formules que l'on connaît sur les sommes d'éléments dans un anneau commutatif (c'est-à-dire quasiment toutes les mêmes que sur $\mathbb{C}$).

- On a
$$(\lambda P)' = \left(\sum_{k=0}^{+\infty} \lambda a_k X^k\right)' = \sum_{k=1}^{+\infty} k(\lambda a_k) X^{k-1} = \lambda \sum_{k=1}^{+\infty} a_k X^{k-1} = \lambda P'.$$
- Pour tout $k \in \mathbb{N}$, notons
$$c_k = \sum_{j=0}^{k} a_j b_{k-j}, \quad d_k = \sum_{j=0}^{k} (j+1) a_{j+1} b_{k-j} \quad \text{et} \quad e_k = \sum_{j=0}^{k} a_j (k-j+1) b_{k-j+1}$$
de sorte que
$$PQ = \sum_{k=0}^{+\infty} c_k X^k, \quad P'Q = \sum_{k=0}^{+\infty} d_k X^k \quad \text{et} \quad PQ' = \sum_{k=0}^{+\infty} e_k X^k.$$
Soit $k \in \mathbb{N}$. Via le changement d'indice $i = j+1$, il vient que
$$d_k = \sum_{i=1}^{k+1} i a_i (k-i) b_{k-i+1}$$

Notons aussi i l'indice dans d_k (possible ce sont des variables muettes) et sortons les terme d'indice 0 et $k+1$.

donc
$$\begin{aligned} d_k + e_k &= \left(\sum_{i=1}^{k} i a_i (k-i) b_{k-i+1} + (k+1) a_{k+1} (k-i) b_0\right) \\ &\quad + \left(a_0 (k+1) b_{k+1} + \sum_{i=1}^{k} a_i (k-i+1) b_{k-i+1}\right) \\ &= (k+1)(a_0 b_{k+1} + a_{k+1} b_0) + \sum_{i=1}^{k} (i+k-i+1) a_i b_{k-i+1} \\ &= (k+1) \sum_{k=0}^{k+1} a_i b_{k-i+1} \\ &= (k+1) c_{k+1}. \end{aligned}$$
On en déduit que
$$P'Q + PQ' = \sum_{k=0}^{+\infty} (d_k + e_k) X^k = \sum_{k=0}^{+\infty} (k+1) c_{k+1} X^k = (PQ)'.$$
- Le fait que $(P^n)' = nP'P^{n-1}$ se démontre par récurrence avec la formule précédente (laissée en exercice).
- Enfin
$$(P \circ Q)' = \left(\sum_{k=0}^{+\infty} a_k Q^k\right)' = \sum_{k=1}^{+\infty} a_k (Q^k)' = \sum_{k=1}^{+\infty} a_k (k Q' Q^{k-1}) = Q' \sum_{k=1}^{+\infty} k a_k Q^{k-1}$$
donc $(P \circ Q)' = Q' \times (P' \circ Q)$. □

Corollaire (linéarité de la dérivation polynomiale). *Soit $k \in \mathbb{N}^*$. Soient $P_1, \dots, P_k$ dans $\mathbb{K}[X]$ et soient $\lambda_1, \dots, \lambda_k$ dans $\mathbb{K}$. Alors*
$$\left(\sum_{i=1}^{k} \lambda_i P_i\right)' = \sum_{i=1}^{k} \lambda_i P_i'.$$

Comme on l'a dit dans la marge, cette définition de la dérivée n'est pas la même que pour les fonctions polynomiale mais, bien sûr, elle a été conçue pour être analogue :

Le $'$ dans $\widetilde{P'}$ est la dérivée formelle d'un polynôme. Le $'$ dans $\widetilde{P}'$ est la dérivée d'une fonction (polynomiale ici donc bien dérivable).

Proposition. *Soit $P \in \mathbb{K}[X]$. Alors $\widetilde{P'} = \widetilde{P}'$.*

b) Dérivées successives

Là encore, on ne justifie surtout pas les dérivabilités successives. On ne parle pas de classe $\mathscr{C}^n$ de polynôme.

Définition (dérivées successives). *Soit $P \in \mathbb{K}[X]$. On pose $P^{(0)} = P$, $P^{(1)} = P$ et, pour tout $k \geqslant 2$, on définit la dérivée $k^{\text{ième}}$ de P et on la note $P^{(k)}$ avec la relation de récurrence suivante :*

$$\forall k \in \mathbb{N}^*, \qquad P^{(k+1)} = (P^{(k)})'.$$

Exemple : *Si $P = X^3 + 5X + 3$, alors $P' = 3X^2 + 5$, $P'' = 6X$, $P^{(3)} = 6$, $P^{(4)} = 0$, $P^{(5)} = 0$, etc.*

Remarque : Si $P = \sum_{k=0}^{+\infty} a_k X^k$, alors $P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$, $P'' = \sum_{k=2}^{+\infty} k(k-1) a_k X^{k-2}$,

$$P^{(3)} = \sum_{k=3}^{+\infty} k(k-1)(k-2) a_k X^{k-3}, \quad \cdots$$

Supposons que P soit de degré $p \in \mathbb{N}^*$ et de coefficient dominant λ, alors on montre par récurrence (immédiate) que :

- Pour tout $n \in [\![0\,;p-1]\!]$, le coefficient dominant de $P^{(n)}$ est
- $P^{(p)}$ est le polynôme constant égal à $p!\lambda$.
- Si $n \geqslant p+1$, $P^{(n)}$ est le polynôme nul.

On en déduit :

Proposition. *Soit $P \in \mathbb{K}[X]$. Soit $n \in \mathbb{N}^*$.*

- *Si $\deg(P) < n$, alors $P^{(n)} = 0$.*
- *Si $\deg(P) \geqslant n$, alors $\deg(P^{(n)}) = \deg(P) - n$.*

Corollaire. *Soit $P \in \mathbb{K}[X]$. Soit $n \in \mathbb{N}^*$. Alors $P^{(n)} = 0$ si et seulement si $\deg(P) < n$.*

Exemple : *Déterminer tous les polynômes P de $\mathbb{K}[X]$ vérifiant $X^2P'' + 2XP = 6P$.*

Contrairement à l'exemple du paragraphe I.4, regarder le degré ne rien donner puisque X^2P'', $2XP'$ et $6P$ ont le même degré. Un réflexe à avoir lorsqu'une équation polynomiale fait intervenir des dérivées et de regarder le coefficient dominant puisque le degré y apparaît.

Par récurrence à partir de la formule $(PQ)' = P'Q + PQ'$, on obtient :

Proposition (formule de Leibniz). *Soient P et Q dans $\mathbb{K}[X]$. Pour tout $n \in \mathbb{N}^*$,*

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

Démonstration. Démonstration identique à celle du chapitre 19 pour les fonctions dérivables (les justifications de dérivabilité en moins). □

Et aussi, par récurrence immédiate :

Proposition. *Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors $\widetilde{P^{(n)}} = \widetilde{P}^{(n)}$.*

c) Formule de Taylor pour les polynômes

Proposition. *Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. Pour tout $k \in \mathbb{N}$, on a $a_k = \dfrac{P^{(k)}(0)}{k!}$.*

On devrait écrire $\widetilde{P^{(k)}}(0)$ (ou $\widetilde{P}^{(k)}(0)$) et non $P^{(k)}(0)$ bien sûr... mais cette abus de notation est classique.

Démonstration.

On devrait écrire $\widetilde{P^{(k)}}(a)$ (ou $\widetilde{P}^{(k)}(a)$) et non $P^{(k)}(a)$ bien sûr... mais cette abus de notation est classique.

Théorème (formule de Taylor pour les polynômes). *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :*

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

Il s'agit d'une somme faussement infinie puisque $P^{(k)}(a) = 0$ pour tout $k > \deg(P)$.

Démonstration.

L'intérêt principal de ce théorème est de relier les coefficients d'un polynôme avec ses dérivées successives évaluées en des valeurs fixées à l'avance. Ce sera l'ingrédient clé de la caractérisation de la multiplicité d'une racine par les dérivées successives dans le paragraphe III.3.b.

□

II Arithmétique sur $\mathbb{K}[X]$

1) Divisibilité dans $\mathbb{K}[X]$

Définition (diviseur et multiple). *Soit $(A,B)\in\mathbb{K}[X]^2$. On dit que B divise A (ou que A est divisible par B ou que B est un diviseur de A ou encore que A est un multiple de B) dans $\mathbb{K}[X]$ si il existe $C\in\mathbb{K}[X]$ tel que $A=BC$.*

Exemples :

- $X-1$ *divise* X^3-1 *car* $X^3-1=(X-1)(X^2+X+1)$.
- $X+\mathrm{i}$ *divise* X^2+1 *car* $X^2+1=(X+\mathrm{i})(X-\mathrm{i})$.
- $2X+2$ *divise* $X+1$ *car* $X+1=\dfrac{1}{2}(2X+2)$.
- X^2+1 *divise* X^4-1 *car* $X^4-1=(X^2+1)(X^2-1)$.
- X^3+2X+3 *divise* X^5+3X^2-4X-6 *car*
$$X^5+3X^2-4X-6=(X^3+2X+3)(X^2-2)$$

Remarques :

- Pour tout $B\in\mathbb{K}[X]$, $0=B\times 0$ donc $B|0$. Autrement dit 0 est un multiple de tout polynôme.
- Le polynôme nul ne divise que le polynôme nul lui même (car $0=0\times 0$ mais, pour tous $A\in\mathbb{K}[X]$ non nul et $C\in\mathbb{K}[X]$, $A\neq 0=C\times 0$).
- Les polynômes constants non nuls divisent tous les polynômes. En effet, pour touS $\lambda\in\mathbb{K}^*$ et $A\in\mathbb{K}[X]$, $A=\lambda\times\left(\dfrac{1}{\lambda}\times P\right)$.

Proposition. *Soient A et B dans $\mathbb{K}[X]$ avec $A\neq 0$. Si $B|A$, alors $\deg(B)\leqslant\deg(A)$.*

Démonstration.

□

Proposition. *Soient A,B,C,D dans $\mathbb{K}[X]$.*

- ***Réflexivité.*** *On a $A|A$.*
- ***Transitivité.*** *Si $C|B$ et $B|A$, alors $C|A$.*
- *Si $B|A$, alors $DB|DA$.*
- *Si $B|A$ et $D|C$, alors $BD|AC$.*
- *Si $B|A$ et $n\in\mathbb{N}^*$, alors $B^n|A^n$.*

Cette démonstration et la suivante sont similaires à celles des résultats analogues dans $\mathbb{Z}$ (cf. chapitre 12).

$\rightsquigarrow$ Démonstration laissée en exercice.

Proposition. *Soit $B \in \mathbb{K}[X]$. Soient $n \in \mathbb{N}^*$. Soient $A_1, \dots, A_n, C_1 \dots, C_n$ dans $\mathbb{K}[X]$ tels que $B|A_k$ pour tout $k \in [\![1\,;n]\!]$. Alors $B \left| \sum_{k=1}^{n} C_k A_k \right.$.*

En particulier, si $\lambda_1, \dots, \lambda_n$ sont dans $\mathbb{K}$, alors

$$B \left| \sum_{k=1}^{n} \lambda_k A_k \right.$$

$\rightsquigarrow$ Démonstration laissée en exercice.

Puisque la divisibilité dans $\mathbb{K}[X]$ est réflexive et transitive, on peut se demandeR s'il s'agit d'une relation d'ordre (bien sûr ce ne peut pas être une relation d'équivalence puisque $X+1|(X+1)^2$ mais pas le contraire). Et bien non... mais presque :

Définition. *Pour tout $(A, B) \in \mathbb{K}[X]^2$, on dit que A et B sont associés si $A|B$ et $B|A$.*

Proposition. *Soient A et B dans $\mathbb{K}[X]$. Alors A et B sont associés si et seulement si il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.*

Démonstration.

□

Pour poursuivre l'analogie avec l'arithmétique dans $\mathbb{Z}$, nous avons besoin d'un théorème de division euclidienne.

2) Théorème de la division euclidienne

Lorsque A et B sont à coefficients réels, on peut appliquer le théorème de la division euclidienne dans $\mathbb{R}[X]$, ce qui donne Q et R dans $\mathbb{R}[X]$ (mais alors P et Q appartiennent $\mathbb{C}[X]$). Mais on peut aussi l'appliquer dans $\mathbb{C}[X]$. Par unicité , on trouve que Q et R sont le quotient et le reste. Autrement dit, le théorème de la division euclidienne ne dépend pas du corps sur lequel on l'applique (lorsque A et B sont à coefficients réels bien sûr... sinon ça n'aurait pas de sens de l'appliquer sur $\mathbb{R}[X]$).

Nous avons déjà parlé de division euclidienne de fonctions polynomiales dans le chapitre 9, sans rien démontrer. Il est beaucoup plus adapté de pratiquer des divisions euclidiennes dans $\mathbb{K}[X]$ plutôt que sur des fonctions polynomiales en fait.

Théorème (division euclidienne). *Soient A et B deux polynômes de $\mathbb{K}[X]$ tels que $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$. Le polynôme Q (resp. R) est appelé le quotient (resp. le reste) de la division euclidienne de A par B.*

Démonstration.

□

Exemples :

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

$$\begin{array}{rrrrrrr|l}
5X^4 & - 2X^3 & + 16X^2 & - X & - 1 & & X^2 + 3 \\
\cline{8-8}
 & & - (5X^4 & + 15X^2) & & & 5X^2 - 2X + 1 \\
\cline{1-5}
 - 2X^3 & + X^2 & - X & - 1 & & & \\
 & & - (-2X^3 & - 6X) & & & \\
\cline{2-5}
 & X^2 & + 5X & - 1 & & & \\
 & & - (X^2 & + 3) & & & \\
\cline{3-5}
 & & 5X & - 4 & & &
\end{array}$$

Nous obtenons que le quotient est $Q = 5X^2 - 2X + 4$ et le reste $R = 5X - 4$ (il s'agit bien d'un polynôme de degré inférieur strictement au degré de B).

- *Soit $n \in \mathbb{N}\backslash\{0;1\}$. Déterminons le reste de la division euclidienne de $X^n + 1$ par $X^2 + 1$.*

Méthode classique : plus généralement, si B est un polynôme de degré n et que l'on connaît n racines distinctes de B, alors pour trouver les n coefficients potentiellement non nuls du reste de la division euclidienne de $A \in \mathbb{K}[X]$ par B, on évalue en les n racines distinctes. Nous verrons dans le paragraphe III.3.b comment faire s'il n'y a pas n racines distinctes.

Remarque : Dans l'exemple ci-dessus, bien que nous ayons utilisé des nombres complexes (et donc effectué une division euclidienne dans $\mathbb{C}[X]$), il était attendu que le reste soit dans $\mathbb{R}[X]$ puisque, X^n+1 et X^2+1 étant dans $\mathbb{R}[X]$, le théorème de la division euclidienne dans $\mathbb{R}[X]$, assurait que $R \in \mathbb{R}[X]$ et qu'il y a unicité du reste.

Lorsque $B|A$, il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$ et cette proposition montre au passage que Q est unique. Poursuivant la remarque dans la marge qui débute ce paragraphe, lorsque A et B sont dans $\mathbb{R}[X]$, si B divise A, le quotient Q tel que $A = BQ$ appartient à $\mathbb{R}[X]$ même si on regarde A et B comme des polynômes de $\mathbb{C}[X]$: la divisibilité ne dépend pas du corps (contrairement aux racines dans le paragraphe III.1).

Proposition. *Soient A et B dans $\mathbb{K}[X]$ tels que $B \neq 0$. On a $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.*

Démonstration. Si $B|A$, il existe $C \in \mathbb{K}[X]$ tel que $A = BC = BC + 0$ donc, par unicité, 0 est le reste de la division euclidienne de A par B. Réciproquement, si le reste de la division euclidienne de A par B est nul alors, en notant Q le quotient, on a $A = BQ$ et donc $B|A$. □

Exemple :

Le théorème de la division euclidienne va nous faire partir dans deux voies. Tout d'abord tout comme la division euclidienne dans $\mathbb{Z}$ nous a permis de faire un chapitre entier d'arithmétique, celle dans $\mathbb{K}[X]$ va aussi nous permettre de faire de l'arithmétique dans $\mathbb{K}[X]$ (avec théorème de Bézout, de Gauss, des polynômes premiers entre eux, etc.) dans la suite de ce paragraphe. Ensuite, nous verrons dans le paragraphe III que ce théorème permet de montrer que, si un polynôme P s'annule en $a \in \mathbb{C}$, alors on peut le factoriser par $X - a$ avec de nombreuses conséquences importantes. Nous explorerons donc la factorisation d'un polynôme de $\mathbb{K}[X]$ dans le paragraphe IV.

3) PGCDs et PPCMs de polynômes

On reprend la même progression que dans le chapitre 12. Nous omettons la plupart des preuves car elles sont analogues.

a) PGCDs de deux polynômes

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.

Soient A et B deux polynômes non tous nuls. Notons que le polynôme constant égal à 1 divise A et B. Il s'ensuit que l'ensemble

$$\{\deg(D) \,|\, D \text{ divise } A \text{ et } B\}$$

est non vide (il contient 0). Puisque 0 ne divise pas A et B à la fois (puisque l'un d'eux est non nul), cet ensemble est une partie de $\mathbb{N}$. Enfin il est majorée (par $\deg(A)$ si $A \neq 0$ et par $\deg(B)$ si $B \neq 0$). Il admet donc un plus grand élément. Ainsi A et B possèdent un diviseur commun qui admet le plus grand degré possible parmi les diviseurs commun de A et B. D'où la définition :

Grosse différence avec les entiers : on dit **un** PGCD et non pas **le** PGCD. En effet, si D est un PGCD alors, pour tout $\lambda \in \mathbb{K}^*$, λD est encore un PGCD : il y en a une infinité (mais ils sont associés comme nous allons le voir dans le prochain paragraphe).

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 :

- Un moyen simple de montrer que 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.
- Comme sur $\mathbb{Z}$:
  - ⋆ Un PGCD de A et B est un PGCD de B et A (le PGCD est commutatif).
  - ⋆ Lorsque $B \neq 0$, B est un PGCD de 0 et B.
  - ⋆ Un PGCD de A et B a un degré inférieur ou égal à $\min\{\deg(A); \deg(B)\}$ avec égalité si et seulement si l'un des deux divise l'autre.

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

b) Algorithme d'Euclide

L'algorithme d'Euclide est toujours valable pour les polynômes puisqu'il repose entièrement sur l'existence d'une division euclidienne dans $\mathbb{K}[X]$. Il repose sur l'idée fondamentale suivante : si R est le reste de la division euclidienne de A par B, alors un PGCD de A et B est un PGCD de B et R.

Exemple : *Déterminons un PGCD de $2X^3 - 8X^2 + 10X - 4$ et de $X^2 - 5X + 6$.*

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

Seule vraie différence avec $\mathbb{Z}$: l'algorithme d'Euclide donne **un** PGCD.

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

Démonstration. Les polynômes associés à R divisent R et tout polynôme divise 0 donc ils 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 : D et R sont associés □

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 $A \wedge B$. .*

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.

Démonstration. Notons $(R_1, \dots, R_n, 0)$ les restes successifs dans 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. □

Exemple : *Dans l'exemple précédent, on a vu qu'un PGCD de $2X^3 - 8X^2 + 10X - 4$ et de $X^2 - 5X + 6$ est $8X - 16 = 8(X - 2)$. Puisque $X - 2$ est unitaire et associé à $8X - 16$, on en déduit que $A \wedge B = X - 2$.*

c) Relation de Bézout

⚠ ... tout en gardant en tête qu'il faut parler d'**un** PGCD et pas du PGCD

L'algorithme d'Euclide étendu est encore valable pour des polynômes donc le théorème de Bézout est encore valable pour des polynômes :

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

- *Il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = A \wedge B$. Une telle relation est appelée relation de Bézout.*
- *Plus généralement, si $P \in \mathbb{K}[X]$, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = P$ si et seulement si P est un multiple de $A \wedge B$.*

⚠ Comme pour les entiers, il n'y a pas unicité de U et V (lorsqu'il y a existence).

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

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

On en tire une relation de Bézout :

$$\begin{aligned} X^4 - 1 &= (X^8 - 1) - X^4(X^4 - 1) \\ &= (X^8 - 1) - X^4((X^{12} - 1) - X^4(X^8 - 1) \\ &= (X^8 + 1)(X^8 - 1) - X^4(X^{12} - 1). \end{aligned}$$

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

📎 On peut montrer (cf. exercice ...) que, pour tous entiers naturels non nuls a et b,

$$(X^a - 1) \wedge (X^b - 1) = X^{a \wedge b} - 1.$$

📎 Une autre relation de Bézout (plus simple d'ailleurs) est $X^4 - 1 = (X^{12} - 1) - X^4(X^8 - 1)$.

On a la même conséquence très importante :

Proposition. *Soient A et B dans $\mathbb{K}[X]$ non tous nuls. Soit $D \in \mathbb{K}[X]$ non nul. Alors D divise A et B si et seulement si D divise $A \wedge B$.*

Et on en déduit encore :

Proposition. *Soient A, B, P dans $\mathbb{K}[X]$ non tous nuls. Si P est un polynôme **unitaire**, alors $(PA) \wedge (PB) = P(A \wedge B)$.*

d) Polynômes premiers entre eux

Définition. *Soient A et B dans $\mathbb{K}[X]$ non tous 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.

⚠ Comme pour les entiers, si aucun des deux ne divise l'autre, cela ne signifie pas qu'ils soient premiers entre eux.

Comme pour les entiers, on a :

Proposition. *Soient A et dans $\mathbb{K}[X]$ non tous nuls. Notons $D = A \wedge B$. Alors le quotient de A par D et le quotient de B par D sont premiers entre eux.*

Théorème (de Bézout). *Soient A et dans $\mathbb{K}[X]$ non tous nuls. Alors A et B sont premiers entre eux si et seulement s'il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.*

Exemple : *Soient a et b distincts dans $\mathbb{K}$. Les polynômes $X - a$ et $X - b$ sont premiers entre eux car*

Théorème (de Gauss). *Soient A, B, C dans $\mathbb{K}[X]$ non nuls. Si $A \wedge B = 1$ et $A|BC$, alors $A|C$.*

Proposition (produit de polynômes). *Soient A, B, C dans $\mathbb{K}[X]$ non nuls.*

- *Si $A \wedge B = 1$ et $A \wedge C = 1$, alors $A \wedge (BC) = 1$.*
- *Si $A|C$, $B|C$ et $A \wedge B = 1$, alors $AB|C$.*

e) PPCMs de deux polynômes

Soient A et B deux polynômes non nul. Notons que AB est un multiple non nul de A et de B. Il s'ensuit que l'ensemble

$$\{\deg(D) \mid D \text{ non nul, } A \text{ et } B \text{ divisent } D\}$$

est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément. Ainsi A et B possèdent un multiple commun qui admet le plus petit degré possible parmi les multiples communs non nuls de A et B. D'où la définition :

Là aussi on dit **un** PPCM et non pas **le** PPCM puisqu'il y en a plusieurs et même une infinité : tous les polynômes associés à un PPCM donné.

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

Remarques :

- Un moyen simple de prouver qu'un polynôme non nul 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.
- Comme sur $\mathbb{Z}$:
  - ⋆ Un PPCM de A et B est un PPCM de B et A (le PPCM est commutatif).
  - ⋆ Un PPCM de A et B a un degré supérieur à $\max\{\deg(A); \deg(B)\}$ avec égalité si et seulement si l'un des deux divise l'autre.

On montre aussi comme dans $\mathbb{Z}$ que :

Proposition. *Soient A et B dans $\mathbb{K}[X]$ non nuls. Soit $D \in \mathbb{K}[X]$ non nul. Alors D est un multiple de A et B si et seulement si D est un multiple de $A \wedge B$.*

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.

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 la proposition précédente, deux PPCMs de A et de B sont multiples l'un de l'autre donc sont associés. □

Pour finir, on a :

L'égalité $(A \wedge B)(A \vee B) = AB$ est fausse. Elle devient vraie si on multiplie le terme de gauche par les coefficients dominants de A et de B.

Proposition. *Soient A et B dans $\mathbb{K}[X]$ non nuls. Alors $(A \wedge B)(A \vee B)$ et AB sont associés.*

f) Extension à plusieurs polynômes

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

L'ensemble des degrés des diviseurs communs à $A_1, \dots, A_n$ est une partie de $\mathbb{N}$ (car 0 ne divise pas tous les A_i) non vide (car 1 divise les A_i) et majorée (par le degré d'un polynôme non nul parmi les A_i). Ainsi un PGCD existe bien.

Proposition/Définition. *Soient $n \in \mathbb{N}\backslash\{0;1\}$ et $A_1, \dots, A_n$ dans $\mathbb{K}[X]$ non tous nuls. Alors :*

- *Tout diviseur commun à $A_1, \dots, A_n$ et à B de degré maximal est appelé **un** PGCD de $A_1, \dots, A_n$.*
- *Les PGCD de $A_1, \dots, A_n$ sont associés.*
- *Il existe un unique PGCD unitaire que l'on note $A_1 \wedge A_2 \wedge \cdots \wedge A_n$.*
- *On dit que $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si $A_1 \wedge A_2 \wedge \cdots \wedge A_n = 1$.*
- *On dit que $A_1, \dots, A_n$ sont premiers entre eux deux à deux si, pour tout $(i,j) \in [\![1;n]\!]^2$ tel que $i \neq j$, $A_i \wedge A_j = 1$.*

Des polynômes premiers entre eux deux à deux le sont dans leur ensemble mais la réciproque est fausse.

Proposition (associativité). *Soient A, B, C dans $\mathbb{K}[X]$ non nuls.*

$$A \wedge B \wedge C = (A \wedge B) \wedge C = A \wedge (B \wedge C).$$

La notion de PPCM de strictement plus que deux polynômes n'est pas au programme, comme celle de strictement plus que deux entiers d'ailleurs.

Proposition. *Soient $n \in \mathbb{N}\backslash\{0;1\}$ et $A_1, \dots, A_n$ dans $\mathbb{K}[X]$ non nuls.*

- *(relation de Bézout) Il existe $U_1, \dots, U_n$ dans $\mathbb{K}[X]$ tels que*

$$A_1U_1 + A_2U_2 + \cdots + A_nU_n = A_1 \wedge \cdots \wedge A_n.$$

- *(théorème de Bézout) $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe $U_1, \dots, U_n$ dans $\mathbb{K}[X]$ tels que*

$$A_1U_1 + A_2U_2 + \cdots + A_nU_n = 1.$$

- *Soit $D \in \mathbb{K}[X]$. On a $D | A_1 \wedge \cdots \wedge A_n$ si et seulement si $D | A_i$ pour tout $i \in [\![1;n]\!]$.*
- *Si $D = A_1 \wedge \cdots \wedge A_n$, alors les quotients des A_i par D, $1 \leqslant i \leqslant n$, sont premiers entre eux dans leur ensemble.*
- *Soit $P \in \mathbb{K}[X]$ unitaire. Alors $(PA_1) \wedge \cdots (PA_n) = P(A_1 \wedge \cdots, A_n)$.*
- *Si $A_i \wedge P = 1$ pour tout $i \in [\![1;n]\!]$, alors $(A_1 \dots A_n) \wedge P = 1$.*
- *Si $A_i | P = 1$ pour tout $i \in [\![1;n]\!]$ et si $A_1, \dots, A_n$ sont premiers entre eux **deux à deux**, alors $(A_1 \dots A_n) | P$.*

Corollaire. *Soient A et B dans $\mathbb{K}[X]$ non nuls. Soient m et n des entiers naturels non nuls. On a $A \wedge B = 1$ si et seulement si $A^n \wedge B^m = 1$.*

Exemple : *Pour tout $(a,b) \in \mathbb{K}^2$ tel que $a \neq b$, on a vu que $X - a$ et $X - b$ sont premiers entre eux. Ainsi, pour tous m et n entiers naturels non nuls, $(X-a)^n$ et $(X-b)^m$ sont premiers entre eux.*

4) Polynômes irréductibles

Définition. *Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible si P n'est pas constant et si ses seuls diviseurs sont 1, P et leurs associés.*

Remarque : Les polynômes irréductibles sont pour les polynômes ce que les nombres premiers sont pour les entiers.

Proposition. *Un polynôme P est irréductible si et seulement s'il est non constant et ne peut pas s'écrire comme le produit de deux polynômes non constants.*

Puisque les polynômes constants non nuls sont les seuls polynômes inversibles de $\mathbb{K}[X]$, on peut reformuler : P est irréductible si P n'est pas inversible et ne peut pas s'écrire comme produit de deux polynômes non inversibles.

Remarques :

- Autrement dit P n'est pas irréductible si et seulement s'il existe A et B deux polynômes de degré compris entre 1 et $\deg(P) - 1$ tels que $P = AB$.
- En particulier, si P n'est pas irréductible, alors :
  - ⋆ ou bien il est constant donc de degré 0 ou $-\infty$.
  - ⋆ ou bien il est le produit de polynômes de degré au moins 1 et donc il est de degré au moins 2.

  Par contraposée, il vient que :

Proposition. *Tout polynôme de $\mathbb{K}[X]$ de degré 1 est irréductible.*

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

On prouve de façon analogue à $\mathbb{Z}$ le théorème suivant :

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

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

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

Le fait qu'un polynôme soit irréductible ou non dépend de $\mathbb{K}$ donc la décomposition en produit de facteurs irréductibles également (cf. paragraphe IV.3 et IV.4).

Remarque : On ne définit pas de valuation p-adique pour les polynômes. On peut tout de même montrer les résultats suivants pour tous polynômes A et B non nuls :

- 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 décompositions en facteurs irréductible n'ont aucun terme commun (sauf des éléments constants non nuls), c'est-à-dire si A et B n'ont aucun facteur irréductible commun.
- 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.

Exemple : *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 :*

III Racines d'un polynôme

1) Définition et caractérisation

Définition (racine d'un polynôme). *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine de P (dans $\mathbb{K}$) si $\widetilde{P}(a) = 0$.*

Mais, désormais, on notera définitivement $P(a)$ au lieu de $\widetilde{P}(a)$ pour simplifier.

Exemples :

- *Le polynôme nul admet tout élément de $\mathbb{K}$ comme racine (il en admet donc une infinité).*
- *Si P est constant non nul, alors P n'admet aucune racine.*
- *Si il existe $a \in \mathbb{R}$ tel que $P = X - a$, alors P admet a pour unique racine.*
- *Le polynôme $X^2 + X$ admet deux racines : 0 et -1.*
- *Le polynôme $X^2 + 1$ n'admet pas de racines dans $\mathbb{R}$ mais admet i et $-\mathrm{i}$ pour racines dans $\mathbb{C}$.*

On n'écrit surtout jamais « $X^2 + X = 0$ si et seulement $X = 0$ ou $X = -1$ »... ce serait une triple erreur : X est un objet précis, il n'est pas égal à -1 ou à 0 et $X^2 + X$ n'est pas le polynôme nul donc il est totalement faux d'écrire $X^2 + X = 0$. On écrirait plutôt : « Soit $x \in \mathbb{K}$. On a $x^2 + x = 0$ si et seulement si $x = 0$ ou $x = -1$. »

Remarque : Deux cas particuliers importants : lorsque $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$,

- 0 est racine de P si et seulement si le coefficient constant a_0 est nul (en effet $P(0) = a_0$).
- 1 est racine de P si et seulement si la somme des coefficients est nulle.

Il est enfin temps de montrer un résultat que nous avons rencontré plusieurs fois en exercice sans jamais le démontrer :

Théorème (caractérisation d'une racine par factorisation). *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de P si et seulement si $X - a$ divise P.*

On montre aussi plus généralement que le reste de la division euclidienne d'un polynôme P par $X - a$ est le polynôme constant égal à $P(a)$.

Démonstration.

□

Dans tout ce chapitre, quand on dit que des racines sont distinctes, cela voudra dire qu'elles sont **deux à deux** distinctes.

Théorème. *Soient $P \in \mathbb{K}[X]$, $n \geqslant 1$ et $a_1, \dots, a_n$ des éléments distincts de $\mathbb{K}$. Si $a_1, \dots, a_n$ sont des racines de P, alors $\prod_{j=1}^{n}(X - a_j)$ divise P.*

Démonstration.

□

2) Lien entre degré et nombre de racines

a) Nombre maximal de racines

Le théorème suivant est le plus important du chapitre !

En particulier, si P est un polynôme non nul, il admet au plus $\deg(P)$ racines distinctes.

Théorème. *Soit $n \in \mathbb{N}$. Soit $P \in \mathbb{K}_n[X]$.*

1. *Si P admet (au moins) $n+1$ racines distinctes, alors $P = 0$.*
2. *Si P est non nul, alors P admet au plus n racines distinctes.*

Démonstration.

□

b) Rigidité des polynômes

Ce corollaire est très important dans la pratique puisque nous ne connaissons pas forcément le degré des polynômes que nous manipulons.

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

Exemple : *La fonction $\sin$ n'est pas polynomiale. En effet :*

Nous pouvons enfin montrer le résultat suivant du paragraphe I.3 :

Théorème. *Le morphisme d'anneaux $\varphi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \widetilde{P} \end{array} \right.$ est injectif.*

Ce résultat est vrai dès que $\mathbb{K}$ est infini (ce qui est le cas pour $\mathbb{R}$ et $\mathbb{C}$). On peut montrer que l'infinité de $\mathbb{K}$ est même une condition nécessaire et suffisante pour que φ soit injectif.

Démonstration.

□

Proposition (rigidité de $\mathbb{K}[X]$). *Soit $n \in \mathbb{N}$. Soient P et $\mathbb{Q}$ dans $\mathbb{K}[X]$.*

1. *Si P et Q sont de degré inférieur à n et coïncident en au moins $n+1$ valeurs distinctes de $\mathbb{K}$, alors $P = Q$.*
2. *Si P et Q coïncident en une infinité de valeurs distinctes, alors $P = Q$.*

Démonstration. C'est une conséquence des résultats précédents puisque $P = Q$ si et seulement si $P - Q$ est le polynôme nul. □

Remarque : En général, lorsque deux fonctions f et g coïncident sur un sous-ensemble E de $\mathbb{K}$ (c'est-à-dire $f(x) = g(x)$ pour tout $x \in E$), même s'il est infini, il n'y a aucune raison qu'elles soient égales.

Par exemple $\sin$ *et* $\cos$ *coïncident sur* $\frac{\pi}{4} + \pi\mathbb{Z}$ *mais ne sont pas égales.*

On vient donc de voir que, si ce sont des fonctions polynomiales, alors il suffit qu'elles coïncident en « suffisamment de points » (une infinité ou seulement en un nombre en $n+1$ point si ils sont de degré au plus n), alors elles sont égales. Les polynômes sont donc des objets extrêmement rigides : il suffit de les connaître en « suffisamment de points » pour les caractériser totalement.

Exemples :

Énorme classique à savoir reproduire !

- *Tout polynôme de* $\mathbb{R}[X]$ *périodique est constant. En effet :*

- *Soit* $n \in \mathbb{N}$. *On a vu dans le paragraphe III.3 du chapitre 7, qu'il existe un polynôme* T_n *tel que, pour tout* $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$. *Existe-t-il un autre polynôme vérifiant cette condition ?*

Il s'agit de

$$T_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (1-X^2)^k X^{n-k}$$

On dit qu'il s'agit du $n^{\text{ième}}$ polynôme de Tchebychev. On en reparlera...

c) Un premier théorème de factorisation

Théorème. *Soit* $n \in \mathbb{N}^*$. *Soit* $P \in \mathbb{K}[X]$ *un polynôme de degré* n. *Supposons que* P *admette* n *racines distinctes* $a_1, \dots, a_n$. *Si* λ *désigne le coefficient dominant de* P, *on a alors :*

$$P = \lambda \prod_{k=1}^{n} (X - a_k).$$

Autre preuve possible : on sait que $Q|P$ d'après le théorème à la fin du paragraphe III.1 donc il existe $C \in \mathbb{K}[X]$ tel que $P = CQ$ donc

$$\deg(P) = \deg(C) + \deg(Q)$$

et donc $\deg(C) = 0$. Le polynôme C est constant. Comme P et Q ont même coefficient dominant, la constante en question est 1 et donc $P = Q$.

Démonstration.

□

Exemple : *On sait que* P *est un polynôme de degré inférieur à* 4 *admettant au moins* $-1, 3, \pi$ *pour racines.*

- *On peut alors conclure que* $(X+1)(X-3)(X-\pi)|P$.
- *Si on sait de plus que* 5 *est racine de* P, *alors on peut conclure que* $P = \lambda(X+1)(X-3)(X-\pi)(X-5)$ *avec* λ *son coefficient dominant si* $P \neq 0$ *et* $\lambda = 0$ *si* $P = 0$.
- *Si on sait de plus que* 5 *et* 17 *sont racines, alors* $P = 0$.

3) Ordre de multiplicité d'une racine

Le résultat que l'on vient d'obtenir est très important et efficace mais il ne permet pas de couvrir tous les cas de figure.

Par exemple $P = X(X-1)^2$ ne possède que deux racines distinctes 0 et 1 donc, on peut seulement conclure que $X(X-1)|P$ avec ce théorème.

Plus généralement le problème est que, lorsque a est racine d'un polynôme P non nul, alors $X-a$ divise P mais rien n'indique jusqu'à présent si on n'a pas aussi $(X-a)^2|P$ ou encore $(X-a)^3|P$, etc. Nous introduisons donc la notion d'ordre de multiplicité d'une racine.

a) Définition et première caractérisation

L'ordre de multiplicité d'une racine a de P est le plus grand entier k tel que $(X-a)^k$ divise P. Cet entier existe car, si a est une racine, alors $\{k \in \mathbb{N}^* \mid (X-a)^k | P\}$ est une partie non vide (elle contient 1) et majorée (par $\deg(P)$ puisque, pour tout $k \in \mathbb{N}^*$, si $(X-a)^k|P$, alors $\deg((X-a)^k) \leqslant \deg(P)$ donc $k \leqslant \deg(P)$) de $\mathbb{N}$ donc admet un maximum.

Définition (ordre de multiplicité d'une racine). *Soient $P \in \mathbb{K}[X]$ un polynôme non nul et $m \in \mathbb{N}^*$. On dit que $a \in \mathbb{K}$ est une racine d'ordre de multiplicité m de P si $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P. L'entier m est appelée l'ordre de multiplicité (ou parfois juste la multiplicité) de la racine a.*

Remarque : Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

- On dit que a est une racine simple de P si elle est de multiplicité 1, c'est-à-dire si $X-a$ divise P mais $(X-a)^2$ ne divise pas P.
- On dit que a est une racine multiple de P si elle est de multiplicité au moins 2, c'est-à-dire si $(X-a)^2$ divise P.
- On dit que a est une racine double de P si elle est de multiplicité 2, c'est-à-dire si $(X-a)^2$ divise P mais $(X-a)^3$ ne divise pas P.

Remarque : Pour tous $m \in \mathbb{N}^*$ et $a \in \mathbb{K}$, $(X-a)^m|0$ donc on dira parfois que tout élément de $\mathbb{K}$ est racine de multiplicité infinie du polynôme nul. On verra dans le paragraphe III.3.c que seul le polynôme nul admet des racines d'ordre de multiplicité infini.

Q est par ailleurs unique.

Proposition. *Soient $P \in \mathbb{K}[X]$ non nul, $m \in \mathbb{N}^*$ et $a \in \mathbb{K}$. Alors a est une racine de P d'ordre de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^k Q$ et $Q(a) \neq 0$.*

Si $m \in \mathbb{N}$ est tel que $(X-a)^m|P$, alors a est d'ordre de multiplicité **au moins** m.

Démonstration.

□

Exemple : *Le polynôme $P = 2X^3 - 6X^2 - 18X - 10 = 2(X-5)(X+1)^2$ admet 5 pour racine simple et -1 pour racine double.*

b) Une caractérisation avec les dérivées successives

Dans la pratique, il n'est pas des plus pratique de diviser un polynôme par $X-a$ (a étant une racine) tant que c'est possible pour obtenir la multiplicité. Il existe une caractérisation utilisant les dérivées successives de ce polynôme :

Théorème. *Soient $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors a est racine d'ordre de multiplicité m de P si et seulement si*

$$P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0 \qquad \text{et} \qquad P^{(k)}(a) \neq 0.$$

Démonstration.

□

Remarque : Regardons quelques cas particuliers :

- a est racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.
- a est racine double de P si et seulement si $P(a) = P'(a) = 0$ et $P''(a) \neq 0$.
- a est racine multiple de P si et seulement si $P(a) = P'(a) = 0$.

Ici il manque l'information de la première dérivée successive qui ne s'annule pas en a (pour tout $k \geqslant 2$, la multiplicité est k si et seulement si il s'agit de $P^{(k)}$).

Exemples :

- *Considérons* $P = X^4 - 5X^3 + 6X^2 + 4X - 8$.

On a vu dans le paragraphe II.2 une méthode permettant de trouver le reste de la division euclidienne d'un polynôme A par un autre B de degré $n \in \mathbb{N}^*$ lorsque l'on connaît n racines distinctes de B. Lorsque les racines sont potentiellement multiples, il faut donc penser à dériver suffisamment de fois l'expression obtenue en appliquant le théorème de la division euclidienne.

- *Soit $n \in \mathbb{N}\backslash\{0;1\}$. Déterminons le reste de la division euclidienne dans $\mathbb{R}[X]$ (ou dans $\mathbb{C}[X]$, peu importe ici) de X^n+1 par $(X+1)^2$.*

Corollaire. *Soient $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $m \in \mathbb{N}\backslash\{0;1\}$. Si a est une racine de P d'ordre de multiplicité m, alors a est racine de P' d'ordre de multiplicité $m-1$.*

Voyons une conséquence qui sera bien pratique pour la factorisation dans $\mathbb{R}[X]$ dans le paragraphe IV.4.

Proposition. *Soit $P \in \mathbb{R}[X]$ (à coefficients **réels** donc). Soit $a \in \mathbb{C}$ et $m \in \mathbb{N}^*$. Alors a est racine de P de multiplicité m si et seulement si $\overline{a}$ est racine de P de multiplicité m.*

Démonstration.

□

c) Un théorème de factorisation prenant en compte les multiplicités

On dit que le nombre de racines, **comptées avec multiplicité**, de P est au plus $\deg(P)$.

Théorème. *Soit $k \in \mathbb{N}^*$. Soit $P \in \mathbb{K}[X]$ **non nul** admettant k racines $a_1, \dots, a_k$ distinctes de P d'ordres de multiplicité respectifs (au moins) $m_1, \dots, m_k$ Alors*

$$\sum_{j=1}^{k} m_j \leqslant \deg(P) \qquad \text{et} \qquad \prod_{j=1}^{k} (X - a_j)^{m_j} \Big| P.$$

De plus, si λ désigne le coefficient dominant de P, alors

$$\sum_{j=1}^{k} m_k = \deg(P) \qquad \Longleftrightarrow \qquad P = \lambda \prod_{j=1}^{k} (X - a_j)^{m_j}.$$

Le cas d'égalité assure alors que ce sont alors les ordres de multiplicité exacts.

Démonstration.

Par contraposée, on a :

Corollaire. *Soient $k \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. Soit $P \in \mathbb{K}_n[X]$. Si P admet des racines $a_1, \dots, a_k$ dont les ordres de multiplicité sont au moins $m_1, \dots, m_k$ vérifiant $\sum_{j=1}^{k} m_j > n$, alors P est le polynôme nul.*

Exemple : *Soit P un polynôme de degré au moins 3 tel que $P(1) = P'(1) = P(-1) = 0$. Comme 1 est racine de multiplicité au moins 2 et que -1 est racine de multiplicité au moins 1, on a $(X-1)^2(X+1) | P$.*

- *Si P est de degré 3 (donc non nul) de coefficient dominant 2, alors $P = 2(X-1)^2(X+1)$.*
- *Si $P''(1) = 0$, alors 1 est de multiplicité au moins 3. Comme $3 + 1 > 3$, il s'ensuit que P est nul.*

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

On vient de voir que la connaissance de racines et de leurs multiplicités permet de factoriser un polynôme. Mais quand s'arrêter dans la factorisation ? Peut-on toujours factoriser un polynôme (non constant) comme produit de polynômes de degré 1 ?

1) Polynômes scindés

Définition. *Soit $P \in \mathbb{K}[X]$ non constant. On dit que 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 $n \in \mathbb{N}^*$ est scindé s'il existe $\lambda \in \mathbb{K}^*$ (le coefficient dominant) et $(a_1, \dots, a_n) \in \mathbb{K}^n$ (ses racines, pas forcément distinctes mais comptées avec multiplicité) tels que
$$P = \lambda(X - a_1) \times \cdots \times (X - a_n).$$
Mais, dans la pratique, on regroupe souvent les racines égales, comme dans le théorème de factorisation du paragraphe précédent :
$$P = a(X - b_1)^{m_1} \times \cdots \times (X - b_k)^{m_k}$$
où les b_i, $1 \leqslant i \leqslant k$ sont les racines distinctes de P de multiplicités respectives $m_1, \dots, m_k$. On a alors $\deg(P) = \sum_{j=1}^{k} m_j$.

On peut aussi l'écrire sous la forme
$$\prod_{j=1}^{n}(\alpha_j X + \beta_j)$$
mais c'est moins pratique pour lire les racines.

On a dien sûr $\{b_1, \dots, b_k\} \subset \{a_1, \dots, a_n\}$.

- Quand une telle écriture est possible, elle est parfois plus intéressant 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 $\mathbb{R}$).
- Un polynôme P non constant est donc scindé sur $\mathbb{K}$ si et seulement si il possède un nombre de racines (comptées avec multiplicité) égal à son degré.

Pour écrire un polynôme sous forme scindée (quand c'est possible !), il faut donc connaître : **ses racines, leur multiplicité et le coefficient dominant**.

Exemples :

- *Le polynôme $4X^3 - 4X^2 + X$...*
- *Le polynôme $X^2 + 1$...*

On voit que le fait qu'un polynôme soit scindé ou non dépend du corps $\mathbb{K}$ sur lequel on se place.

- *De même, $X^2 + X + 1$...*

Remarque :
Plus généralement, lorsque $P = aX^2 + bX + c \in \mathbb{K}[X]$ est de degré 2 (donc avec $a \neq 0$), la quantité $\Delta = b^2 - 4ac$ s'appelle toujours le discriminant du polynôme P. Reprenons les résultats vus dans les chapitres 3 et 6 :

- Si $\mathbb{K} = \mathbb{C}$, P est scindé. Plus précisément :
  - ⋆ Si $\Delta \neq 0$, $P = a(X - r_1)(X - r_2)$ où $r_1 = \dfrac{-b + \delta}{2a}$ et $r_2 = \dfrac{-b - \delta}{2a}$ et $\delta^2 = \Delta$.
  - ⋆ Si $\Delta = 0$, $P = a(X - r_0)^2$ où $r_0 = -\dfrac{b}{2a}$.
- Si $\mathbb{K} = \mathbb{R}$, P est scindé si et seulement si $\Delta \geqslant 0$. Plus précisément :
  - ⋆ Si $\Delta > 0$, $P = a(X - r_1)(X - r_2)$ où $r_1 = \dfrac{-b + \sqrt{\Delta}}{2a}$ et $r_2 = \dfrac{-b - \sqrt{\Delta}}{2a}$.
  - ⋆ Si $\Delta = 0$, $P = a(X - r_0)^2$ où $r_0 = -\dfrac{b}{2a}$.

2) Relations coefficients/racines

Lorsque $P = aX^2 + bX + c \in \mathbb{C}[X]$ est de degré 2, il est donc scindé sur $\mathbb{C}$. Notons x_1 et x_2 ses deux racines (éventuellement égales). On a alors

$$P = a(X - x_1)(X - x_2) = aX^2 - a(x_1 + x_2)X + ax_1x_2.$$

Dès lors :

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

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 pour un polynôme $P = aX^3 + bX^2 + cX + d$ de degré 3 que l'on suppose scindé sur $\mathbb{K}$.

Là aussi on peut exprimer les coefficients à l'aide des racines et du coefficient dominant.

Pour un polynôme scindé de degré supérieur, on a besoin d'introduire de nouvelles notations.

Pour faire simple : on prend tous les choix possibles de k indices parmi $1, \dots, n$, c'est-à-dire 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 (cf. chapitre 30).

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

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

En particulier :

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

Exemple : *Si $n = 4$ et $k = 2$, on a*

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

Remarques :

- On les appelle symétriques car, si on intervertit x_i et x_j, la somme reste la même.
- Conformément au programme : Les formules pour $k = 1$ et $k = n$ doivent être sues sur le bout des doigts. Les autres doivent être retrouvées facilement dans un cas explicite.

On peut désormais généraliser les résultats précédents à un polynôme scindé de degré quelconque.

Théorème (relations coefficients/racines ou formules de Viète). *Soit $n \in \mathbb{N}^*$. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré n **scindé** de racines (pas forcément distinctes) $x_1, \dots, x_n$. Alors, pour tout $k \in [\![1\,;n]\!]$,*

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

donc a_n est non nul : c'est son coefficient dominant.

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

c'est-à-dire que :

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

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 $(-x_{i_1}) \times \cdots \times (-x_{i_k}) = (-1)^k x_{i_1} \cdots x_{i_k}$ avec $i_1 < \cdots < i_k$, 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. □

Remarques :

- Nous montrerons dans le paragraphe suivant que tout polynôme à coefficients complexes non constant est scindé : ce théorème est donc valable pour tout polynôme à coefficients complexes non constant.
- ⚠ Dans la formule du théorème, on trouve σ_k dans le terme à la puissance $n-k$. On fera également atttention à l'alternance des signes (c'est-à-dire au $(-1)^k$).
- Par conséquent, on peut retrouver les coefficients quand on connaît les racines. Malheureusement, le contraire est faux : à partir du degré 5, il n'existe pas de formule permettant d'obtenir les racines à partir des coefficients.

Il est démontré qu'il n'en existe pas !

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

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

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 !

3) Factorisation dans $\mathbb{C}[X]$

a) Le théorème de D'Alembert-Gauss

Le théorème suivant est admis, conformément au programme.

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

Remarque : Ce théorème est très important : on l'appelle parfois « théorème fondamental de l'algèbre ».

b) Décomposition en produit de facteurs irréductibles

Corollaire. *Les irréductibles de $\mathbb{C}[X]$ 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 que l'on note α. Dès lors P est divisible par $X - \alpha$, c'est-à-dire il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-\alpha)Q$. 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. Ainsi Q est constant (non nul car P est non nul) si bien que P est de degré 1. □

Lorsque l'on demande de factoriser un polynôme sur $\mathbb{C}[X]$, il est sous-entendu qu'il faut l'écrire sous cette forme (en regroupant éventuellement les racines identiques en mettant en puissance la multiplicité). On dit aussi qu'il est écrit sous forme factorisée (puisque cette écriture est sa factorisation en produit de facteurs irréductibles).

Théorème (Factorisation d'un polynôme dans $\mathbb{C}[X]$). *Soit $P \in \mathbb{C}[X]$ non constant. Alors P est scindé, c'est-à-dire qu'il existe $\lambda \in \mathbb{C}^*$ (son coefficient dominant) et $(a_1, \dots, a_n) \in \mathbb{C}^n$ (ses racines, pas forcément distinctes) tels que*

$$P = \lambda \prod_{k=1}^{n} (X - a_i).$$

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

Démonstration. On a vu dans le paragraphe II.4 que 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. □

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

c) Méthodes et exemples

Disons le tout de suite : en général, on ne sait pas factoriser un polynôme quelconque (surtout à partir du degré 5 puisque, on l'a dit, il n'y a pas de formules donnant les racines en fonction des coefficients). Il y a tout de même plusieurs méthodes, que nous avons déjà vues dans le chapitre 6. Notamment :

Mais, si ces méthodes échouent (typiquement, si on ne trouve même pas de racine évidente), alors c'est vraiment très difficile.

- Trouver des racines évidentes, puis leur multiplicité (par exemple avec le critère avec les dérivées successives) puis factoriser (par exemple en posant la division euclidienne). On essaie de se ramener à des polynômes de degré 2 que l'on sait totalement factoriser (cf. paragraphe IV.1).
- Utiliser des racines $n^{\text{ièmes}}$ de complexes.
- Faire des changements de variables pour se ramener aux deux situations précédentes..

Mais, pour la énième fois, on n'utilise pas X pour faire des changements de variables. On ne pose pas non plus $Y = X^2$ par exemple mais on raisonne sur l'application polynomiale associée. A la place, on se donne un complexe z, on pose $\zeta = z^2$ s'il faut, etc. Autre possibilité, on introduit un polynôme Q tel que $P = Q \circ X^2$ et on cherche les racines de Q.

Exemples :

- *Factoriser $P = 4X^4 + 4X^3 - 2X^2 + 2$.*

- *Soit $n \in \mathbb{N}^*$. Factorisons $P_n = X^n - 1$ dans $\mathbb{C}[X]$.*

Exemple explicitement au programme !

- *Factorisons $P = X^6 + X^3 + 1$ dans $\mathbb{C}[X]$.*

On peut aussi introduire $Q = X^2 + X + 1$ et dire que $P = Q(X^3)$. On a

$$Q = (X - \mathrm{j})(X - \mathrm{j}^2)$$

donc

$$P = (X^3 - \mathrm{j})(X^3 - \mathrm{j}^3)$$

et il reste à factoriser ces deux polynômes.

d) Conséquences sur la divisibilité

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. On a évoqué à la fin du paragraphe II.4 qu'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 à coefficients complexes soient premiers entre eux.

Proposition. *Deux polynômes à coefficients 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 à coefficients 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.

Ce résultat est faux dans un corps $\mathbb{K}$ quelconque, en particulier sur $\mathbb{R}$. 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 commune (ils n'ont aucune racine tout court)

- Si A et B ont une racine complexe a commune, alors ils sont tous les deux divisibles par $X - a$ donc ils ne sont pas premiers entre eux (ils ont un diviseur commun non constant).
- Réciproquement, supposons que A et B ne soient pas premiers entre eux. Notons D un PGCD de A et B. Celui-ci n'est alors pas constant. Le théorème de d'Alembert-Gauss entraîne que D admet une racine complexe notée a. Or, D divise A et B donc il existe Q et R tels que $A = DQ$ et $B = DR$ si bien que a est racine de A et B : A et B ont bien une racine complexe commune. □

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

Puisque $\mathbb{R}$ est inclus dans $\mathbb{C}$, on a aussi :

Corollaire. *Deux polynômes de $\mathbb{R}[X]$ non tous nuls sont premiers entre eux si et seulement s'ils n'ont aucune racine **complexe** commune.*

Exemple : *X^2+X+1 et X^2-3X+2 sont premiers entre eux puisque le premiers admet j et j^2 pour racines et le second admet 1 et 2 pour racines.*

4) Factorisation dans $\mathbb{R}[X]$

a) Décomposition en produit de polynômes irréductibles

On a vu dans le paragraphe III.3.b qu'un polynôme de $\mathbb{R}[X]$ admettant une racine complexe α admet aussi $\overline{\alpha}$ pour racine et avec même multiplicité. Remarquons que :

C'est l'ingrédient clef de la démonstration du théorème suivant :

Quand on demande de factoriser un polynôme de $\mathbb{R}[X]$, il est sous-entendu qu'on doit l'écrire sous cette forme. On ne s'arrête pas tant qu'il demeure dans la factorisation des polynômes de degré supérieur à 3 ou de degré 2 à discriminant positif.

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

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

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 $\lambda\in\mathbb{R}^*$ (son coefficient dominant : il est donc réel) et $(a_1,\dots,a_q)\in\mathbb{C}^q$ distincts (les racines, qui sont donc complexes) de multiplicités respectives $m_1,\dots,m_q$ tels que

$$P=\lambda\prod_{k=1}^{q}(X-a_k)^{m_j}.$$

Notons r le nombre de racines réelles (on a $r\in[\![0\,;q]\!]$). 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, on a vu dans le paragraphe III.3.b que, si $b\in\mathbb{C}$ est racine de P, alors $\overline{b}$ est racine avec la même multiplicité que b. Encore une fois, quitte à changer l'ordre des racines, on suppose que :

$$a_{r+2}=\overline{a_{r+1}},\quad a_{r+4}=\overline{a_{r+3}},\quad \dots,a_q=\overline{a_{q-1}}.$$

Notons $b_1=a_{r+1}$, de multiplicité n_1, $b_2=a_{r+3}$, de multiplicité n_2, et ainsi de suite jusqu'à $b_s=\alpha_{q-1}$, de multiplicité n_s. En d'autres termes :

$$P=\lambda\prod_{k=1}^{r}(X-a_k)^{m_j}\prod_{k=1}^{s}(X-b_k)^{n_k}(X-\overline{b_k})^{n_k}.$$

Or, pour tout $k\in[\![1\,;s]\!]$,

$$(X-b_k)\times\left(X-\overline{b_k}\right)=X^2-2\,\mathrm{Re}(b_k)X+|b_k|^2,$$

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 $Q_k=(X-b_k)\times\left(X-\overline{b_k}\right)$. Finalement,

$$P=\lambda\prod_{k=1}^{r}(X-a_k)^{m_k}\prod_{k=1}^{s}Q_k^{n_j}.$$

□

Dans la pratique, il est inutile de calculer un discriminant si on sait que le polynôme n'admet pas de racine : le discriminant sera automatiquement strictement négatif !

Corollaire. *Tout polynôme de $\mathbb{R}[X]$ de degré impair admet une racine réelle.*

Ce résultat a aussi été montré dans le chapitre 18 avec le TVI.

Démonstration. Soit $P \in \mathbb{R}[X]$. Montrons la contraposée : supposons que P n'a pas de racine réelle. Il n'y a donc pas de polynôme de degré 1 dans sa décomposition en produit de facteurs irréductibles, seulement des polynômes de degré 2 de discriminants strictement négatifs. Avec les notations de la démonstration précédente, on a alors

$$\deg(P) = \sum_{k=1}^{s} \deg(Q_k^{n_k}) = \sum_{k=1}^{s} \deg(Q_k^{n_k}) = \sum_{k=1}^{s} 2n_k$$

et donc $\deg(P)$ est pair. D'où le résultat par contraposée. □

Il est tout de même remarquable que les irréductibles de $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$ 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 !

Corollaire. *Les irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif. De plus, 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.

« 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 (on déterminera, dans le paragraphe suivant, sa décomposition en produit de facteurs irréductibles).

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

b) Méthodes et exemples

Disons le tout de suite, tout comme dans $\mathbb{C}[X]$, on ne sait pas factoriser un polynôme quelconque dans $\mathbb{R}[X]$ (surtout à partir du degré 5 puisqu'il n'y a pas de formule donnant les racines en fonction des coefficients).

Puisque $\mathbb{R}[X] \subset \mathbb{C}[X]$, on peut factoriser un polynôme à coefficients réels dans $\mathbb{C}[X]$ puis, dans le cas où il y a des racines non réelles, on regroupe chaque racine non réelle avec son conjugué (qui est racine de même multiplicité).

Sinon, sans passer par $\mathbb{C}[X]$, la méthode est la même : on trouve des racines évidentes puis leur multiplicité. La différence est que, si on rencontre un trinôme du second degré à discriminant strictement négatif, on le laisse tel quel dans la factorisation (contrairement à $\mathbb{C}[X]$).

En un mot, on reproduit la démonstration du théorème de factorisation dans $\mathbb{R}[X]$ dans le cas concret rencontré.

Exemples :

- *Factoriser $P = 4X^4 + 4X^3 - 2X^2 + 2$ dans $\mathbb{R}[X]$. On a déjà rencontré cet exemple dans le paragraphe IV.3.c où on a montré que -1 était de multiplicité 2.*

On peut aussi dire qu'il existe a, b, c réels tels que

$$P = X(X-1)(X+1) \times (aX^2 + bX + c),$$

puis développer :

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

et utiliser l'unicité des coefficients d'un polynôme pour obtenir que $a = 1$, $b = 1$, $c - a = 0$ et $-c = -1$.

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

- *Factorisons $P = X^6 + X^3 + 1$ dans $\mathbb{R}[X]$. On l'a déjà fait dans $\mathbb{C}[X]$ dans le paragraphe IV.3.c :*

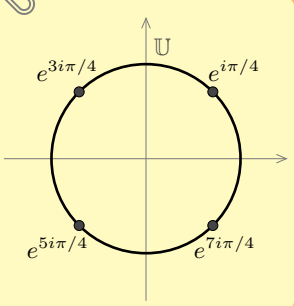
$$P = (X - \mathrm{e}^{\frac{2\mathrm{i}\pi}{9}})(X - \mathrm{e}^{-\frac{2\mathrm{i}\pi}{9}})(X - \mathrm{e}^{\frac{4\mathrm{i}\pi}{9}})(X - \mathrm{e}^{-\frac{4\mathrm{i}\pi}{9}})(X - \mathrm{e}^{\frac{8\mathrm{i}\pi}{9}})(X - \mathrm{e}^{-\frac{8\mathrm{i}\pi}{9}}).$$

- *Soit $n \in \mathbb{N}^*$. Factorisons $X^{2n} - 1$ dans $\mathbb{R}[X]$. On l'a déjà fait dans $\mathbb{C}[X]$ dans le paragraphe IV.3.c :*

$$P_n = \prod_{k=0}^{2n-1} (X - \mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}).$$

- *Factorisons $P = X^4 + 1$.*

  ⋆ ***Méthode 1 (utilisation de $\mathbb{C}$).***



Cela ressemble à la méthode de la forme canonique mais, au lieu de faire apparaître une identité remarquable avec les termes de degré 1 et 2, on le fait avec les termes de degré 0 et 2.

En général, cette méthode de donne pas de résultat puisqu'on se retrouve souvent avec d'autres équations polynomiales que l'on ne sait pas résoudre. Bref, on oublie !

On aurait aussi pu écrire $P = Q(X^2)$ avec

$$Q = X^2 - 7X + 9.$$

Le discriminant de ce dernier est 13 donc Q admet deux racines $\frac{7 \pm \sqrt{13}}{2}$. Ainsi

$$P = \left(X^2 - \frac{7+\sqrt{13}}{2}\right)\left(X^2 - \frac{7-\sqrt{13}}{2}\right).$$

et on factorise chacun de ces deux trinômes. On trouve bien les mêmes racines puisque

$$\left(\frac{1+\sqrt{13}}{2}\right)^2 = \frac{7+\sqrt{13}}{2},$$

etc.

⋆ ***Méthode 2 (en faisant apparaître une identité remarquable).***

Méthode 3 (en résolvant un système). *On sait (par le théorème de factorisation), qu'il existe a, b, c, d réels tels que*

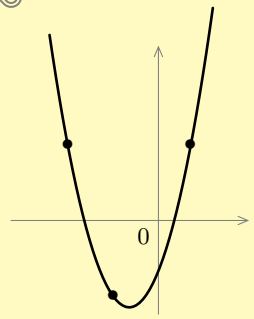
$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

(puisqu'il n'y a pas de racines, il n'y a que des polynômes de degré 2 à discriminant strictement négatif). En développant, par unicité des coefficients d'un polynôme, on a $a + c = 0$, $b + d + ac = 0$, $ad + bc = 0$ et $bc = 1$... mais ce système est très compliqué à résoudre. On passe !

- *Dans le même goût, factorisons $P = X^4 - 7X^2 + 9$.*

- *Factorisons $P = X^4 + 3X^2 - 28$. On ne peut pas faire apparaître d'identité remarquable ici mais on peut utiliser la méthode vue dans la marge ci-dessus :*

V Polynôme d'interpolation de Lagrange



Soit $n \in \mathbb{N}^*$. On considère :

- $a_1, \dots, a_n$ des éléments **distincts** de $\mathbb{K}$.
- $b_1, \dots, b_n$ (pas forcément distincts) des éléments de $\mathbb{K}$.

On cherche $P \in \mathbb{K}[X]$ tel que, pour tout $k \in [\![1\,;n]\!]$, $P(a_k) = b_k$.

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 $(a_1, b_1), \dots, (a_n, b_n)$.

La démarche est à connaître sur le bout des doigts. Il faut savoir qu'un tel polynôme P existe et le retrouver explicitement (voir connaître directement l'expression de celui de degré minimal, appelé polynôme d'interpolation de Lagrange).

On ne dit pas que P est unique : on dit que c'est le seul polynôme de degré inférieur à $n-1$ qui convient. Mais, comme nous allons le voir ci-dessous, une infinité de polynômes conviennent (mais de degré supérieurs à n).

Retenons :

Théorème. *Avec les notations précédentes, le polynôme*

$$P = \sum_{k=1}^{n} b_k \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq k}} \frac{X - a_j}{a_k - a_j}$$

est l'unique polynôme à coefficients dans $\mathbb{K}$ et de degré inférieur ou égal à $n-1$ tel que, pour $k \in [\![1\,;n]\!]$, $P(a_k) = b_k$. Ce polynôme est appelé polynôme d'interpolation de Lagrange passant par les points $(a_1, b_1), \dots, (a_n, b_n)$.

Exemple : *Cherchons un polynôme à coefficients réels tel que $P(-1) = 4$, $P(1) = -5$ et $P(2) = -3$. Le théorème précédent assure que :*

En développant, on trouve $P = \frac{1}{6}(23X^2 - 27X - 16)$.

Remarque :

- Si $n = 2$, on a

  $$P = b_1 \frac{X - a_2}{a_1 - a_2} + b_2 \frac{X - a_1}{a_2 - a_1} = \frac{b_1(X - a_2) - b_2(X - a_1)}{a_1 - a_2} = \frac{(b_1 - b_2)X + a_1 b_2 - b_1 a_2}{a_1 - a_2}$$

  et donc

  $$P = \frac{b_1 - b_2}{a_1 - a_2}(X - a_1) + b_1.$$

  On retrouve le fait que, par deux points d'abscisses distinctes, passent une unique droite non verticale (le graphe d'une fonction affine).
- Si $n = 3$, cela résultat démontrer qu'il existe une unique fonction polynomiale de degré inférieur ou égal à 2 dont le graphe passe par ces trois points.

Et si on n'impose plus la condition sur le degré ?

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 si et seulement s'il existe $B \in \mathbb{K}[X]$ tel que*

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

C'est-à-dire si et seulement si P est le reste de la division euclidienne de Q par $(X - a_1) \dots (X - a_n)$.

Démonstration. Un polynôme de cette forme est immédiatement solution. Réciproquement, supposons que Q convienne. Alors $a_1, \dots, a_n$ sont des racines distinctes de $Q - P$ (puisque, pour tout $k \in [\![1\,;n]\!]$, $Q(a_k) = b_k = P(a_k)$) et donc $Q - P$ est divisible par $(X - a_1) \cdots (X - a_n)$ ce qui permet de conclure. □

Nous dirons au chapitre 37 que l'ensemble des solutions est un espace affine.

Remarque : Pour terminer ce chapitre, remarquons que finalement connaître un polynôme à coefficients complexes de degré $n \in \mathbb{N}$ consiste à posséder $n + 1$ informations :

- ou bien ses $n + 1$ coefficients.
- ou bien ses n racines complexes (comptées avec multiplicité) et le coefficient dominant.
- ou bien la valeur qu'il prend en $n + 1$ points distincts quelconques.