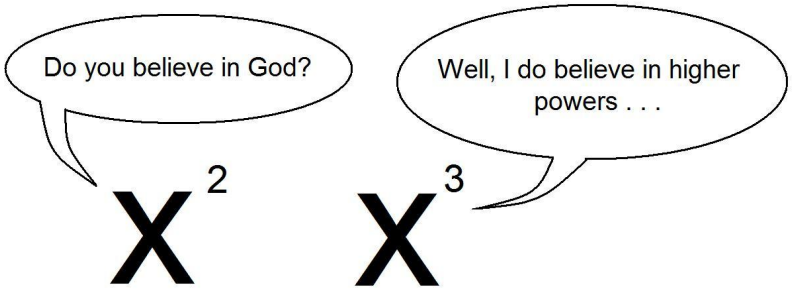
Chapitre 15
Polynômes

Simon Dauguet
simon.dauguet@gmail.com

13 janvier 2026



Les polynômes sont en quelques sortes le couteau suisse des mathématiciens. Ils permettent de tout faire, de tout simplifier et de faire des liens entre pleins de branches des mathématiques.

Les polynômes ont des propriétés algébriques formidables. On va pouvoir faire de l'arithmétique sur les polynômes. On va donc définir une notion de divisibilité qui va fonctionner exactement comme les entiers. On va également montrer que les opérations définis sur les polynômes va munir l'ensemble des polynôme d'une structure d'espace vectoriel. On pourra donc faire de l'algèbre linéaire sur les polynômes (c'est quasi systématique). Mais les polynômes peuvent également être vu comme des fonctions polynomiales. On pourra alors leur appliquer tous les outils analytiques. Par ailleurs, dans les prochains chapitres, on verra qu'on peut approcher (presque) toute fonction par des polynômes, de sorte qu'on pourra toujours approximer une fonction par un bon polynôme au voisinage d'un point (comme vous l'avez déjà vu en physique).

C'est d'ailleurs un raisonnement classique en mathématiques : on commence à établir une nouvelle notion sur les polynômes, puis on l'étend aux fonctions grâce à l'approximation d'une fonction par une suite de polynômes.

Table des matières

Dans l'ensemble de ce cours, on se placera sur un corps $\mathbb{K}$ qui sera soit $\mathbb{R}$ soit $\mathbb{C}$. Les résultats seront donc valables indifféremment sur les deux corps, sauf s'il est précisé, bien sûr.

1 L'algèbre $\mathbb{K}[X]$ des polynômes en une indéterminée

1.1 Généralités

On va commencer par donner une définition abstraite des polynômes. Elle n'est pas indispensable et elle sera peu (voir jamais) utilisée en pratique. Mais elle est utile pour pouvoir faire des distinction de nature d'objet. Il ne faut pas confondre un polynôme, qui est un objet abstrait, avec la fonction polynomiale associée, qui est une fonction.

Les premières définitions que l'on va donner ici sont surtout là pour deux choses : d'abord créer les polynômes à partir de rien et permettre d'en déduire toutes les propriétés que l'on veut ; et ensuite, permettre de bien comprendre que la nature profonde des polynômes est quelque chose de contre-intuitif et donc, de ne pas se faire avoir par les manipulations apparemment simples que l'on va en faire. C'est surtout le deuxième point qui est intéressant. En gardant à l'esprit la première définition des polynômes, on pourra rester vigilant pour éviter d'écrire des choses fausses suggérées par l'intuition et de mieux comprendre les subtilités ultérieures. Le but est donc essentiellement pédagogique.

1.1.1 Premières définitions

Définition 1.1 (Suites presque nulles [✓]) :
Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ une suite à valeurs dans $\mathbb{K}$.

On dit que la suite (a_n) est une suite presque nulle si elle est nulle à partir d'un certain rang, *i.e.* si $\exists n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0$, $a_n = 0$. On a donc

$$(a_n)_{n\in\mathbb{N}} = (a_0, a_1, \dots, a_{n_0-1}, a_{n_0}, 0, 0, \dots)$$

⚠ Attention ! Dans une suite presque nulle (a_n), il peut parfaitement y avoir des 0 dans les premiers termes. L'important étant qu'à partir d'un certain rang, tous les termes doivent être nuls. Mais ça ne dit rien sur les premiers termes. Les premiers termes peuvent prendre toutes les valeurs possibles. Il peut donc en particulier y avoir des 0 qui traînent dans la première partie de la suite.

Exemple 1.1 :
La suite définie par $a_n = n$ pour $0 \leq n \leq 10$ et $a_n = \max(0, 10 - n)$ pour $n \geq 11$ est une suite presque nulle. La suite $b_n = \max(\cos((2n+1)\pi/2), \sin(\frac{3\pi}{2} - \frac{3\pi}{n+1})$ pour tout $n \in \mathbb{N}$ également.

Définition 1.2 (Symbole de Krœnecker [✓]) :
Le symbole de Kroœnecker des entiers p et q, noté $\delta_{p,q}$, est défini par :

$$\forall p, q \in \mathbb{N},\ \delta_{p,q} = \begin{cases} 1 & \text{si } p = q \\ 0 & \text{sinon} \end{cases}$$

Le symbole de Krœnecker est très utile dans les formules. Il sera particulièrement utilisé dans le chapitre sur les matrices. Mais on va en avoir besoin déjà dans ce chapitre.

Définition 1.3 (L'indéterminée) :
On note X la suite $(0, 1, 0, 0, 0, \dots) = (\delta_{1,n})_{n\in\mathbb{N}}$. Par extension, on note $\forall k \in \mathbb{N}$, $X^k = (\delta_{k,n})_{n\in\mathbb{N}} = (0, \dots, 0, 1, 0, 0, \dots)$ avec le 1 en k-ème position. X s'appelle l'indéterminée.

!!! ATTENTION !!!

⚠ L'indéterminé X est donc quelque chose de très spécifique. C'est une suite et pas n'importe quelle suite. On ne peut donc pas "remplacer" X par quoi ce que soit, et surtout pas par un nombre. Ça n'aurait pas de sens de remplacer une suite par un nombre. Ce ne sont pas les mêmes natures d'objets.

Remarque :
La notations X^k qui paraît un peu artificielle pour le moment prendra tout son sens un peu plus tard. On lui donnera sa raison d'être avec la définition des opérations.

Remarque :
Avec cette définition, toute suite presque nulle est une combinaison linéaire des $\{X^k, k \in \mathbb{N}\}$, c'est à dire que si $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle, alors $\exists n_0 \in \mathbb{N}$, tel que $\forall n \geq n_0$, $a_n = 0$ et donc $a = (a_n)_{n\in\mathbb{N}} = (a_0, a_1, \dots, a_{n_0}, 0, 0, \dots) = \sum_{k=0}^{n_0} a_k X^k$.

Définition 1.4 (Polynôme, Ensemble des polynômes [✓]) :

- On appelle polynôme à coefficients dans $\mathbb{K}$ en l'indéterminée X tout objet noté

$$P(X) = \sum_{k=0}^{+\infty} a_k X^k = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \cdots + a_d X^d + \dots$$

  où $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est une suite presque nulle de $\mathbb{K}$.

  La suite (a_n) est la suite des coefficients du polynôme P.
- On note $\mathbb{K}[X]$ l'ensemble des polynôme à coefficients dans $\mathbb{K}$.

Remarque :
La définition d'un polynôme semble problématique à cause de la somme infinie qui n'est pas clairement définie (convergence, existence, condition d'existence, etc...). En fait, comme on considère une suite presque nulle de coefficients, elle ne contient que des zéros à partir d'un certain rang, et donc la somme

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

ne contient que des zéros à partir d'un certain rang et donc est, en réalité, une somme finie.

Donc l'apparence de problème de définition n'est, en fait, qu'apparent et n'existe pas dans la réalité. Il ne faut pas se laisser tromper par les apparences qui sont, bien souvent, trompeuses.

Remarque :
On rappelle que la suite $(a_n)_{n\in\mathbb{N}}$ des coefficients des P est une suite presque nulle. Donc elle est stationnaire en 0 à partir d'un rang d, mais on peut tout de même trouver des zéros dans ces premiers termes. Par exemple, le polynôme $P(X) = X^3 + X - 1$ est un polynôme dont la suite des coefficients est nulle à partir du rang 4 et le coefficient d'indice 2 est nul aussi.

Remarque (Notation) :
Dans la littérature, on peut trouver parfois un polynôme noté P ou $P(X)$, sans, parfois, de distinction claire entre les deux. En fait, il est bon de réserver la simple lettre P lorsque l'on veut parler du polynôme en toute généralité, si l'on veut parler de lui de façon abstraite, en tant qu'individu de l'ensemble $\mathbb{K}[X]$. Mais il vaut mieux l'appeler $P(X)$ dès que l'indéterminée prend de l'importance, c'est à dire quand on veut calculer avec le polynôme. Il faut donc éviter d'écrire $P = \sum_{k=0}^{d} a_k X^k$. C'est désagréable d'avoir une expression dépendant de l'indéterminée X à droite qui est égale à une expression qui ne dépend plus a priori (du moins, moins clairement) de l'indéterminée X. Soit on met des X partout, soit on en met pas. Mais c'est gênant de mélanger les deux.

En d'autres termes, il faut utiliser l'une ou l'autre des notations un peu comme on le ferait avec des fonctions. Soit on utilise f pour parler de l'objet fonctionnelle, soit on écrit $f(x)$ (en définissant x) pour parler de l'expression de f et calculer, factuellement. Il faut faire de même ici, mais avec la particularité que X a déjà une définition précise (c'est l'indéterminé, c'est la suite presque nulle $(\delta_{1,n})_{n\in\mathbb{N}}$).

Cependant, vous croiserez certainement dans la littérature des auteurs qui écriront $P = \sum_{k=0}^{n} a_k X^k$. Ce n'est pas très heureux en fait un confusion entre le polynôme abstrait et son expression. Mais pour éviter des maladresses rédactionnelles ultérieures, il vaut mieux éviter. Si on a les idées très claires (ce qui n'est encore notre cas), on peut le faire. Sinon, il vaut mieux éviter.

!!! ATTENTION !!!

⚠ Il faut prendre garde à la notation ! C'est $\mathbb{K}[X]$ et pas $\mathbb{K}(X)$ ni $\mathbb{K}\{X\}$. Il faut des crochets. Et des crochets simples. Pas $\mathbb{K}[\![X]\!]$. $\mathbb{K}\{X\}$ n'est pas clairement défini, ça ne fait référence à rien de canonique. L'ensemble $\mathbb{K}(X)$ existe et correspond aux fractions rationnelles à coefficients dans $\mathbb{K}$ qui n'est pas au programme. Et $\mathbb{K}[\![X]\!]$ n'existe pas non plus (du moins à ma connaissance) mais $\mathbb{K}[[X]]$ existe et correspond aux sommes formelles à coefficients dans $\mathbb{K}$. Ce n'est pas non plus au programme. Donc faites attention aux notations. Si vous mettez des parenthèses, la majorité de ce que vous écrirez deviendra faux ou n'aura plus de sens.

Exemple 1.2 :
Donner la suite des coefficients des polynômes $2 + X - X^2$ et $X^3 + X - 1$.

Donner les polynômes P_a et P_b dont la suite des coefficients sont (a_n) et (b_n) définies dans l'exemple précédent.

En résumé, un polynôme n'est rien d'autre qu'une suite presque nulle. Un polynôme est une suite particulière. Et l'indéterminée est une suite spécifique à l'intérieur de cet ensemble. Penser aux polynômes en ces termes devrait vous dissuader de donner des valeurs à l'indéterminé X. Ça n'a pas de sens. On ne peut pas donner une valeur particulière à une suite.

!!! ATTENTION !!!

⚠ Il faut bien faire la différence entre X et x. Pour le moment, on introduit X qui est une indéterminée (et que je ne vais pas définir complètement proprement dans ce cours par écrit). On introduira ensuite la variable x. Et ce n'est pas la même chose. L'indéterminée X n'est PAS la variable x, qui n'est pas l'indéterminée X. Il faudra bien faire la distinction entre les deux et j'insisterais beaucoup sur cette distinction.

Remarque :
Il y a d'autres façons de définir les polynômes (et plus particulièrement l'indéterminée X). Mais celle-ci me paraît encore la plus clair et la plus éclairante pour faire la distinction entre X et x.

Remarque :
Dans la mesure où, dans la définition, les polynômes sont des types de suites particulières (les suites presque nulles), certaines opérations vont provenir des opérations sur les suites. Notamment l'addition et la multiplication par un scalaire.

Définition 1.5 (Égalité dans $\mathbb{K}[X]$) :
Soit deux polynômes $P(X) = \sum_{k=0}^{+\infty} a_k X^k$ et $Q(X) = \sum_{k=0}^{+\infty} b_k X^k$ de $\mathbb{K}[X]$ (donc les suites (a_n) et (b_n) sont donc des suites presque nulles.

On dit que P et Q sont égaux si les suites de leurs coefficients sont égales, *i.e.*

$$P = Q \iff \forall n \in \mathbb{N},\ a_n = b_n$$

La notion d'égalité entre polynômes provient donc de la notion d'égalité entre suites. Les polynômes sont un cas particuliers de suites (ce sont des suites presque nulles).

Définition 1.6 (Polynôme constant, Polynôme nul) :

- On appelle polynôme constant de $\mathbb{K}[X]$ un polynôme de la forme $CX^0 = (C, 0, 0, \dots)$ avec $C \in \mathbb{K}$.
- En particulier, on appelle polynôme nul, le polynôme constant égale à 0.

Remarque :
Du coup, au vu de la définition, on fait souvent un amalgame entre un polynôme constant et la valeur de la constante (donc de son coefficient non nul). Ce n'est pas bien. C'est une erreur à strictement parlé. Mais c'est pratique. On en a très envie et ça allège beaucoup les notations. Un peu comme on identifie une fonction constante avec sa valeur.

Autrement dit, par commodité, on identifiera les polynômes constants à leur constante via la bijection (que nous verrons être une forme linéaire) $CX^0 \mapsto C$.

Définition 1.7 (Monôme) :
On appelle monôme de $\mathbb{K}[X]$ tout polynôme de la forme

$$aX^n$$

avec $a \in \mathbb{K}$.

Étymologiquement, "monôme" veut dire un seul "nôme". Les "nôme" sont justement les éléments constitutif de $\mathbb{K}[X]$, c'est à dire les objets de la forme aX^n. Donc un monôme est un seul de ces machins. Et étymologiquement, un "polynôme" est objet composé de plusieurs "nôme", c'est donc un objet de la forme $a_0X^0 + a_1X^1 + \cdots + a_nX^n$ avec plusieurs monôme.

En particulier, les polynômes constants sont des monômes (de la formes aX^0 avec toujours $a \in \mathbb{K}$).

Remarque :
Un polynôme est donc une combinaison linéaire de monôme.

Définition 1.8 (Polynôme pair et polynôme impair) :
Soit $P(X) = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$ un polynôme.

- On dit que P est pair ssi $\forall n \in \mathbb{N}$, $a_{2n+1} = 0$.
- On dit que P est impair ssi $\forall n \in \mathbb{N}$, $a_{2n} = 0$.

Remarque :
On notera que le polynôme nul est à la fois pair et impair. C'est le seul (facile à montrer).

1.1.2 Degré

La notion de degré est aux polynômes ce que la notion de dimension est aux espaces vectoriels de dimension finies.

Définition-Propriété 1.9 (Degré d'un polynôme [✓]) :
Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$.

- Si $P \neq 0$, on appelle degré de P le plus grand entier $d \in \mathbb{N}$ tel que $a_d \neq 0$. On le note $\deg(P)$, *i.e.*

$$\deg(P) = \max\{k \in \mathbb{N},\ a_k \neq 0\}.$$

- Par convention, on note $\deg(0) = -\infty$.

Démonstration :
On suppose $P \neq 0$. On rappelle que si $P(X) = \sum_{k=0}^{+\infty} a_k X^k$ est un polynôme, alors la suite de ses coefficients (a_n) est une suite presque nulle. Comme $P \neq 0$, alors $(a_n) \neq 0$ et donc $\exists n_0 \in \mathbb{N}$ tel que $a_{n_0} \neq 0$. Donc $\{k \in \mathbb{N},\ a_k \neq 0\} \neq \emptyset$.

La suite (a_n) étant une suite presque nulle, donc $\exists d \in \mathbb{N}$ tel que $\forall n \geq d$, $a_n = 0$. On en déduit donc que $\{k \in \mathbb{N},\ a_k \neq 0\}$ est majorée par d.

Donc l'ensemble $\{k \in \mathbb{N},\ a_k \neq 0\}$ est un sous-ensemble non vide et majorée de $\mathbb{N}$, donc il admet un maximum. On note $\deg(P)$ ce maximum. □

!!! ATTENTION !!!

⚠

On ne parle de degré QUE pour des polynômes. Rien d'autres ! (enfin pour nous...) Au même titre que l'on ne parle de dimension QUE pour des espaces vectoriels et rien d'autres.

La convention est là pour assurer un bon fonctionnement des formules qui vont venir par la suite. Comme ça, on n'a pas besoin de se préoccuper (en général) du fait que P soit nul ou pas dans les formules faisant intervenir le degré d'un polynôme.

Cet entier est unique :

Proposition 1.1 (Expression du degré et Unicité du degré) :
Soit $P \in \mathbb{K}[X]$, $P \neq 0$.
Alors $\deg P = \max\{k \in \mathbb{N},\ a_k \neq 0\} = \min\{k \in \mathbb{N}, \forall n > k,\ a_n = 0\}$.
En particulier, le degré est unique pour un polynôme donné.

La démonstration n'est pas très dur. On pourrait l'exprimer autrement. Ces expressions ne sont pas toujours très utiles, mais elles ont l'avantage de justifier que le degré est unique pour un polynôme donné et que l'on peut donc parlé DU degré d'un polynôme.

!!! ATTENTION !!!

⚠ On rappelle qu'un polynôme est essentiellement une suite presque nulle. Donc on peut toujours écrire un polynôme P sout la forme $P(X) = \sum_{k=0}^{d} a_k X^k$. Attention cependant, avec cette notation, cela ne veut pas dire que P est de degré d. Cela veux juste dire que $\deg P \leq d$. Cela veut dire qu'il n'y a pas de terme de degré plus grand que d. Mais pour que le degré de P soit vraiment d, il faut imposer un condition supplémentaire (par exemple $\deg P = d$ ou encore $a_d \neq 0$). On a juste un majorant du degré avec cette notation.

Définition 1.10 ($\mathbb{K}_n[X]$ [✓]) :
Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur à n, *i.e.*

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X],\ \deg(P) \leq n\}.$$

Définition 1.11 (Coefficient dominant, Coefficient constant [✓]) :
Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ un polynôme non nul de degré $d \in \mathbb{N}$.

- On appelle coefficient dominant de P le coefficient a_d de X^d. C'est donc le dernier coefficient non nul.
- On appelle coefficient constant de P le coefficient a_0 devant X^0.

Remarque :
On pourra noter $\operatorname{coeff}\operatorname{dom}(P)$ le coefficient dominant de P. Mais attention ! Cette notation n'a rien de canonique. C'est la mienne. Que j'utilise parce que c'est pratique. Et parce qu'elle est transparente et parfaitement compréhensible. Mais ce n'est pas une notation standard. Il est possible que l'on vous la reproche si vous l'utilisez.

Exemple 1.3 :
Déterminer $\deg(X^3 + X^2 - 1)$ et $\deg(aX + b)$ en fonction de a et b deux éléments de $\mathbb{K}$ ainsi que leurs coefficients dominants et constants.

Remarque (Caractérisation des polynômes constants) :
Les polynômes de degré 0 sont très exactement les polynômes constants non nuls.

Définition 1.12 (Polynôme unitaire [✓]) :
Soit $P \in \mathbb{K}[X]$, $P \neq 0$.
On dira que P est unitaire si $\operatorname{coeff}\operatorname{dom}(P) = 1$.

Remarque :
En particulier, tout polynôme unitaire est non nul. Forcément puisqu'il a un coefficient qui est 1 donc non nul... (et ce coefficient doit être son coefficient dominant)

Exemple 1.4 :
Le polynôme $X^n - 1$ est unitaire pour tout $n \in \mathbb{N}^*$. Mais le polynôme $1 - X^n$ ne l'est pas.

1.1.3 Opérations sur $\mathbb{K}[X]$ et structure algébrique

Nous allons définir dans cette partie toutes les opérations qui existent entre polynômes. Il va y en avoir 4 (5 sur $\mathbb{C}[X]$).

1.1.3.1 Structure d'espace vectoriel

Définition-Propriété 1.13 (Combinaison linéaire) :
Soit $P(X) = \sum_{n=0}^{+\infty} a_n X^n, Q(X) = \sum_{n=0}^{+\infty} b_n X^n \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

- On définit le polynôme $P + Q$ de $\mathbb{K}[X]$ par

$$(P+Q)(X) = \sum_{n=0}^{+\infty} (a_n + b_n) X^n$$

- On définit le polynôme λP de $\mathbb{K}[X]$ par

$$(\lambda P)(X) = \sum_{n=0}^{+\infty} (\lambda a_n) X^n$$

Démonstration :
Il faut montrer que $P + Q$ et λP sont bien des polynômes à coefficients dans $\mathbb{K}$, càd qu'il faut montrer que la suite de leurs coefficients sont des suites presque nulles de $\mathbb{K}$.

Soit $n_P, n_Q \in \mathbb{N}$ tel que $\forall n \geq n_P$, $a_n = 0$ et $\forall n \geq n_Q$, $b_n = 0$ (attention, ce ne sont que des majorants du degré). Alors $\forall n \geq n_P$, $\lambda a_n = 0$ donc la suite $(\lambda a_n) = \lambda(a_n)$ est une suite presque

nulles de $\mathbb{K}$. Et $\forall n \geq \max(n_P, n_Q)$, on a $a_n + b_n = 0 + 0 = 0$. Donc la suite $(a_n) + (b_n) = (a_n + b_n)$ est également une suite presque nulle. □

Remarque :
En fait, ce qu'on sous-entend, c'est que l'ensemble des suites presque nulles de $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel. Et comme cet ensemble "est" l'ensemble des polynômes ...

Exemple 1.5 :
Déterminer le polynôme $(2 + X + X^2) + (X^3 + X - 1)$ et $2 \cdot (X^2 - 1)$.

Théorème 1.2 ($\mathbb{K}[X]$ est un $\mathbb{K}$-ev [✓]) :
$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel dont l'élément neutre est le polynôme nul

On a donc les relations

1. $\forall P, Q \in \mathbb{K}[X]$, $P + Q \in \mathbb{K}[X]$, $\forall \lambda \in \mathbb{K}$, $\lambda P \in \mathbb{K}[X]$.
2. $\forall P, Q \in \mathbb{K}[X]$, $P + Q = Q + P$
3. $\exists E \in \mathbb{K}[X]$, $\forall P \in \mathbb{K}[X]$, $P + E = E + P = P$ (ici E est le polynôme nul).
4. $\forall P \in \mathbb{K}[X]$, $\exists Q \in \mathbb{K}[X]$, $P + Q = Q + P = E$.
5. $\forall P, Q, R \in \mathbb{K}[X]$, $(P + Q) + R = P + (Q + R) = P + Q + R$
6. $\forall P \in \mathbb{K}[X]$, $1 \cdot P = P$
7. $\forall \lambda, \mu \in \mathbb{K}$, $\forall P \in \mathbb{K}[X]$, $(\lambda + \mu)P = \lambda P + \mu P$
8. $\forall \lambda \in \mathbb{K}$, $\forall P, Q \in \mathbb{K}[X]$, $\lambda(P + Q) = \lambda P + \lambda Q$.
9. $\forall \lambda, \mu \in \mathbb{K}$, $\forall P \in \mathbb{K}[X]$, $\lambda(\mu P) = (\lambda\mu)P$

Démonstration :

1. Déjà fait dans la définition 1.13.
2. Soit $P, Q \in \mathbb{K}[X]$,

$$(P + Q)(X) = \sum_{n=0}^{+\infty} (a_n + b_n)X^n = \sum_{n=0}^{+\infty} (b_n + a_n)X^n = (Q + P)(X)$$

car l'addition est commutative dans $\mathbb{K}$. (On aurait pu dire aussi que $(\mathbb{K}[X], +)$ est un sous-groupe du groupe abélien $(\mathbb{K}^{\mathbb{N}}, +)$ mais ce n'est pas au programme).

3. Soit $P \in \mathbb{K}[X]$. On note E le polynôme nul. Alors
$$(P+E)(X) = \sum_{k=0}^{+\infty}(a_k+0)X^k = \sum_{k=0}^{+\infty} a_k X^k = P(X)$$
et $E+P=P$ est vérifiée automatiquement par commutativité de l'addition dans $\mathbb{K}[X]$.
4. Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k$. Alors la suite $(-a_n)$ est une suite presque nulle de $\mathbb{K}$ donc on peut considérer le polynôme $Q(X) = \sum_{k=0}^{+\infty} -a_k X^k$ associé. Et $(P+Q)(X) = \sum_{k=0}^{+\infty}(a_k - a_k)X^k = \sum_{k=0}^{+\infty} 0 \cdot X^k = E(X)$. De même pour l'autre identité par commutativité de l'addition.
5. On prend $P(X) = \sum_{k=0}^{+\infty} a_k X^k$, $Q(X) = \sum_{n=0}^{+\infty} b_n X^n$, $R(X) = \sum_{n=0}^{+\infty} c_n X^n$. Alors, par définition de la somme de deux polynômes, $((P+Q)+R)(X) = \sum_{n=0}^{+\infty}((a_n+b_n)+c_n)X^n = \sum_{n=0}^{+\infty}(a_n+b_n+c_n)X^n = \sum_{n=0}^{+\infty}(a_n+(b_n+c_n))X^n = (P+(Q+R))(X)$.
6. Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. Alors $1 \cdot P(X) = \sum_{k=0}^{+\infty}(1 \cdot a_k)X^k = \sum_{k=0}^{+\infty} a_k X^k = P(X)$.
7. Soit $\lambda, \mu \in \mathbb{K}$ et $P(X) = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. Alors $(\lambda+\mu)P(X) = \sum_{k=0}^{+\infty}(\lambda+\mu)a_k X^k = \sum_{k=0}^{+\infty}(\lambda a_k + \mu a_k)X^k = \lambda P(X) + \mu P(X)$ et il est clair que les suites en présences sont toutes des suites presque nulles.
8. Soit $\lambda \in \mathbb{K}$ et $P(X) = \sum_{k=0}^{+\infty} a_k X^k, Q(X) = \sum_{k=0}^{+\infty} b_k X^k \in \mathbb{K}[X]$. Alors $\lambda(P(X)+Q(x)) = \lambda(P+Q)(X) = \sum_{k=0}^{+\infty}\lambda(a_k+b_k)X^k = \sum_{k=0}^{+\infty}(\lambda a_k + \lambda b_k)X^k = \lambda P(X) + \lambda Q(X)$ avec que des suites presque nulles partout.
9. soit $\lambda, \mu \in \mathbb{K}$ et $P(X) = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. Alors $\lambda(\mu P(X)) = \lambda\left(\sum_{k=0}^{+\infty} \mu a_k X^k\right) = \sum_{k=0}^{+\infty}\lambda(\mu a_k)X^k = \sum_{k=0}^{+\infty}(\lambda\mu)a_k X^k = (\lambda\mu)P(X)$. Ici encore, les suites sont des suites presque nulles.

(Ouf !) □

Proposition 1.3 (Degré de λP [✓]) :
On a :
$$\forall P \in \mathbb{K}[X],\ \forall \lambda \in \mathbb{K},\ \deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases}$$

Démonstration :
Si $\lambda = 0$, alors $\lambda P = 0$ et donc $\deg(\lambda P) = -\infty$. Si $\lambda \neq 0$ et $P = 0$, alors $\lambda P = 0$ et donc $\deg(\lambda P) = -\infty = \deg P$. Si $\lambda \neq 0$ et $P(X) = \sum_{k=0}^{\deg P} a_k X^k$ avec $\deg P \geq 0$, on a $\lambda P(X) = \sum_{k=0}^{\deg P} \lambda a_k X^k$. Mais, par définition de $\deg P$, $a_{\deg P} \neq 0$, donc $\lambda a_{\deg P} \neq 0$. Donc $\deg(\lambda P) = \deg P$. □

Proposition 1.4 (Degré d'une somme de polynômes [✓]) :
Soit $P, Q \in \mathbb{K}[X]$. Alors

$$\deg(P+Q) \leq \max(\deg P, \deg Q).$$

De plus :

$$\deg(P+Q) = \max(\deg P, \deg Q) \iff \begin{cases} \deg(P) \neq \deg(Q) \\ \text{ou} \\ \begin{cases} \deg(P) = \deg(Q) \\ \text{coeff dom}(P) + \text{coeff dom}(Q) \neq 0 \end{cases} \end{cases}$$

Démonstration :
On pose $P(X) = \sum_{k=0}^{p} a_k X^k$ et $Q(X) = \sum_{k=0}^{q} b_k X^k$ avec $p = \deg P$ et $q = \deg Q$. Sans perte de généralité, on peut supposer $\deg P \leq \deg Q$. Alors $(P+Q)(X) = \sum_{k=0}^{p} a_k X^k + \sum_{k=0}^{q} b_k X^k = \sum_{k=0}^{p}(a_k + b_k)X^k + \sum_{k=p+1}^{q} b_k X^k$. Si $\deg P < \deg Q$, alors $\deg(P+Q) = q = \max(\deg P, \deg Q)$.

Et si $\deg P = \deg Q$, alors $(P+Q)(X) = \sum_{k=0}^{p}(a_k + b_k)X^k$ donc $\deg(P+Q) \leq \deg P$ selon si $a_p + b_p = 0$ ou non. □

Remarque :
Si $\deg P = \deg Q$ et que les coefficients dominants de P et Q s'annulent, alors

$$\deg(P+Q) < \max(\deg P, \deg Q)$$

Exemple 1.6 :
Déterminer le degré de $P+Q$ avec $P(X) = X^3 - X + 1$ et $Q(X) = X^2 - X^3 - 1$.

Proposition 1.5 :
Soit $n \in \mathbb{N}$. Alors $\mathbb{K}_n[X]$ est un sev de $\mathbb{K}[X]$.

Démonstration :
Il suffit d'utiliser la caractérisation des sev. Ce n'est pas très dur avec ce qui a été fait précédemment. □

Remarque :
En fait, $\mathbb{K}_n[X]$ est un $\mathbb{K}$-ev de dimension finie, mais on le reverra plus tard.

1.1.3.2 L'anneau $(\mathbb{K}[X], +, \times)$

On définit maintenant un produit sur $\mathbb{K}[X]$:

Définition-Propriété 1.14 (Produit de polynômes [✓]) :
Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k$ et $Q(X) = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbb{K}[X]$.
On définit le polynôme $PQ \in \mathbb{K}[X]$ par

$$PQ(X) = \sum_{k=0}^{+\infty} c_k X^k$$

où $\forall n \in \mathbb{N}$,

$$c_n = \sum_{\substack{p,q\in\mathbb{N}\\ p+q=n}} a_p b_q = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0.$$

Démonstration :
Il faut montrer que PQ tel qu'il est définit est bien un polynôme, c'est-à-dire que la suite des ses coefficients est une suite presque nulle.

On sait $\exists n \in \mathbb{N}$ et $\exists m \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k \geq n$ et $b_j = 0$ pour tout $j \geq m$. En prenant $k > n + m$, alors

$$c_k = \sum_{j=0}^{k} a_j b_{k-j} = \sum_{j=0}^{n} a_j b_{k-j} + \sum_{j=n+1}^{k} a_j b_{k-j} = 0$$

En effet, si $0 \leq j \leq n$, alors $m < k - j \leq k$ donc $b_{k-j} = 0$ et si $n + 1 \leq j \leq k$, on a $a_j = 0$. Donc (c_k) est une suite nulle à partir de $n + m$, donc c'est une suite presque nulle et donc PQ est bien un polynôme de $\mathbb{K}[X]$. □

Remarque :
On vient en particulier de montrer que $\deg(PQ) \leq n + m = \deg P + \deg Q$.

Remarque :
On définit une nouvelle opération sur les suites presque nulles. Qui est une multiplication différente de celle définie sur les suites génériques. Sur $\mathbb{K}^{\mathbb{N}}$ on a définie une multiplication terme à terme. Ici, on

définit une nouvelle multiplication qui est plutôt une sorte de développement pour coïncider avec ce qu'il se passe sur $\mathbb{R}$ avec des produits de sommes. Sur les suites presque nulles, c'est cette nouvelle multiplication qui va être intéressante, même si l'autre fonctionne toujours. Elle aura simplement moins d'intérêt car moins cohérente avec la structure polynomiale.

Exemple 1.7 :
Déterminer le polynôme $(2 + X - X^2)(X^3 + X - 1)$.

Proposition 1.6 (Produit de monôme) :
$\forall p, q \in \mathbb{N}$,

$$X^p \times X^q = X^{p+q}$$

Démonstration :
Pour les besoins de cette démo, on utilise le symbole de Kronecker dont on rappel la définition.

$$\forall p, q \in \mathbb{N},\ \delta_{p,q} = \begin{cases} 1 & \text{si } p = q \\ 0 & \text{sinon} \end{cases}$$

Alors $X^p = \sum_{k=0}^{+\infty} \delta_{k,p} X^k$ et $X^q = \sum_{k=0}^{+\infty} \delta_{k,q} X^k$. Alors $X^p \times X^q = \sum_{k=0}^{+\infty} c_k X^k$ avec $\forall k \in \mathbb{N}$,

$$c_k = \sum_{i=0}^{k} \delta_{i,p} \delta_{k-i,q}$$

Or

$$\begin{aligned} \delta_{i,p}\delta_{k-i,q} \neq 0 &\iff \begin{cases} i = p \\ k - i = q \end{cases} \\ &\iff \begin{cases} i = p \\ k = p + q \end{cases} \end{aligned}$$

Donc $c_k \neq 0 \iff k = p + q$. Et dans ce cas, $c_{p+q} = \sum_{i=0}^{p+q} \delta_{i,p}\delta_{p+q-i,q} = \delta_{p,p}\delta_{q,q} = 1$. Donc $X^p \times X^q = 1 \times X^{p+q} = X^{p+q}$. □

Remarque :
Cette démo vient donc de justifier a posteriori la notation pour la suite presque nulle $X^k = (0, \dots, 0, 1, 0, \dots)$. On a bien

$$X^k = \underbrace{X \times X \times \cdots \times X}_{k}.$$

Proposition 1.7 (Degré d'un produit de polynômes [✓]) :

$$\forall P, Q \in \mathbb{K}[X],\ \deg(PQ) = \deg P + \deg Q$$

Démonstration :
D'abord, par la définition du produit polynomiale, il est facile de voir que si $P = 0$ ou $Q = 0$, alors $PQ = 0$ et donc $\deg(PQ) = -\infty = \deg(P) + \deg(Q)$. On suppose donc $P \neq 0$ et $Q \neq 0$.

On pose $n = \deg P$ et $m = \deg Q$ et $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$. Alors $PQ(X) = \sum_{k=0}^{d} c_k X^k$ avec $c_k = \sum_{p+q=k} a_p b_q$ et $d = \deg(PQ)$. Or on a vu que $c_k = 0$ pour tout $k > n + m$. Donc $\deg PQ \leq n + m$ puisque $\deg(PQ)$ est le minimum de $\{k \in \mathbb{N}, \forall j \geq k, c_j = 0\}$. Et $c_{n+m} = \sum_{i=0}^{n+m} a_i b_{n+m-i} = \sum_{i=0}^{n} a_i b_{n+m-i} = a_n b_m \neq 0$. Donc $\deg(PQ) = n + m$. □

Démonstration :
Déterminer le degré de $(2 + X - X^2)(X^3 + X - 1)$ de l'exemple précédent. □

Théorème 1.8 ($(\mathbb{K}[X], +, \times)$ est un anneau.) :
$(\mathbb{K}[X], +, \times)$ est un anneau commutatif, munit de ses deux LCI, dont l'élément neutre pour le produit polynomial est le polynôme constant égal à 1. Le produit polynomial est bilinéaire (*i.e.* $(\mathbb{K}[X], +, \times, \cdot\ )$ est une $\mathbb{K}$-algèbre commutative).

An d'autres termes :

1. $\forall P, Q \in \mathbb{K}[X],\ PQ \in \mathbb{K}[X]$ [*LCI*]
2. $\forall P, Q, R \in \mathbb{K}[X],\ \forall \lambda, \mu \in \mathbb{K},\ (\lambda P + \mu Q)R = \lambda PR + \mu QR$ [*Linéarité à gauche*]
3. $\forall P, Q, R \in \mathbb{K}[X],\ \forall \lambda, \mu \in \mathbb{K},\ P(\lambda Q + \mu R) = \lambda PQ + \mu PR$ [*Linéarité à droite*]
4. $\forall P, Q \in \mathbb{K}[X],\ PQ = QP$ [*Commutativité*]
5. $\exists U \in \mathbb{K}[X],\ \forall P \in \mathbb{K}[X],\ UP = PU = P$ (où $U = 1 \in \mathbb{K}[X]$) [*Élément neutre*]
6. $\forall P, Q, R \in \mathbb{K}[X],\ (PQ)R = P(QR) = PQR$ [*Associativité*]

Démonstration :

1. Déjà fait dans la définition du produit de deux polynômes.
2. C'est un jeu d'écriture. On pose $P(X) = \sum_{k=0}^{p} a_k X^k$, $Q(X) = \sum_{k=0}^{q} b_k X^k$ et $R(X) = \sum_{k=0}^{r} c_k X^k$. On a alors $(\lambda P + \mu Q)R(X) = \sum_{k=0}^{+\infty} d_k X^k$ où $d_k = \sum_{j=0}^{k} (\lambda a_j + \mu b_j) c_{k-j} = \lambda \sum_{j=0}^{k} a_j c_{k-j} + \mu \sum_{j=0}^{k} b_j c_{j-k}$. Donc $(\lambda P + \mu Q)R = \lambda PR + \mu QR$.
3. On fait exactement la même chose.

4. Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ deux polynômes à coefficients dans $\mathbb{K}$ de degré n et m respectivement. Alors $QP(X) = \sum_{k=0}^{m+n} d_k X^k$ avec $d_k = \sum_{p+q=k} b_p a_q = \sum_{q+p=k} a_q b_p = c_k$ où $PQ(X) = \sum_{k=0}^{n+m} c_k X^k$. Donc $PQ = QP$
5. On va montrer que le produit de polynôme admet un élément neutre qui est le polynôme contant égal à 1. On note U le polynôme constant égal à 1. Donc $U(X) = \sum_{k=0}^{+\infty} \delta_{0,k} X^k = 1X^0 = 1$. Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ de degré n. Alors $UP(X) = \sum_{k=0}^{n+0} c_k X^k$ avec $c_k = \sum_{p+q=k} \delta_{0,p} a_q = a_k$ donc $UP = P$. Et la commutativité se charge de l'autre identité.
6. Soit $P(X) = \sum_{k=0}^{\alpha} a_k X^k$, $Q(X) = \sum_{k=0}^{\beta} b_k X^k$ et $R(X) = \sum_{k=0}^{\gamma} c_k X^k$ trois polynômes de $\mathbb{K}[X]$. Alors $QR(X) = \sum_{k=0}^{\beta+\gamma} d_k X^k$ où $d_k = \sum_{i+j=k} b_i c_j$ et $(P(QR))(X) = \sum_{k=0}^{\alpha+\beta+\gamma} e_k X^k$ où $e_k = \sum_{p+q=k} a_p d_q$. On note enfin $(PQ)(X) = \sum_{k=0}^{\alpha+\beta} f_k X^k$ où $f_k = \sum_{i+j=k} a_i b_j$ et $((PQ)R)(X) = \sum_{k=0}^{\alpha+\beta+\gamma} g_k X^k$ où $g_k = \sum_{p+q=k} f_p c_q$. Alors

$$\begin{aligned} e_k &= \sum_{p+q=k} a_p d_q \\ &= \sum_{p+q=k} a_p \left(\sum_{i+j=q} b_i c_j \right) \\ &= \sum_{p+q=k} \sum_{i+j=q} a_p b_i c_j \\ &= \sum_{p+i+j=k} a_p b_i c_j \\ &= \sum_{q+j=k} c_j \left(\sum_{p+i=q} a_p b_i \right) \\ &= \sum_{q+j=k} c_j f_q \\ &= g_k \end{aligned}$$

D'où la relation.

□

Théorème 1.9 (Binôme de Newton) :
Soit $P, Q \in \mathbb{K}[X]$. Comme $\mathbb{K}[X]$ est commutatif (au sens de la multiplication polynomiale), on a :

$$\forall n \in \mathbb{N},\ (P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}$$

!!! ATTENTION !!!

⚠ On a déjà vu que le binôme de Newton ne fonctionne pas tous le temps. Ici ça marche bien. Mais ce n'est pas parce qu'il y a un polynôme qui apparaît que ça fonctionnera bien. Par exemple, si f et g sont des endomorphismes d'un ev E, alors on ne peut rien dire, en toute généralité, en ce qui concerne le développement de $(\widetilde{P}(f)+\widetilde{P}(g))^n$! !

Comme $\mathbb{K}[X]$ est un anneau, il y a donc le groupe des inversibles.

Exemple 1.8 :
Le polynôme X n'est pas inversible.

!!! ATTENTION !!!

⚠ La notion d'inversibilité dépend évidemment de la définition de l'opération que l'on considère, mais également de l'ensemble dans lequel on se place.

Par exemple, on a une multiplication dans $\mathbb{Z}$. 2 n'est pas inversible dans $\mathbb{Z}$ mais a un inverse dans $\mathbb{Q}$ (et donc dans $\mathbb{R}$ aussi).

Proposition 1.10 (Polynômes inversibles [✓]) :
Les polynômes inversibles de $\mathbb{K}[X]$ pour la multiplication sont les polynômes constants non nuls, *i.e.* $\mathbb{K}[X]^\times = \mathbb{K}^*$.

Autrement dit, l'ensemble des polynômes inversibles est $\mathbb{K}_0[X]\setminus\{0\}$ que l'on identifie à $\mathbb{K}\setminus\{0\}$ via la forme linéaire bijective (donc l'isomorphisme) $\mathbb{K}_0[X]\to\mathbb{K}$ canonique défini par $CX^0\mapsto C$.

Démonstration :
Soit $C\in\mathbb{K}^*$. Alors $\frac{1}{C}\in\mathbb{K}^*$ et $C\times\frac{1}{C}=1$. Donc le polynôme C est inversible.

Réciproquement, soit $P\in\mathbb{K}[X]$ un polynôme inversible. Donc $\exists Q\in\mathbb{K}[X]$ tel que $PQ=1$. Alors $0=\deg 1=\deg P+\deg Q$. Mais $\deg P,\deg Q\in\mathbb{N}\cup\{-\infty\}$. Donc $\deg P=\deg Q=0$. Ce sont donc des constantes non nuls. □

Corollaire 1.11 ($\mathbb{K}[X]$ est intègre [✓]) :
Il n'y a pas de diviseurs de 0 dans $\mathbb{K}[X]$, *i.e.* :

$$\forall P, Q \in \mathbb{K}[X],\ \Big(PQ = 0 \iff P = 0 \text{ ou } Q = 0\Big)$$

Vous le pressentez, on appelle diviseurs de 0, un élément pour lequel il existe un autre élément dont le produit vaut 0 (*i.e.* on dit que P est un diviseur de 0 si $\exists Q \in \mathbb{K}[X]$ tq $PQ = 0$). Il existe des ensembles dans lesquels ça existe. Ce n'est pas gagné à priori d'avoir la propriété du dessus.

Démonstration :
Le sens indirecte est évident.

On va démontrer la réciproque par contraposée. Supposons que $P, Q \in \mathbb{K}[X]\backslash\{0\}$. Donc $\deg P \geq 0$ et $\deg Q \geq 0$. Alors $\deg PQ = \deg P + \deg Q \geq 0$. Donc $\deg PQ \neq -\infty$ et donc $PQ \neq 0$. □

1.1.3.3 Composition de polynômes

Définition-Propriété 1.15 (Composition de polynôme [✓]) :
Soit $P, Q \in \mathbb{K}[X]$ avec $P(X) = \sum_{k=0}^{d} a_k X^k$ de degré d.
On définit alors le polynôme $P \circ Q$ par

$$P \circ Q = \sum_{k=0}^{d} a_k Q^k \in \mathbb{K}[X]$$

La puissance étant à comprendre en tant que produit ici.

Autrement dit,

$$P \circ Q(X) = P(Q(X)) = \sum_{k=0}^{d} a_k Q(X)^k$$

Démonstration :
Il faut montrer qu'on obtient un polynôme, c'est à dire que la suite des coefficients de $P \circ Q$ est presque nulle.

On a $P \circ Q = \sum_{k=0}^{d} a_k Q^k$. Or on sait que $\forall k \in \mathbb{N}$, $Q^k \in \mathbb{K}[X]$. Et comme $\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel, il est stable par combinaison linéaire, donc $\sum_{k=0}^{d} a_k Q^k$ est un polynôme. □

Remarque :
On voit plusieurs choses. D'abord, l'outil des espaces vectoriels est un outil très efficace. On le

savait déjà, mais on enfonce le clou. Une fois qu'on s'est fatigué à montrer qu'un ensemble avait la structure d'espace vectoriel, ça simplifie énormément pas mal de calcul ultérieur (voir carrément les rend inutiles) et démontre tout un tas de propriétés d'un seul coup, sans avoir besoin de calculer quoi que ce soit.

D'autre part, on voit qu'on fait des compositions. Or cette opération est normalement réservé aux fonctions. Mais pour le moment ce n'est qu'une notation pour une nouvelle opération sur $\mathbb{K}[X]$. On verra par la suite (partie 1.2 page 25) que c'est cohérent avec ce qu'il se passe pour les fonctions polynomiales ce qui justifiera *a posteriori* cette notation. Mais ne pas confondre pour autant les polynômes avec des indéterminés X et les fonctions polynômiales qui seront d'une variable x.

!!! ATTENTION !!!

La composition n'est pas commutative. Donc $P \circ Q \neq Q \circ P$ même si les deux existes.

Proposition 1.12 (Degré de la composée de deux polynômes [✓]) :
Soit $P, Q \in \mathbb{K}[X]$, $Q \neq 0$.

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

Démonstration :
Supposons que $P = 0$. Alors bien sûr, $P \circ Q = 0$ et donc la formule est vrai. Supposons donc que $P \neq 0$.

On pose $P(X) = \sum_{k=0}^{\deg P} a_k X^k$. Alors $P \circ Q = \sum_{k=0}^{\deg P} a_k Q^k$. Mais $\deg Q^k = \underbrace{\deg Q + \deg Q + \cdots + \deg Q}_{k} = k \deg Q$. Donc $\deg P \circ Q = \deg P \deg Q$, car $\forall k \in \mathbb{N}$, $\deg Q^k < \deg Q^{k+1}$ et $a_{\deg P} \neq 0$ (et degré d'une somme de polynômes). □

Exemple 1.9 :
Déterminer $P \circ Q$ avec $P(X) = 2 + X - X^2$ et $Q(X) = X^3 + X - 1$. Déterminer également $R(X^2)$ et $R(X)^2$ si $R(X) = \sum_{k=0}^{r} a_k X^k$.

Remarque :
Si $Q = 0$, alors $P \circ Q = a_0$, le coefficient constant de P, qui est de degré 0 ou $-\infty$ selon que $a_0 \neq 0$ ou non.

Proposition 1.13 (Caractérisation de la parité d'un polynôme) :
Soit $P \in \mathbb{K}[X]$.

(i) P est paire si et seulement si $P(-X) = P(X)$.

(ii) P est impaire si et seulement si $P(-X) = -P(X)$.

où $P(-X)$ est la composée du polynôme P par le polynôme $-X$.

Donc la notion de parité qu'on a introduite auparavant (1.8 p.8) est cohérente avec celle que l'on connaissait déjà.

Démonstration :

(i) On démarre de ce que l'on veut montrer :

$$\begin{aligned} P(-X) = P(X) &\iff \sum_{k=0}^{+\infty} a_k X^k = \sum_{k=0}^{+\infty} (-1)^k a_k X^k \\ &\iff \sum_{k=0}^{+\infty} (1-(-1)^k) a_k X^k = 0 \\ &\iff \forall k \in \mathbb{N},\ (1-(-1)^k) a_k = 0 \\ &\iff \forall k \in \mathbb{N},\ 2a_{2k+1} = 0 \\ &\iff P \text{ pair} \end{aligned}$$

(ii) On fait pareil pour l'imparité.

□

Proposition 1.14 (Propriété algébrique de la LCI $\circ$ [✓]) :
La loi de composition interne $\circ$ sur $\mathbb{K}[X]$ vérifie :

1. $\forall P, Q, R \in \mathbb{K}[X],\ (PQ) \circ R = (P \circ R)(Q \circ R)$ [*Distributivité de $\circ$ sur $\times$ à gauche*]
2. $\forall P, Q, R \in \mathbb{K}[X],\ \forall \lambda, \mu \in \mathbb{K},\ (\lambda P + \mu Q) \circ R = \lambda P \circ R + \mu Q \circ R.$ [*La composition est linéaire à gauche*]

Démonstration :

1. On pose $P(X) = \sum_{k=0}^{+\infty} a_k X^k$, $Q(X) = \sum_{k=0}^{+\infty} b_k X^k$ et $R(X) = \sum_{k=0}^{+\infty} c_k X^k$. On pose également $PQ(X) = \sum_{k=0}^{+\infty} d_k X^k$ avec $d_k = \sum_{i=0}^{k} a_i b_{k-i}$. Alors $(PQ) \circ R = \sum_{k=0}^{+\infty} d_k R^k$. D'autre part, $P \circ R = \sum_{k=0}^{+\infty} a_k R^k$ et $Q \circ R = \sum_{k=0}^{+\infty} b_k R^k$. Alors $(P \circ R) \times (Q \circ R) = \sum_{k=0}^{+\infty} d_k R^k$. D'où l'égalité.
2. $(\lambda P + \mu Q) \circ R = \sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) R^k = \sum_{k=0}^{+\infty} \lambda a_k R^k + \sum_{k=0}^{+\infty} \mu b_k R^k = \lambda P \circ R + \mu Q \circ R$.

□

Remarque :
Autrement dit,

$$\begin{array}{ccc} \mathbb{K}[X] \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ (P, Q) & \mapsto & P \circ Q \end{array}$$

est linéaire par rapport à la variable de gauche. Mais pas la variable de droite.

Exemple 1.10 :
On prend $P(X) = 2 + X - X^2$ et $Q(X) = X^3 + X - 1$ et $R(X) = X + 1$. Calculer $(PQ) \circ R$ et $(3P - 2Q) \circ R$.

1.1.3.4 Conjugaison complexe

Dans $\mathbb{C}$, vous savez qu'on dispose d'une opération supplémentaire qui est la conjugaison complexe. On va donc regarder ce que ça fait sur les polynômes.

Définition 1.16 (Polynôme conjugué) :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$.
On appelle polynôme conjugué de P le polynôme

$$\overline{P}(X) = \sum_{k=0}^{n} \overline{a_k} X^k \in \mathbb{C}[X]$$

Proposition 1.15 (Conjugaison et opérations) :
Soit $P, Q \in \mathbb{C}[X]$ et $\lambda, \mu \in \mathbb{C}$. Alors

1. $\overline{\overline{P}} = P$ [*Involution*]
2. $\overline{\lambda P + \mu Q} = \overline{\lambda}\,\overline{P} + \overline{\mu}\overline{Q}$
3. $\overline{PQ} = \overline{P}\,\overline{Q}$
4. $\overline{P \circ Q} = \overline{P} \circ \overline{Q}$

Démonstration :
Je n'oserais vous faire l'affront de l'écrire. □

!!! ATTENTION !!!

⚠ On rappelle que la conjugaison n'est PAS linéaire ! ! Mais la conjugaison est sesquilinéaire. Vous reverrez cette notion dans le chapitre sur les espaces hermitiens en deuxième année.

Proposition 1.16 (Caractérisation des polynômes réels par leur conjugué) :
Soit $P \in \mathbb{C}[X]$. On a

$$P \in \mathbb{R}[X] \iff P = \overline{P}$$

Démonstration :
Facile □

Remarque :
On peut faire une caractérisation des polynômes imaginaires purs aussi de la même façon. Mais ils nous intéresseront moins a priori. On peut la faire tout de même et donc il est possible de l'utiliser, si besoin est.

1.2 Fonctions polynomiales

Attention, il va y avoir dans ce paragraphe des distinctions assez subtiles du point de vue philosophique. Elles sont nécessaires. Et vitales. Et elles proviennent directement de la définition (première) des polynômes.

Définition 1.17 (Évaluation d'un polynôme [✓]) :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme et $\alpha \in \mathbb{K}$. On appelle valeur de P en α, ou évaluation de P en α, le scalaire $\sum_{k=0}^{n} a_k \alpha^k$.

Définition 1.18 (Fonctions polynomiales [✓]) :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme. On définit la fonction polynomiale associée à P sur $\mathbb{K}$, notée $\widetilde{P}$, définie par

$$\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \sum_{k=0}^{n} a_k x^k \end{array}$$

!!! ATTENTION !!!

⚠ A strictement parlé, $\widetilde{P} \neq P$. Ce n'est pas le même objet. P est polynôme. C'est une suite presque nulle. Alors que $\widetilde{P}$ est une fonction. Ce n'est pas le même objet. Néanmoins, on peut créer une fonction à partir d'un polynôme. On l'appelle $\widetilde{P}$. Mais ce n'est plus un polynôme. C'est une fonction polynomiale. Ne pas confondre les deux.

Remarque :
L'amalgame entre un polynôme et sa fonction polynomiale associée étant très tentante, elle sera souvent faite en deuxième année. Et pourtant, vous devrez tout de même savoir différencier les deux. Vous pourrez simplement passer de l'un à l'autre sans le préciser, mais sans confondre les deux (donc ne pas confondre les manipulations et les théorèmes qu'on le droit d'appliquer).

Cet amalgame sera précisé dans les sujets. Attention, si ce n'est pas préciser, vous ne pourrez pas le faire. La phrase usuelle pour permettre cet amalgame est "On identifiera un polynôme P de $\mathbb{K}[X]$ à la fonction polynomiale associée sur $\mathbb{R}$". Ou une autre phrase similaire.

On insistera pour cette année, puisque le programme demande de faire la distinction et que, si la distinction n'est pas claire, au moment où on s'autorisera de faire ces amalgames en sachant utiliser les propriétés des uns et des autres sans se tromper et en les différenciant, les choses risquent de s'embrumer. Ce n'est pas parce qu'on écrit plus la distinction qu'il ne faut pas savoir la faire. La distinction sera toujours faite, mais on ne précisera plus qu'on l'a fait.

Exemple 1.11 :
La fonction polynomiale associée au polynôme X^2+1 de $\mathbb{R}[X]$ est la fonction

$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2+1 \end{array}$$

Remarque :
En fait, pour fabriquer la fonction polynomiale, on récupère l'information essentielle du polynôme, c'est-à-dire les coefficients d'une combinaison linéaire. Par définition, un polynôme est essentiellement des coefficients d'une combinaison linéaire finie. On peut alors considérer ces coefficients dans n'importe quel espace vectoriel et transporté cette combinaison linéaire dans cet ev. Les coefficients étant les même, on appelle alors polynôme d'un vecteur (pour peu qu'on puisse donner un sens à X^n) cette combinaison linéaire dans ce nouvel ev.

Ce processus de fabrication est classique. On l'utilise très régulièrement. Et pas nécessairement dans ce sens là. On l'a d'ailleurs déjà utilisé dans un exo. À partir d'une combinaison linéaire de vecteur, on peut extraire la suite des coefficients et du coup, fabriquer le polynôme dont la suite de coefficients correspond à la suite des coefficients de la combinaison linéaire.

Définition 1.19 (Fonction évaluation) :
On définit les fonctions évaluations pour tout $\alpha \in \mathbb{K}$, notée ev_α par

$$\mathrm{ev}_\alpha : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P(X) & \mapsto & \widetilde{P}(\alpha) \end{array}$$

Remarque :
L'application ev_α est linéaire. C'est très facile à vérifier.

Remarque :
On notera que $\widetilde{P}(0)$ est le coefficient constant de P. On peut faire d'autres petites remarques relativement évidentes de ce genre là.

Proposition 1.17 (Opérations et fonctions polynomiales) :
On a

1. $\forall P,Q \in \mathbb{K}[X]$, $\forall \lambda,\mu \in \mathbb{K}$, $\widetilde{\lambda P+\mu Q} = \lambda\widetilde{P}+\mu\widetilde{Q}$ [*Linéarité*]
2. $\forall P,Q \in \mathbb{K}[X]$, $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$
3. $\forall P,Q \in \mathbb{K}[X]$, $\widetilde{P\circ Q} = \widetilde{P}\circ\widetilde{Q}$

Démonstration :
Il suffit de l'écrire □

Compte tenu de ces relations, on peut définir une application

$$\begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{F}(\mathbb{K},\mathbb{K}) \\ P & \mapsto & \widetilde{P} \end{array}$$

cette application est compatible avec toutes les opérations sur $\mathbb{K}[X]$ (on peut dire que c'est un homomorphisme d'algèbre, mais encore une fois, cette structure algébrique est HP).

Remarque :
En particulier, en prenant un peu d'avance sur les prochains chapitres, on vient de montrer que

$$\begin{array}{ccc} \mathbb{R}[X] & \to & \mathcal{C}^\infty(\mathbb{R},\mathbb{R}) \\ P & \mapsto & \widetilde{P} \end{array}$$

est une application linéaire (entre les deux $\mathbb{R}$-ev). Il est facile de voir que cette application est injective (l'étude du noyau est facile). En revanche, elle n'est pas du tout surjective. Par exemple $\exp$ n'a pas d'antécédent par cette application. Ni le cosinus.

La conséquence dramatique est que cette application n'a pas de réciproque. Et donc :

!!! ATTENTION !!!

⚠ On ne peut pas passer d'une fonction à un polynôme ! Même si l'expression de la fonction ressemble à une fonction polynomiale. Il faut poser un polynôme et vérifier que la fonction polynomiale associée correspond à la fonction qu'on étudie. C'est une partie des problèmes de rédaction classiques et c'est ce qui rend les copies intéressantes. Ou pas.

Définition 1.20 (Racine d'un polynôme [✓]) :
Soit $P \in \mathbb{K}[X]$ un polynôme. On appelle racine de P tout scalaire $a \in \mathbb{K}$ tel que $\widetilde{P}(a) = 0$.

!!! ATTENTION !!!

⚠ La notion de racine d'un polynôme dépend du corps que l'on considère. Par exemple, le polynôme X^2+1 est dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$, mais il n'a pas de racines dans $\mathbb{R}$ (en tant que polynôme de $\mathbb{R}[X]$) alors qu'il en a 2 dans $\mathbb{C}$ (en tant que polynôme de $\mathbb{C}[X]$).

Ces distinctions seront l'objet de la dernière section. Il y a des différences notables avec lesquelles il faut savoir jouer.

Exemple 1.12 :
Déterminer les racines du polynôme X^n-1 dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Proposition 1.18 (Conjugué et évaluation) :
Soit $P\in\mathbb{C}[X]$ et $a\in\mathbb{C}$. Alors
$$\overline{\widetilde{P}(a)}=\overline{\widetilde{P}}(\overline{a})=\widetilde{\overline{P}}(\overline{a})$$

Démonstration :
Là encore, il suffit d'écrire les définition et de passer aux conjugués □

Remarque :
L'ordre dans lequel on conjugue (et ce qu'on conjugue, la nature de l'objet que l'on conjugue) n'a finalement que peu d'influence. Que l'on conjugue un complexe (évaluation d'un polynôme), ou que l'on conjugue l'évaluation d'un polynôme en un conjugué, ou encore que l'on évalue le conjugué d'un polynôme en un conjugué d'un complexe, on obtient à chaque fois le même résultat.

Dans le premier cas, c'est une conjugaison dans $\mathbb{C}$ classique, que l'on sait faire depuis le début d'année ; dans le second, on commence par considérer l'application associée à P, on la conjugue en tant qu'applications ; dans le troisième cas, c'est la fonction polynomiale associée au polynôme conjugué de P que l'on considère. Et conjugué l'image, ou la fonction polynomiale ou le polynôme, c'est pareil.

Définition 1.21 (Polynôme d'endomorphisme d'un ev) :
Soit E un $\mathbb{K}$-ev et $f \in \mathcal{L}(E)$. On définit une application

$$\begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & \widetilde{P}(f) \end{array}$$

où, si $P(X) = \sum_{k=0}^{n} a_k X^k$, $\widetilde{P}(f) = \sum_{k=0}^{n} a_k f^k$ au sens de la composition d'endomorphisme.

On verra d'autres évaluation polynomiale. En fait, dès qu'on a un espace vectoriel munit d'une autre LCI (jouant le rôle de multiplication) entre vecteur pour pouvoir donner un sens à la puissance n-ème d'un vecteur, on peut définir une application de $\mathbb{K}[X]$ dans cet ensemble.

Exemple 1.13 :
On prend $E = \mathbb{R}^3$ et l'application $f(x,y,z) = (y+z, x+z, x+y)$. Calculer alors $\widetilde{P}(f)$ pour $P(X) = X^2 - X - 2$. Que peut-on en déduire sur f ?

Remarque :
Si $f \in \mathcal{L}(E)$, un polynôme $P \in \mathbb{K}[X]$ tel que $\widetilde{P}(f) = 0$ s'appelle un polynôme annulateur de f. Ils vont jouer un rôle important dans la suite.

Proposition 1.19 (Propriété algébrique de l'application $\mathbb{K}[X] \to \mathcal{L}(E)$ [✓]) :
Soit E un $\mathbb{K}$-ev et $f \in \mathcal{L}(E)$.
L'application

$$\begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & \widetilde{P}(f) \end{array}$$

est une application linéaire vérifiant
(i) $\forall P, Q \in \mathbb{K}[X]$, $\widetilde{PQ}(f) = \widetilde{P}(f) \circ \widetilde{Q}(f)$
(ii) $\forall P, Q \in \mathbb{K}[X]$, $\widetilde{P \circ Q}(f) = \widetilde{P}(\widetilde{Q}(f))$

!!! ATTENTION !!!

⚠ Le sens de l'évaluation d'un polynôme et les opérations qu'on a le droit de lui faire dépend bien évidemment de la nature de l'objet sur lequel est évalué le polynôme. Autrement dit, les opérations possibles sur $\widetilde{P}(f)$ ne sont pas les mêmes si $f \in \mathcal{L}(E)$, $f \in \mathbb{K}$ etc.
En particulier, on notera que $\widetilde{PQ}(f)$ est une composition si $f \in \mathcal{L}(E)$ et un produit (un vrai) si $f \in \mathbb{K}$. Il y a une ambiguïté sur l'opération qui est levée automatiquement par la nature de f. Il faut donc être délicat ici.

Remarque :
Dans cette propriété, on fixe $f \in \mathcal{L}(E)$ et on fait varier $P \in \mathbb{K}[X]$. Mais on pourrait faire l'inverse : on pourrait fixer $P \in \mathbb{K}[X]$ et faire varier $f \in \mathcal{L}(E)$ dans l'évaluation $\widetilde{P}(f)$. Autrement dit, on pourrait regarder l'application $f \mapsto \widetilde{P}(f)$ où $P \in \mathbb{K}[X]$ est fixé.

Ces deux applications donnent naturellement naissance à des applications qui vont de $\mathcal{L}(E)$ dans un ensemble d'applications ou de $\mathbb{K}[X]$ dans un autre ensemble d'applications, selon si c'est

$f \in \mathcal{L}(E)$ ou $P \in \mathbb{K}[X]$ qui est fixé en premier dans $\widetilde{P}(f)$.

Autrement dit, on pourrait également définir une application

$$\begin{array}{ccc} \mathcal{L}(E) & \to & \mathcal{L}\Big(\mathbb{K}[X], \mathcal{L}(E)\Big) \\ f & \mapsto & \Big(P \mapsto \widetilde{P}(f)\Big) \end{array}$$

et montrer qu'elle est également linéaire, puis voir les propriétés qu'elle a par rapport à la composition etc. C'est un bon exercice. Ce n'est pas excessivement difficile mais c'est surtout un problème de notation.

De la même manière, on peut faire le même genre de jeu sur

$$\begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{F}\Big(\mathcal{L}(E), \mathcal{L}(E)\Big) \\ P & \mapsto & \Big(f \mapsto \widetilde{P}(f)\Big) \end{array}$$

et essayer de voir les propriétés.

On peut même définir une application

$$\begin{array}{ccc} \mathbb{K}[X] \times \mathcal{L}(E) & \to & \mathcal{L}(E) \\ (P, f) & \mapsto & \widetilde{P}(f) \end{array}$$

mais elle serait un peu moins intéressante.

Proposition 1.20 (Factorisation de Hörner) :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ avec $n \in \mathbb{N}$. Alors

$$P(X) = ((\dots(((a_n X + a_{n-1})X + a_{n-2})X + a_{n-3})\dots)X + a_1)X + a_0$$

Démonstration :
On va démontrer le résultat par récurrence sur le degré de P. Si P est nul ou une constante, c'est évident. Si P est de degré 1, aussi.

Si $P(X) = aX^2 + bX + c$, $a, b, c \in \mathbb{K}$ et $a \neq 0$. Alors $P(X) = X(aX + b) + c$.

Supposons que la factorisation de Hörner fonctionne pour tout polynôme de degré $\leq n$. Prenons $P(X) = \sum_{k=0}^{n+1} a_k X^k$ un polynôme de degré $n+1$. Alors

$$\begin{aligned} P(X) &= \sum_{k=0}^{n+1} a_k X^k \\ &= X\left(\sum_{k=1}^{n+1} a_k X^{k-1}\right) + a_0 \\ &= X\left(\sum_{k=0}^{n} a_{k+1} X^k\right) + a_0 \end{aligned}$$

Or $\sum_{k=0}^{n} a_{k+1} X^k$ est un polynôme de degré n, donc par principe de récurrence, il peut se factoriser avec la factorisation de Hörner. Et donc P également, compte tenu de la forme de la première factorisation de P. □

La factorisation de Hörner permet de minimiser le nombre d'opérations nécessaire dans l'évaluation d'un polynôme. Naïvement, pour calculer $\widetilde{P}(x_0)$, on a besoin $\frac{d(d+1)}{2} + d + d$ opérations, où $d = \deg(P)$. Avec la méthode de Hörner, on aura (toujours naïvement) seulement $d + d$ opérations. Ce qui permet d'améliorer grandement la complexité des algorithmes utilisant des évaluations polynomiales.

Voir les TD d'info de début d'année pour des algorithmes permettant d'obtenir l'écriture d'un polynômes avec la factorisation de Hörner.

1.3 Dérivations

On va commencer ici par définir une "dérivation" dans $\mathbb{K}[X]$. Ce n'est pas une dérivation au sens fonctionnelle. C'est une nouvelle opération dans $\mathbb{K}[X]$. Mais on se rendra compte que cette opération coïncide avec la dérivation fonctionnelle (classique). D'où le choix de la terminologie.

Évidemment, il ne faudra pas confondre les deux.

1.3.1 Dérivée polynomiale première

Définition 1.22 (Dérivée formelle [✓]) :
Soit $P(X) = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ un polynôme.

On appelle polynôme dérivé de P le polynôme, noté P', défini par

$$P'(X) = \begin{cases} \sum_{k=1}^{d} k a_k X^{k-1} = \sum_{k=0}^{d-1} (k+1) a_{k+1} X^k & \text{si } \deg(P) \geq 1 \\ 0 & \text{si } \deg(P) \leq 0 \end{cases}$$

Exemple 1.14 :
Déterminer le polynôme dérivé de $3X^3 + X^2 - 5$.

Proposition 1.21 (Degré et dérivé [✓]) :
Soit $P \in \mathbb{K}[X]$.

Alors $\deg(P') \leq \deg P - 1$. Plus précisément, on a

$$\deg(P') = \begin{cases} -\infty & \text{si } \deg P \leq 0 \\ \deg P - 1 & \text{si } \deg P \geq 1 \end{cases}$$

Démonstration :
Ça vient de l'expression de P'. Si P est constant, alors $P(X) = \sum_{k=0}^{0} a_k X^k$. Donc P' est le polynôme

nul. Et si P est non constant, alors il est de degré $n \in \mathbb{N}^*$ et $a_n \neq 0$ et $P(X) = \sum_{k=0}^{n} a_k X^k$. Dans ce cas, $P'(X) = \sum_{k=0}^{n-1}(k+1)a_{k+1}X^k$ et $na_n \neq 0$. Donc P' est de degré $n-1 = \deg P - 1$. □

Corollaire 1.22 (Caractérisation des polynômes constants par les dérivés) :
Soit $P \in \mathbb{K}[X]$.

$$P \text{ constant} \iff P' = 0$$

Démonstration :
On vient de voir le sens direct. Il manque juste la réciproque.

Supposons donc $P' = 0$. Or si $P(X) = \sum_{k=0}^{+\infty} a_k X^k$, on a $P'(X) = \sum_{k=1}^{+\infty} k a_k X^{k-1}$. Donc $\forall k \geq 1$, $ka_k = 0$, c'est à dire $\forall k \geq 1$, $a_k = 0$ et donc $P(X) = a_0 \in \mathbb{K}_0[X] \approx \mathbb{K}$. Donc P est constant (éventuellement nul). □

Proposition 1.23 (Dérivation et opérations) :
La dérivation vérifie :

1. $\forall P, Q \in \mathbb{K}[X]$, $\forall \lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$ *[La dérivation est linéaire]*
2. $\forall P, Q \in \mathbb{K}[X]$, $(PQ)' = P'Q + PQ'$ *[Formule de Leibniz]*

Démonstration :
Exercice. Il suffit d'écrire chacun des polynômes qui interviennent avec leurs coefficients, puis les dériver et voir que les formules sont vraies. □

Remarque :
Avec le premier point et le fait que $\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel, on a :

$$D : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & P' \end{array}$$

est un endomorphisme de $\mathbb{K}[X]$.

Autrement dit, $D \in \mathcal{L}(\mathbb{K}[X])$. C'est en ces termes qu'il faut le retenir.

En fait, grâce au résultat sur le degré de la dérivé, la dérivation D est même un endomorphisme

de $\mathbb{K}_n[X]$.

Proposition 1.24 (Et avec beaucoup de polynôme) :
Soit $n \in \mathbb{N}^*$ et $P_1, \dots, P_n \in \mathbb{K}[X]$. Alors

$$\left(\prod_{k=1}^{n} P_k\right)' = \sum_{k=1}^{n} \left(P_k' \prod_{\substack{1 \leq i \leq n \\ i \neq k}} P_i\right)$$

et en particulier,

$$(P^n)' = nP' \times P^{n-1}$$

Démonstration :
Il suffit de faire une petite récurrence pour le premier et de faire $P_1 = \cdots = P_n = P$ pour avoir la deuxième relation. □

Corollaire 1.25 (Dérivé d'une composée de polynôme) :
Soit $P, Q \in \mathbb{K}[X]$.

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

Démonstration :
Là encore c'est un jeu d'écriture. Il suffit d'écrire P et Q en fonctions de leurs coefficients, et dérivé $P \circ Q$ grâce à la proposition précédente (on connaît la dérivé de Q^k). □

⚠ Vous remarquerez que ces formules sont les mêmes que la dérivation de fonction qu'on a vu dans le chapitre précédent. Cependant, ATTENTION ! ! Ce ne sont pas des fonctions, mais des polynômes. Il faudrait des $\tilde{}$ pour avoir des fonctions. Cette dérivation ne correspond donc pas à celle du chapitre précédent. Il n'y a pas ici de limite. La définition n'est pas la même. On aurait donc pas du appeler ça comme ça. Attention donc. Le type de la dérivation que vous utilisez (et donc sa définition intrinsèque qui dépend de limite ou juste d'une relation entre coefficients) dépend du type des objets que vous dérivez.

Définition 1.23 (Polynôme primitif (HP ?)) :
Soit $P \in \mathbb{K}[X]$.
On appelle polynôme primitif de P tout polynôme $Q \in \mathbb{K}[X]$ tel que $Q' = P$.

⚠ ATTENTION ! Il n'y a pas de primitive ici. La notion de primitive est réservée aux fonctions. Elle dépend de la notion de dérivée avec des limite. On ne parle ici que de polynôme primitif. C'est à dire de polynôme ayant une certaine propriété qui est celle de la définition.

Proposition 1.26 (Ensemble des polynômes primitifs (HP ?)) :
Tout polynôme $P \in \mathbb{K}[X]$ admet au moins un polynôme primitif $Q \in \mathbb{K}[X]$ et l'ensemble de ses polynômes primitifs est constitué des polynômes de la forme $Q + c$ avec $c \in \mathbb{K}$, *i.e.* $\{Q + c, c \in \mathbb{K}\} = Q + \mathbb{K}$.

Démonstration :
Il suffit de faire le lien avec les équations différentielles linéaire d'ordre 1 □

1.3.2 Dérivation polynomiale d'ordre supérieure

On a déjà introduit

$$D : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & P' \end{array}$$

On peut donc considérer ses itérés $D^0 = \mathrm{Id}_{\mathbb{K}[X]}$, $D^1 = D$ et $D^n = \underbrace{D \circ D \circ \cdots \circ D}_{n}$.

Définition 1.24 (Dérivée n-ème d'un polynôme) :
Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.
Le polynôme dérivé de P d'ordre n est le polynôme $P^{(n)} = D^n(P)$.

C'est donc le polynôme dérivé de P par la dérivation polynomiale appliquée n-fois successive à P.

Remarque :
En particulier, $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = (P')' = P''$ etc.

Proposition 1.27 (Degré d'une dérivée d'ordre n) :
Soit $P \in \mathbb{K}[X]$. Alors :

1. $\forall n > \deg P$, $\deg P^{(n)} = -\infty$
2. $\forall n \leq \deg P$, $\deg P^{(n)} = \deg P - n$.

Autrement dit $\forall n > \deg P$, $P^{(n)} = 0$ puisque le polynôme nul est le seul polynôme de degré $-\infty$.

Démonstration :
Petite récurrence sur n. □

Proposition 1.28 (Dérivée d'une combinaison linéaire et d'un produit) :
On a les relations :

1. $\forall P, Q \in \mathbb{K}[X]$, $\forall \lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$ *[Linéarité]*
2. $\forall P, Q \in \mathbb{K}[X]$, $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$ *[Formule de Leibniz]*

Démonstration :
Le premier point s'obtient soit en faisant une récurrence sur n, soit en utilisant la linéarité de D (pour plus tard). Et le second point est essentiellement la même démo que la formule de Leibniz du chapitre précédent. □

Exemple 1.15 ([✓]) :
Exprimer $P_n^{(k)}$ pour tout $k, n \in \mathbb{N}$ où $\forall n \in \mathbb{N}$, $P_n(X) = X^n$.

Proposition 1.29 (Expression de la dérivée n-ème [✓]) :
Soit $P(X) = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$, alors

$$\forall n \in \{0, \dots, d\},\ P^{(n)}(X) = \sum_{k=n}^{d} a_k \frac{k!}{(k-n)!} X^{k-n} = \sum_{k=0}^{d-n} a_{n+k} \frac{(n+k)!}{k!} X^k$$

Démonstration :
La démo vient directement de la linéarité de la dérivation, de la composition de la dérivation et de l'exemple précédent avec le calcul de dérivée n-ème des monômes. □

1.3.3 Formule de Taylor

Théorème 1.30 (Formule de Taylor pour les polynômes [✓]) :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors

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

Ce théorème est fondamentale. On le reverra dans le chapitre suivant.

On donne ici une démonstration qui n'utilise que ce qu'il y a pour le moment dans ce cours. Par la suite, on pourra le démontré en quelques lignes seulement. On aura des outils (d'algèbre linéaire encore et toujours) très efficace qui nous permettrons de gagner beaucoup de temps et d'énergie.

Démonstration :
On donne une démo ne faisant appel qu'aux nouvelles notions polynomiales.

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Si $P = 0$, il n'y a rien à faire puisque $\forall n \in \mathbb{N}$, $P^{(n)} = 0$. On suppose donc $P \neq 0$. On pose $d = \deg P \geq 0$. Donc $\forall k \geq d+1$, $P^{(k)} = 0$ et donc $Q(X) = \sum_{k=0}^{+\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k = \sum_{k=0}^{d} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k \in \mathbb{K}[X]$.

Mais $\forall i \in \{0,\dots,d\}$, $P^{(i)}(X) = \sum_{k=i}^{d} a_k \frac{k!}{(k-i)!}X^{k-i}$. Donc :

$$\begin{aligned}
Q(X) &= \sum_{i=0}^{d} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^i \\
&= \sum_{i=0}^{d} \left(\left(\sum_{k=i}^{d} a_k \frac{k!}{(k-i)!} a^{k-i} \right) \frac{(X-a)^i}{i!} \right) \\
&= \sum_{i=0}^{d} \sum_{k=i}^{d} a_k \frac{k!}{i!(k-i)!} a^{k-i}(X-a)^i \\
&= \sum_{k=0}^{d} \left(a_k \sum_{i=0}^{k} \binom{k}{i} a^{k-i}(X-a)^i \right) \\
&= \sum_{k=0}^{d} a_k (X-a+a)^k \\
&= \sum_{k=0}^{d} a_k X^k \\
&= P(X)
\end{aligned}$$

□

On pourrait donner une démo d'algèbre linéaire, mais il nous manque quelques petits détails pour pouvoir le faire sans trop de douleur.

Remarque :
Par un petit changement de variable pas dur, on peut écrire la formule de Taylor sous la forme :

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

Corollaire 1.31 (Expression des coefficients avec les dérivées [✓]) :
Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. Alors

$$\forall n \in \mathbb{N},\ a_n = \frac{\widetilde{P^{(n)}}(0)}{n!}$$

Démonstration :
Il suffit d'appliquer la formule de Taylor en 0. □

Exemple 1.16 :
Soit le polynôme $P(X) = X^5 - (3+2i)X^4 + (5-i)X + 2$. Déterminer $\widetilde{P^{(4)}}(0)$ et $\widetilde{P^{(2)}}(1)$ sans calculé la dérivée de P.

Remarque :
On notera que cette relation est vraie pour tous les entiers. Dès que n dépassera le degré de P, les coefficients sont nuls, mais les dérivées également. Donc c'est cohérent.

1.3.4 Dérivée et fonction polynomiale

Théorème 1.32 (Dérivée polynomiale et dérivée fonctionnelle coïncident [✓]) :
Si $P \in \mathbb{K}[X]$, alors

$$\widetilde{(P')} = \left(\widetilde{P}\right)'$$

Autrement dit, la fonction polynomiale du polynôme dérivée coïncide avec la dérivée de la fonction polynomiale. Et c'est tant mieux. Ce qui justifie, a posteriori, la notation et le choix des termes.

Démonstration :
On va faire la démo pour $P(X) = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ avec $d \geq 1$. Soit $\alpha \in \mathbb{K}$ et $x \in \mathbb{K}$ avec $x \neq \alpha$.

$$\begin{aligned}
\tau_{\widetilde{P}}(x,\alpha) &= \frac{\widetilde{P}(x) - \widetilde{P}(\alpha)}{x-\alpha} \\
&= \frac{1}{x-\alpha} \sum_{k=1}^{d} a_k (x^k - \alpha^k) \\
&= \sum_{k=1}^{d} \left(a_k \sum_{i=0}^{k-1} x^i \alpha^{k-i-1} \right)
\end{aligned}$$

Donc

$$\begin{aligned}
\frac{\widetilde{P}(x) - \widetilde{P}(\alpha)}{x-\alpha} \xrightarrow[x\to\alpha]{} & \sum_{k=1}^{d} \left(a_k \sum_{i=0}^{k-1} \alpha^{k-1} \right) \\
&= \sum_{k=1}^{d} k a_k \alpha^{k-1} \\
&= \widetilde{(P')}(\alpha)
\end{aligned}$$

car $x \mapsto \sum_{k=1}^{d} a_k \sum_{i=0}^{k-1} x^i \alpha^{k-i-1}$ est une fonction polynomiale donc continue sur $\mathbb{K}$.
Si $d = 1, 0$, c'est encore plus facile. Et si $P = 0$, on s'ennuie.
Donc $\left(\widetilde{P}\right)' = \widetilde{(P')}$. □

Cette proposition est possible sur $\mathbb{K}$ car on sait maintenant dériver des fonctions à valeur complexe.

Exemple 1.17 :
Avec le polynôme $P(X) = X^3 - 2X^2 + 1$, on a $\widetilde{(P')}(x) = \widetilde{(P)}'(x)$.

1.4 Le cas de $\mathbb{K}_n[X]$ (algèbre linéaire)

Définition 1.25 (Famille de polynômes échelonnée en degré [✓]) :
Soit $P_1, \dots, P_n \in \mathbb{K}[X]$. On dit que la famille $(P_1, \dots, P_n)$ est échelonnée en degré si $\forall i \in \{1, \dots, n-1\}$, $\deg P_i < \deg P_{i+1}$.

Exemple 1.18 :
La famille $(1, X, X^2, \dots, X^n)$ est échelonnée en degré. Cette famille est la base canonique de $\mathbb{K}_n[X]$.

La famille $((1+X)^k, k = 2, \dots, 5)$ est échelonnée en degré. Tout comme la famille $(1, X^2, (1+X)^3, (2+X+X^2)^3, (2+(1+X^2)^2+(1+X^2)^3)^2)$.

Proposition 1.33 (Liberté de famille échelonnée en degré [✓]) :
Soit $(P_0, \dots, P_n)$ une famille de polynôme de $\mathbb{K}[X]$ échelonnée en degré avec $\deg P_0 \geq 0$.
Alors $(P_0, \dots, P_n)$ est une famille libre.

On peut démontrer cette proposition par récurrence ou directement. On va faire les deux.

Démonstration (Récurrence) *:*
D'abord, pour $n = 0$, on ne considère qu'un polynôme non nul, donc il est forcément libre.

Supposons que toute famille de $n+1$ polynôme échelonnée en degré soit libre, pour un certain $n \geq 0$. Soit alors $(P_0, \dots, P_{n+1})$ une famille de $n+2$ polynôme échelonnée en degré avec $P_0 \neq 0$. Soit $\lambda_0, \dots, \lambda_{n+1} \in \mathbb{K}$ tels que $\sum_{k=0}^{n+1} \lambda_k P_k = 0$. On pose également, $\forall i \in \{0, \dots, n+1\}$, $d_i = \deg(P_i)$. Donc $0 \leq d_0 < d_1 < \cdots < d_n < d_{n+1}$.

C'est encore un polynôme. On peut le dériver plusieurs fois. Par exemple, on a

$$\left(\sum_{k=0}^{n+1} \lambda_k P_k\right)^{(d_0+1)} = \sum_{k=0}^{n+1} \lambda_k P_k^{(d_0+1)} = \sum_{k=1}^{n+1} \lambda_k P_k^{(d_0+1)}$$

par linéarité de la dérivation et puisque $\deg(P_0) = d_0 < d_0 + 1$. Et par ailleurs, $\forall i \in \{1, \dots, n+1\}$, $\deg(P_i^{(d_0+1)}) = d_i - d_0 - 1$. Donc la famille $(P_1^{(d_0+1)}, \dots, P_{n+1}^{(d_0+1)})$ est une famille de $n+1$ polynômes non nuls échelonnée en degré et est donc libre par hypothèse de récurrence. On en déduit donc $\lambda_1 = \cdots = \lambda_{n+1} = 0$.

Ce qui nous amène à $\lambda_0 P_0 = 0$. Mais comme $P_0 \neq 0$, on en déduit également $\lambda_0 = 0$ et donc la famille est libre. □

Démonstration (Direct) *:*

On reprend une famille $(P_0, \dots, P_n)$ de polynômes non nuls échelonnée en degré et $\lambda_0, \dots, \lambda_n \in \mathbb{K}$ tels que $\sum_{k=0}^{n} \lambda_k P_k = 0$. On pose encore $d_k = \deg(P_k)$ pour $0 \leq k \leq n$. On en déduit donc, par dérivation successive,

$$\left(\sum_{k=0}^{n} \lambda_k P_k\right)^{(d_n)} = \sum_{k=0}^{n} \lambda_k P_k^{(d_n)} = \lambda_n P_n^{(d_n)} = 0$$

par linéarité de la dérivation et puisque, $\forall k \in \{0, \dots, n-1\}$, $d_k < d_n$. On en déduit donc $\lambda_n = 0$ puisque $P_n^{(d_n)} = d_n! \operatorname{coeff} \operatorname{dom}(P_n) \in \mathbb{K}^*$. (Ici aussi, on pourrait alors entamer une autre récurrence). On a donc $\sum_{k=0}^{n-1} \lambda_k P_k = 0$. Puis en dérivant d_{n-1} fois, on trouve alors $\lambda_{n-1} = 0$. En réitérant ce processus $n+1$ fois, on aboutit à $\lambda_0 = \cdots = \lambda_n = 0$ et la famille est donc libre. □

Définition 1.26 ($\mathbb{K}_n[X]$ Ensemble des polynômes de degré $\leq n$ [✓]) :
Pour tout $n \in \mathbb{N}$, on pose $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur ou égale à n, *i.e.*

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X], \deg P \leq n\}$$

En particulier $\mathbb{K}_0[X] = \{P \in \mathbb{K}[X], \deg P \leq 0\}$ est isomorphe à $\mathbb{K}$.

Proposition 1.34 (Structure de l'ensemble des polynômes de $\deg \leq n$ [✓]) :
Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est un sous $\mathbb{K}$-ev de $\mathbb{K}[X]$ de dimension finie dont $(1, X, \dots, X^n)$ est la base canonique et donc

$$\dim \mathbb{K}_n[X] = n + 1$$

Démonstration :
On sait déjà que $\mathbb{K}[X]$ est un $\mathbb{K}$-ev. Il suffit donc d'appliquer la caractérisation des sev. Laissé en exercice.

Par ailleurs, on sait que

$$\mathbb{K}_n[x] = \{P \in \mathbb{K}[X], \deg P \leq n\} = \left\{\sum_{k=0}^{n} a_k X^k, a_0, \dots, a_n \in \mathbb{K}\right\} = \operatorname{Vect}_{\mathbb{K}}(1, X, \dots, X^n)$$

(ce qui prouve également la structure d'ev). Donc la famille $(1, X, \dots, X^n)$ est une famille génératrice de $\mathbb{K}_n[X]$. Par ailleurs, c'est une famille échelonnée en degré de polynômes non nuls, donc elle est libre. C'est donc une base de $\mathbb{K}_n[X]$. □

Exemple 1.19 :
On considère la famille $P_0(X) = 2$, $P_1(X) = 3X - 1$, $P_2(X) = (X-1)^2$ et $P_3(X) = X^2(X+1)$. Montrer que (P_0, P_1, P_2, P_3) est une base de $\mathbb{K}_3[X]$.

⚠ Attention ! La multiplication n'est pas une loi de composition interne sur $\mathbb{K}_n[X]$. Le résultat n'est pas (toujours) dans $\mathbb{K}_n[X]$. La cause en est la formule du degré d'un produit.

Remarque :
Tout polynôme est dans un certain $\mathbb{K}_n[X]$. En effet, si on considère $P \in \mathbb{K}[X]$, alors il existe $n \in \mathbb{N}$ tel que $P \in \mathbb{K}_n[X]$. Il suffit de prendre $n \geq \deg P$. On a même $P \in \mathbb{K}_n[X]$ pour tout $n \geq \deg P$.

Remarque ("Identifications des coefficients") :
On sait maintenant à quoi correspond "l'identification des coefficients" que vous utilisiez plus jeune. Elle correspond en fait à la liberté de la base canonique de $\mathbb{K}_n[X]$. Il faudra le dire en ces termes. Et ne plus utilisez ce mot-valise qui n'a pas grand sens.

On peut utiliser l'isomorphisme

$$\begin{array}{rccc} \varphi : & \mathbb{K}_n[X] & \to & \mathbb{K}^{n+1} \\ & \sum_{k=0}^{n} a_k X^k & \mapsto & (a_0, a_1, \ldots, a_n) \end{array}$$

C'est un isomorphisme par théorème de l'isomorphisme (utiliser la même dimension et le noyau, ou le fait que $(1, X, \ldots, X^n)$ est une base de $\mathbb{K}_n[X]$). Cet isomorphisme permet de réduire un polynôme à la seul information de ses coefficients. Et à partir du n-uplet, on peut utilisez ce que l'on sait de $\mathbb{K}^{n+1}$. (Cet isomorphisme sera largement utilisé dans les chapitres ultérieurs).

Dit autrement, si on a $P(X) = Q(X)$, on se place $\mathbb{K}_{\max(\deg(P),\deg(Q)}[X]$ qui est un ev de dimension finie. Si on pose $N = \max(\deg(P), \deg(Q))$ et (a_p) et (b_q) la suite des coefficients de P et Q, alors on a $P(X) - Q(X) = 0$ et donc $\sum_{k=0}^{N}(a_k - b_k)X^k = 0$. La liberté de la base canonique de $\mathbb{K}_N[X]$ nous permet d'avoir alors immédiatement $\forall k \in \{0, \ldots, N\}$, $a_k = b_k$. C'est ce qui se passe quand on utilise "l'identification des coefficients".

Remarque :
On a donc en particulier $\mathbb{K}_0[X]$ isomorphe à $\mathbb{K}$. On a donc tendance à "étendre" l'isomorphisme et noté $\mathbb{K}$ encore les éléments de $\mathbb{K}_0[X]$ (ce qui, a strictement parlé, n'est pas très correct, mais qu'on a quand même déjà utilisé plusieurs fois par soucis de simplification de notations).

Exemple 1.20 :
On considère l'application f définie par $f(P)(X) = P(X+1) + P(X+2) - 2P(X)$. Montrer que $f \in \mathcal{L}(\mathbb{R}_3[X])$. Donner une base de $\ker(f)$ et calculer $\mathrm{rg}(f)$.

2 Arithmétique des polynômes

Dans cette partie, on va apprendre à manipuler vraiment les polynômes. On va voir en fait qu'ils se comportent un peu comme les entiers, c'est-à-dire qu'on va introduire une notion de polynôme irréductible (l'équivalent des nombres premiers), de division euclidienne ce qui va nous permettre de faire de l'arithmétique (lemme de Gauss etc) et aussi de décomposer un polynôme en produit de polynôme irréductible. Cette étape est cruciale pour la suite (et plus particulièrement pour l'année prochaine et la réduction des endomorphismes qui nécessitera de faire de l'arithmétique sur les polynômes).

2.1 Divisibilité

Officiellement, il n'est écrit au programme que la notion de diviseurs et multiples. Le problème, c'est que de ces notions découlent immédiatement de toute une flopée de petites propriétés qu'il n'est pas raisonnable de ne pas mettre. On ne peut pas utiliser la divisibilité sans utiliser l'une ou l'autre de ces petites propriétés. J'ai donc complété le programme par les propriétés qui me semblent les plus utiles et les plus raisonnables (en termes de cohérence avec l'esprit du programme et d'utilité). Vous en trouverez certainement d'autres ou moins dans la littérature. Ça dépend du point de vue de l'auteur.

La notion de divisibilité est difficilement contournable, mais comme elle est extrêmement délicate (l'arithmétique est l'une des branches les plus ardues des mathématiques), elle est à la limite du programme. D'où les frontières floues et l'interprétation nécessaire de ces frontières.

Proposition 2.1 :
Si $P, Q, R \in \mathbb{K}[X]$, si $P \neq 0$,

$$PQ = PR \implies Q = R$$

Démonstration :
En effet, on a alors $P(Q-R) = 0$, ce qui veut dire $P = 0$ ou $Q - R = 0$, puisqu'il n'y a pas de diviseurs de 0. Or $P \neq 0$, donc forcément $Q - R = 0$, *i.e.* $Q = R$. □

C'est grâce à cette proposition simplissime que l'on va pouvoir définir et parler de divisibilité. Il faudra bien sûr être très au clair de ce que l'on entend par divisibilité.

On peut noter que la réciproque de cette proposition est vraie, mais n'a aucun intérêt. On notera également qu'en réalité, cette proposition est une reformulation du fait que $\mathbb{K}[X]$ soit intègre (qu'il n'y ait pas de diviseurs de 0).

C'est surtout la démonstration de cette propriété qui est utile. C'est un type de raisonnement qui est très utile dans les polynômes.

Exemple 2.1 :
Montrer que si $P \in \mathbb{R}[X]$ tel que $(X-1)P(X)+1 = X^2+X+2$, alors P est unique.

Définition 2.1 (Divisibilité, Diviseurs, Multiples [✓]) :
Soit $A, B \in \mathbb{K}[X]$.

- On dira que A divise B si $\exists P \in \mathbb{K}[X]$ tel que $B = AP$. On notera alors $A|B$ pour rappeler la notation dans $\mathbb{Z}$.
- On appelle diviseurs de B tout polynôme $P \in \mathbb{K}[X]$ tel que $P|B$.
- On appelle multiple de B tout polynôme $P \in \mathbb{K}[X]$ tel que $B|P$.

!!! ATTENTION !!!

La notion de divisibilité dépend entièrement et complètement du corps sur lequel on se place. Dans la définition, c'est "$\exists P \in \mathbb{K}[X]$ [...]" donc la notion de divisibilité dépend de l'existence d'un polynôme à coefficient dans le corps de base $\mathbb{K}$. Si on change de corps (ce qu'on fera), on peut perdre la relation de divisibilité.

⚠ Par exemple, $X - i$ divise X^2+1 dans $\mathbb{C}[X]$. Donc X^2+1 a des diviseurs non triviaux dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$. En effet, s'il admettait un diviseur dans $\mathbb{R}[X]$ non trivial, ce serait nécessairement un polynôme de degré 1. Mais alors il aurait une racine réelle, ce qui est absurde.

On aurait pu (dû ?) noter la relation de divisibilité par $|_{\mathbb{K}}$ pour indiquer dans quel corps on divise les polynômes. Mais cette notation n'a rien d'officielle. Néanmoins, vous pouvez parfaitement la définir en début de problème et l'utiliser sans vergogne par la suite si ça peut vous trouver ça plus clair avec le corps de base en indice. Mais ATTENTION, n'oubliez pas de définir cette notation en début de copie. Juste une phrase suffit : "On notera $|_{\mathbb{K}}$ la relation de divisibilité dans $\mathbb{K}[X]$" par exemple.

Exemple 2.2 :
On a $(X+1)|(X^2-1)$ dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ mais $(X-i)|X^2+1$ n'est valable que dans $\mathbb{C}[X]$ et pas dans $\mathbb{R}[X]$.

Proposition 2.2 (Reformulation diviseur et multiple) :
Soit $P \in \mathbb{K}[X]$.

1. $Q \in \mathbb{K}[X]$ est un diviseur de P si et seulement si $\exists A \in \mathbb{K}[X]$ tel que $P = AQ$.
2. $Q \in \mathbb{K}[X]$ est un multiple de P si et seulement si $\exists A \in \mathbb{K}[X]$ tel que $Q = AP$.

Exemple 2.3 :
Montrer que $(X+1)|(X^4-1)$ et $(X-1)|(X^n-1)$ pour tout $n \in \mathbb{N}$.

Remarque :
Bien sûr, tout polynôme est un diviseurs de 0 :

$$\forall P \in \mathbb{K}[X],\ P|0 \text{ car } 0 = P \times 0.$$

Définition 2.2 (Diviseur trivial [✓]) :
Soit $P \in \mathbb{K}[X]$.
On appelle diviseur trivial de P tout polynôme constant non nul ou tout polynôme de la forme λP avec $\lambda \in \mathbb{K}^*$.

En effet, pour tout polynôme P, on aura toujours $P = a \times (\frac{1}{a}P)$ avec $a \in \mathbb{K}^*$. Donc a est un diviseurs de P mais également $\frac{1}{a}P$.

Exemple 2.4 :
5, $1/2$, $\sqrt{2}$, $X^2+5/4$, $-8X^2-10$ sont des diviseurs triviaux de $4X^2+5$ ans $\mathbb{R}[X]$. Dans $\mathbb{C}[X]$, on peut rajouter i, $3+5i$, $iX^2+5i/4$ par exemple. Et encore beaucoup d'autres. La liste n'est bien sûr pas exhaustive.

Remarque :
Les diviseurs triviaux de $P \in \mathbb{K}[X]$ sont donc les polynômes inversibles (au sens de la multiplication, bien entendu) et les produits de P avec les polynômes inversibles.

Remarque :
Si on fait un parallèle avec les entiers relatifs, dans $\mathbb{Z}$, les diviseurs triviaux de $n \in \mathbb{Z}$ sont 1, -1, n et $-n$.

Proposition 2.3 (Se ramener à des polynômes unitaires) :
Soit $P \in \mathbb{K}[X]$.
Si $P \neq 0$ alors $\exists! Q \in \mathbb{K}[X]$ unitaire et $\exists! \alpha \in \mathbb{K}$ tels que $P = \alpha Q$.
En particulier, $\deg P = \deg Q$.

Démonstration :
Il suffit de l'écrire. Si $P(X) = \sum_{k=0}^{n} a_k X^k$ avec $n \geq 0$ et $a_n \neq 0$, alors $P(X) = a_n \left(\sum_{k=0}^{n} \frac{a_k}{a_n} X^k \right)$. On pose donc $Q(X) = \sum_{k=0}^{n} \frac{a_k}{a_n} X^k$. Q est clairement de degré n (puisque P l'est) et le coefficient dominant de Q est $\frac{a_n}{a_n} = 1$ donc Q est unitaire.

Supposons $P = \alpha Q = \beta R$ avec $\alpha, \beta \in \mathbb{K}$ et $Q, R \in \mathbb{K}[X]$ unitaire. Comme $P, Q, R \neq 0$, on a $\alpha, \beta \neq 0$ et donc $Q = \frac{\beta}{\alpha} R$. Mais Q et R étant unitaire, on doit avoir $\beta/\alpha = 1$, *i.e.* $\beta = \alpha$. Et par suite $Q = R$. □

En fait, la construction de Q et α fournissait aussi l'unicité, mais c'est pas tellement plus facile à dire.

On rappelle aussi que les polynômes inversibles de $\mathbb{K}[X]$ sont exactement les polynômes constants non nuls.

Exemple 2.5 :
On prend $P(X) = 5X^4 - 2X^3 + 3 - 2i$. Déterminer le polynôme unitaire de même degré que P proportionnel à P et le coefficient de proportionnalité.

Proposition 2.4 (Réduction aux polynôme unitaires de la divisibilité) :
Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}^*$. Alors

$$(\lambda P) | (\mu Q) \iff P | Q$$

Démonstration :
On a :

$$\begin{aligned}(\lambda P)|(\mu Q) &\iff \exists R \in \mathbb{K}[X], \mu Q = \lambda P R \\ &\iff \exists R \in \mathbb{K}[X], Q = P \times \left(\frac{\lambda}{\mu} R\right) \\ &\iff P|Q\end{aligned}$$

□

Cette proposition nous dit que l'on peut s'affranchir des constantes multiplicatives dans l'étude de divisibilité entre polynôme. Or, tout polynôme est égale (de façon unique) à une constante (son coefficient dominant) fois un polynôme unitaire. Donc en divisant par les coefficients dominants, on se ramène à étudier la divisibilité entre polynômes unitaires. Et c'est ce qu'on va faire.

Une autre façon de le dire, est que les polynômes inversibles sont "transparents" du point de vue de la divisibilité. Qu'ils soient là ou non, ne change rien pour la divisibilité. On peut donc toujours multiplier ou diviser par les polynômes unitaires. Et grâce à ça, se ramener à des polynômes unitaires.

Proposition 2.5 (Propriété algébrique de la relation de divisibilité) :
Soit $A, B, C \in \mathbb{K}[X]$. Alors :

1. $A|B$ et $B|C \implies A|C$ *[Transitivité]*
2. $A|B$ et $B|A \implies \exists \lambda \in \mathbb{K},\ A = \lambda B$.

Démonstration :

1. On sait $\exists P, Q \in \mathbb{K}[X]$ tels que $B = PA$ et $C = BQ$. Donc $C = PAQ$ donc $A|C$ car $PQ \in \mathbb{K}[X]$.
2. $\exists P, Q \in \mathbb{K}[X]$ tels que $A = BP$ et $B = AQ$. Si A ou B est le polynôme nul, alors l'autre aussi et donc on $A = B$ ce qui est plus fort encore que ce qu'on veut montrer. On suppose A et B non nul. Alors $A = APQ$. Mais comme $A \neq 0$, cf proposition 1.11 p.20, on en déduit $PQ = 1$. Donc P (et Q) est inversible. Donc $P \in \mathbb{K}[X]^\times = \mathbb{K}_0[X]^* = \mathbb{K}^*$. D'où le résultat.

□

⚠ Attention, on a pas la symétrie ici de la relation de divisibilité. On obtient A et B sont égaux à une constante multiplicative près. Mais comme les constantes non nuls sont précisément les inversibles de $\mathbb{K}[X]$, on peut dire plutôt que A et B sont égaux à une multiplication par un inversible près. Cette formulation est plus agréable car peut se transporter dans d'autres situations (et surtout, elle est plus cohérente avec ce qui se passe).

Ce sont ces "inversibles invisibles" qui empêche la relation de divisibilité d'être une relation d'ordre (partielle) sur $\mathbb{K}[X]$. C'est bien une relation binaire, réflexive et transitive. Mais elle n'est pas symétrique.

Remarque :
Pour avoir l'égalité entre A et B dans le second point, il faut rajouter quelque chose. Par exemple, le fait que A et B ont le même coefficient dominant (qui sera souvent 1 puisqu'on se ramènera souvent au cas de polynômes unitaires). Mais ce n'est pas la seul façon de faire. De même que dans $\mathbb{Z}$, il fallait rajouter une notion de signe pour avoir l'égalité.

Définition 2.3 (Polynômes associés) :
Soit $A, B \in \mathbb{K}[X]$.
On dit que A et B sont associés si $A|B$ et $B|A$.

Remarque :
Donc deux polynômes associés diffèrent d'une constante multiplicative.

Remarque :
Le problème de la divisibilité est qu'il y a une catégorie de polynômes qu'elle ne "voit" pas, qu'elle ne peut pas "attraper". Les polynômes en question sont les polynômes inversibles qui sont les "invisibles" du point de vue de la divisibilité.

Proposition 2.6 :
Soit $A, B, C, D \in \mathbb{K}[X]$. Alors

1. $A|B$ et $A|C \implies A|(\lambda B + \mu C)$ pour tout $\lambda, \mu \in \mathbb{K}$.
2. $A|B$ et $C|D \implies AC|BD$.
3. $A|B \implies \forall n \in \mathbb{N},\ A^n|B^n$.

Démonstration :

1. Soit $P, Q \in \mathbb{K}[X]$ tels que $B = AP$ et $C = AQ$. Alors $\lambda B + \mu C = A(\lambda P + \mu Q)$.
2. Soit $P, Q \in \mathbb{K}[X]$ tels que $B = AP$ et $D = CQ$. Alors $BD = ACPQ$.

3. Soit $P \in \mathbb{K}[X]$ tel que $B = AP$ et $n \in \mathbb{N}$. Alors $B^n = (AP)^n = A^n P^n$ car le produit de polynôme est commutatif dans $\mathbb{K}[X]$.

□

Exemple 2.6 :
Soit $a, b \in \mathbb{N}$. Montrer que

$$a|b \iff (X^a - 1)|(X^b - 1)$$

Proposition 2.7 (Conjugaison et divisibilité) :
Soit $A, B \in \mathbb{C}[X]$. Alors

$$A|B \iff \overline{A}\Big|\overline{B}$$

Démonstration :
Il suffit d'écrire la définition de la divisibilité et de passer ensuite aux conjugués. □

2.2 Division euclidienne

La division euclidienne, en revanche, celle là est clairement et entièrement au programme. Il n'y a pas de doute.

Théorème-Définition 2.4 (Division euclidienne polynomiale [✓]) :
$\forall A, B \in \mathbb{K}[X]$ avec $B \neq 0$, $\exists!(Q, R) \in \mathbb{K}[X]^2$ tel que

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

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

Démonstration :
Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Donc $\deg B \geq 0$.

Commençons par montrer l'unicité (c'est ce qu'il y a de plus facile). Supposons donc que $A = BQ_1 + R_1 = BQ_2 + R_2$ avec $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ et $\deg R_1, \deg R_2 < \deg B$. Alors dans ce cas $B(Q_1 - Q_2) = R_2 - R_1$. Donc $\deg B + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg B$. Donc $\deg(Q_2 - Q_1) < 0$ et donc $Q_2 - Q_1 = 0$. Ce qui amène directement à $(Q_2, R_2) = (Q_1, R_1)$ et donc l'unicité.

D'abord, si $\deg B = 0$, alors $B = b \in \mathbb{K}^*$ et $A = b\frac{1}{b}A$ donc il suffit de poser $Q = \frac{1}{b}A$ et $R = 0$. On peut donc désormais supposer $\deg B \geq 1$.

On va montrer l'existence d'un tel couple par récurrence sur le degré de A. Si $\deg A < \deg B$, il suffit de prendre $B = 0$ et $R = A$.

Si $\deg A = \deg B$, on note a le coefficient dominant de A et b celui de B. Alors $A = \frac{a}{b}B + (A - \frac{a}{b}B)$. On pose $Q = \frac{a}{b}$ et $R = A - \frac{a}{b}B$. Alors le coefficient dominant de $\frac{a}{b}B$ est a et de degré $\deg B = \deg A$, donc le coefficient de degré $\deg A$ de R est nul, donc $\deg R < \deg A = \deg B$ et donc on a bien l'existence d'un couple (Q, R) vérifiant la division euclidienne.

Supposons que $\exists n \geq \deg B$ tel que $\forall A \in \mathbb{K}_n[X]$, $\exists (Q, R) \in \mathbb{K}[X] \times \mathbb{K}_{\deg(B)-1}[X]$ tel que $A = BQ + R$.

Soit $A \in \mathbb{K}[X]$ tel que $\deg A = n+1$. Alors $\exists a \in \mathbb{K}^*$, $\exists \widehat{A} \in \mathbb{K}_n[X]$ tels que $A(X) = aX^{n+1} + \widehat{A}$. Donc $\exists Q_1, R_1 \in \mathbb{K}[X]$ tel que $\widehat{A} = BQ_1 + R_1$ et $\deg R_1 < \deg B$. On note b le coefficient dominant de B et $d = \deg B$. Donc $b \neq 0$. Or

$$\exists \widehat{B} \in \mathbb{K}_n[X],\ \frac{a}{b}BX^{n+1-d} = aX^{n+1} + \widehat{B}$$

Donc $\exists Q_2, R_2 \in \mathbb{K}[X]$ tel que $\deg R_2 < \deg B = d$ et $\widehat{B} = BQ_2 + R_2$. Finalement

$$\begin{aligned} A &= aX^{n+1} + \widehat{A} \\ &= \frac{a}{b}BX^{n+1-d} - BQ_2 - R_2 + BQ_1 + R_1 \\ &= B\left(\frac{a}{b}X^{n+1-d} - Q_2 + Q_1\right) + R_1 - R_2 \end{aligned}$$

On pose $Q = \frac{a}{b}X^{n+1-d} - Q_2 + Q_1$ et $R = R_1 - R_2$. Alors $\deg(R_1 - R_2) \leq \max(\deg R_1, \deg R_2) < \deg B$. Donc $\exists Q, R \in \mathbb{K}[X]$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

Donc on vient de montrer par récurrence que $\forall A \in \mathbb{K}[X]$ avec $\deg A \geq \deg B$, $\exists Q, R \in \mathbb{K}[X]$ avec $\deg R < \deg B$ tels que $A = BQ + R$. Mais le résultat est vrai aussi pour $\deg A \leq \deg B$ (fait avant la récurrence). D'où le résultat. □

Exemple 2.7 :
Déterminer la division euclidienne de A par B avec :

$$A(X) = X^4 - 3X^2 + X - 1 \qquad B(X) = X^2 - X + 1$$

$$A(X) = X^5 - X^4 - 2X^2 - 3X + 1 \qquad B(X) = X^2 + 2$$

Remarque :
Dans le cas où $B = X - a$, on a $A(X) = Q(X)(X-a) + \widetilde{A}(a)$.

Exemple 2.8 :
Effectuer la division euclidienne de $P \in \mathbb{K}[X]$ par $(X-a)(X-b)$ avec $a, b \in \mathbb{K}$.

Bien entendu, on peut écrire un programme en python qui permet de calculer la division euclidienne de deux polynômes. Mais le langage Python n'étant pas un langage de calcul formelle, c'est assez pénible à coder. Ça reste néanmoins faisable.

Proposition 2.8 (Caractérisation de la divisibilité par la division euclidienne [✓]) :
Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On a

$$B|A \iff \text{le reste de la division euclidienne de } A \text{ par } B \text{ est } 0$$

Démonstration :
Il suffit de l'écrire □

Remarque :
Dans la pratique, c'est souvent seulement le reste de la division euclidienne qui nous intéresse. Pour déterminer le reste de la division euclidienne de A par B, on écrit (de façon théorique) $A = BQ + R$ avec $R = \sum_{k=0}^{\deg B - 1} a_k X^k$. Il faut déterminer les coefficients $a_0, \ldots, a_{\deg B - 1}$ de R. Il suffit alors d'évaluer A (ou plus exactement $\widetilde{A}$) sur $\deg B$ valeurs distinctes pour déterminer ces coefficients. Tant qu'à faire, on choisit bien les valeurs où évaluer la relation. Le mieux étant de choisir des racines de B de sorte que l'on ait $A(\alpha) = R(\alpha)$.

Exemple 2.9 :
Déterminer le reste de la division euclidienne de $A(X) = X^5 - X^4 + X^2 + 2$ par $X^2 - 2$.

Remarque :
Comme on a une notion de divisibilité, on vient de commencer à faire un peu d'arithmétique. On va continuer à en faire un petit peu. Dans la droite de lignée de ce que l'on vient de faire, on pourrait définir une notion de PGCD de polynômes et de PPCM.

2.3 Polynômes irréductibles

On revient à l'arithmétique pure et dure. La notion de polynômes irréductibles est parfaitement au programme. Pas d'ambiguïté. Et elle va être très délicate. J'ai essayé ici de ne mettre que ce qui me semble le stricte minimum pour bien comprendre la suite. Mais cette partie va rester néanmoins très abstraite.

Définition 2.5 (Polynômes premiers entre eux [✓]) :
Soit $A, B \in \mathbb{K}[X]$. On dit que A et B sont premiers entres eux si les seuls diviseurs communs à A et B sont les constantes non nuls (*i.e.* les polynômes de degré 0).

Exemple 2.10 :
Soit $a, b \in \mathbb{K}$ avec $a \neq b$. Montrer que $X - a$ et $X - b$ sont premiers entre eux.

Définition 2.6 (Polynômes irréductibles [✓]) :
Soit $P \in \mathbb{K}[X]$ non constant. On dit que P est irréductible dans $\mathbb{K}[X]$ si ses seuls diviseurs sont ses diviseurs triviaux (*i.e.* constantes non nulles et produit de P par une constante non nulle). Autrement dit P est irréductible si et seulement si $\forall Q \in \mathbb{K}[X]$ tel que $Q|P$, $\exists \lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$ ou $Q = \lambda$.

Remarque :
La contraposé est très utile :

$$P \in \mathbb{K}[X] \text{ non irréductible } \iff \exists Q \in \mathbb{K}[X], 1 \leq \deg Q < \deg P,\ Q|P$$

Exemple 2.11 :
Soit $a \in \mathbb{K}$. Alors $X - a$ est irréductible.

La notion de polynômes irréductibles est indispensable pour la suite. C'est la pierre angulaire de

l'étude des polynômes. Tous ce que vous savez sans en avoir conscience repose en réalité sur cette définition.

L'idée est que les polynômes irréductibles forment des sortes de briques élémentaires dans $\mathbb{K}[X]$. On peut alors décrire (du point de vue divisibilité) n'importe quel polynôme à l'aide de ces "briques élémentaires". Il est donc nécessaire dans un premier temps de bien comprendre comment fonctionnent les polynômes irréductibles pour arriver ensuite à la décomposition souhaitée dans le théorème fondamentale de l'arithmétique 4.5 page 80.

Proposition 2.9 (L'irréductibilité est conservé par produit par un inversible [✓]) :
Soit $P \in \mathbb{K}[X]$ irréductible.
Alors $\forall \lambda \in \mathbb{K}^*$, λP est irréductible.

Démonstration :
Il suffit d'observer un diviseur de λP. □

!!! ATTENTION !!!

⚠ L'irréductibilité d'un polynôme dépend du corps $\mathbb{K}$ que l'on considère. On insistera là dessus plus en détail un peu plus bas, mais autant le dire tout de suite : le polynôme $P(X) = X^2+1$ est un polynôme de $\mathbb{R}[X]$ et aussi de $\mathbb{C}[X]$. Sur $\mathbb{C}$, il n'est pas irréductible, mais il l'est dans $\mathbb{R}$. C'est parce que la notion d'irréductible dépend complètement de la notion de divisibilité qui, elle même, dépend complètement du corps sur lequel on se place.

!!! ATTENTION !!!

⚠ $$A|BC \not\Rightarrow A|B \text{ ou } A|C$$

Un contre-exemple est donné par $A(X) = X^2 - 1$, $B(X) = X + 1$ et $C(X) = X - 1$. Il faut faire TRÈS attention ! Votre intuition va être mis à rude épreuve. Soyez très prudent avec l'arithmétique. C'est vraiment traître.

Théorème 2.10 (Lemme de Gauss) :
Soit $A, B, C \in \mathbb{K}[X]$.
Si A et B sont premiers entre eux et si $A|BC$, alors $A|C$.

Ce théorème est admis pour nous. La démonstration utilise des notions de PGCD et le théorème de Bézout qui sont HP. Donc tant pis.

Le théorème de Gauss n'est pas explicitement au programme. Mais il est pratique et il nous sera utile dans la suite (pour la démo du théorème fondamental de l'arithmétique).

!!! ATTENTION !!!

⚠

$$A|C \text{ et } B|C \not\Longrightarrow AB|C$$

Un contre-exemple est donné par $A(X) = X^2 - 1$, $B(X) = (X+1)^2$ et $C(X) = (X+1)(X^2-1)$.

Théorème 2.11 (Réciproque partielle au théorème de Gauss) :
Soit $A, B, C \in \mathbb{K}[X]$.
Si $A|C$, $B|C$ et A et B premiers entres eux, alors $AB|C$.

Démonstration :
Soit $P \in \mathbb{K}[X]$ tel que $C = BP$. Alors $A|BP$. Mais A et B étant premiers entres eux, le théorème de Gauss nous donne $A|P$ et donc $AB|BP = C$. □

Proposition 2.12 (Condition suffisante pour être premiers entres eux [✓]) :
Soit $A, P \in \mathbb{K}[X]$, P irréductible.
Si $P \not| A$ alors A et P sont premiers entre eux.

Démonstration :
Il faut montrer que les seuls diviseurs communs à A et P sont les constantes non nuls. Soit Q un diviseurs communs à A et P. Donc Q est en particulier un diviseurs de P. Mais P étant irréductibles, ses seuls diviseurs sont les diviseurs triviaux, c'est à dire les constantes non nulles ou des multiples de P par une constante non nulle. Donc $\exists \lambda \in \mathbb{K}^*$ tel que $Q = \lambda$ ou $Q = \lambda P$. Mais si $Q = \lambda P$, alors $\lambda P|A$, donc $P|A$ ce qui aboutit à ☠. Donc $Q = \lambda$. Donc A et P sont premiers entres eux. □

Proposition 2.13 (Lemme d'Euclide [✓]) :
Soit $A, B \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ irréductible. Alors

$$P|AB \implies P|A \text{ ou } P|B$$

Démonstration :
Si $P|A$, il n'y a rien à faire.

Supposons que $P \not| A$ et montrons que $P|B$. Comme $P \not| A$ et P est irréductible, P et A sont premiers entres eux. Donc le théorème de Gauss nous donne directement $P|B$. □

Pareil que pour le théorème de Gauss. Le lemme d'Euclide n'est pas explicitement au programme mais il est très pratique et on va en avoir besoin dans les théorèmes suivants.

Proposition 2.14 :
Soit $a, b \in \mathbb{K}$ avec $a \neq b$ et $n, m \in \mathbb{N}$.

Alors $(X-a)^n$ et $(X-b)^m$ sont premiers entres eux.

Démonstration :
Supposons qu'ils ne le sont pas. Donc $\exists P \in \mathbb{K}[X]$ tel que $P|(X-a)^n$ et $P|(X-b)^m$ avec $\deg P \geq 1$. Or les seuls diviseurs de $(X-a)^n$ sont les $(X-a)^k$ avec $0 \leq k \leq n$ et les multiples de ces polynômes par des constantes non nuls. Donc P est de la forme $\alpha(X-a)^k$ avec $\alpha \in \mathbb{K}^*$ et $0 \leq k \leq n$. Donc $\alpha(X-a)^k|(X-b)^m$. En particulier, si $k \geq 1$, $(X-a)|\alpha(X-a)^k|(X-b)^m$. Mais $X-a$ est un polynôme irréductible et il ne divise pas $(X-b)$. Donc il ne divise pas $(X-b)^m$. Donc si $k \geq 1$, on aboutit à ☠. Donc $k = 0$. Donc $P = \alpha \in \mathbb{K}^*$ et donc les seuls diviseurs communs à $(X-a)^n$ et $(X-b)^m$ sont les constantes non nuls. Ces deux polynômes sont donc premiers entres eux. □

En fait, cette proposition est plutôt un exercice qu'une proposition. Mais il est pratique de la connaître. Elle permet de pouvoir commencer à faire de l'arithmétique avec plus de facilité surtout si l'on connaît le théorème fondamental de l'arithmétique 4.5.

2.4 PGCD

Proposition 2.15 (Ensemble des diviseurs communs) :
Soit $A, B \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$.

L'ensemble des diviseurs communs de A et B est un ensemble de polynôme dont les degrés sont majorés.

Démonstration :
Soit $\mathcal{D} = \{P \in \mathbb{K}[X],\ P|A,\ P|B\}$ l'ensemble des diviseurs communs de A et B. Alors $\mathcal{D} \neq \emptyset$ car $\mathbb{K}^* \subset \mathcal{D}$ car ce sont les diviseurs triviaux. De plus, $\forall P \in \mathcal{D}$, $\deg(P) \leq \min(\deg(A), \deg(B))$. Donc $D = \{\deg(P),\ P \in \mathcal{D}\}$ est un sous-ensemble non vide ($0 \in D$) et majorée de $\mathbb{N}$. Donc D admet un maximum. □

Définition-Propriété 2.7 (PGCD de deux polynômes) :
Soit $A, B \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$.
On appelle PGCD de A et B, tout diviseurs commun de A et B de degré maximal.

Démonstration :
On vient de voir que les degrés des diviseurs communs de A et B admettent un maximum. Il existe donc des diviseurs communs de A et B de degré maximum. Ce sont les PGCD. □

!!! ATTENTION !!!

Il n'y a pas unicité du PGCD. Il y a une infinité de PGCD.

Exemple 2.12 :
Avec $A(X) = X^2 + 2X + 1$ et $B(X) = X^2 - 1$, $X + 1$ est un PGCD, mais $2X + 2$ aussi, $-3X - 3$ également etc.

Remarque :
Si $B = 0$, les PGCD de A et 0 sont les λA, $\lambda \in \mathbb{K}^*$.

Proposition 2.16 (Ensemble des diviseurs communs) :
Soit $A, B \in \mathbb{K}[X]$, $(A, B) \neq (0, 0)$. Soit D un PGCD de A et B.
Alors si on note Div l'ensemble des diviseurs,

$$\mathrm{Div}(A, B) = \mathrm{Div}(D).$$

Remarque :
En particulier, tous les PGCD ont le même ensemble de diviseurs.

Démonstration :
On peut suppose $A \neq 0$ sans perte de généralités quitte à renommer les deux polynômes. On a déjà facilement $\mathrm{Div}(D) \subset \mathrm{Div}(A, B)$ par transitivité de la relation de divisibilité.

Supposons $B = 0$ ou $\deg(B) = 0$. Alors $\mathrm{Div}(A, B) = \mathrm{Div}(A)$ et $D = \lambda A$ avec $\lambda \in \mathbb{K}^*$. Donc ça marche.

Supposons que $\mathrm{Div}(A, B) = \mathrm{Div}(D)$ pour tout polynôme B de degré $\leq d$ (avec $d \in \mathbb{N}$). Soit B un polynôme de degré $d + 1$. On effectue la division euclidienne de A par B : $A = BQ + R$ avec $\deg(R) < \deg(B)$. De plus, il est facile de voir que $\mathrm{Div}(A, B) = \mathrm{Div}(B, R)$. Donc $D \in \mathrm{Div}(B, R)$ et D est de degré maximal. Donc D est un PGCD de B et R. Comme $\deg(R) \leq d$, on a $\mathrm{Div}(B, R) = \mathrm{Div}(D)$. Et donc $\mathrm{Div}(A, B) = \mathrm{Div}(D)$. □

Remarque :
En particulier, on vient de montre qu'un PGCD de A et B est aussi un PGCD de B et R, où R est le reste de la division euclidienne de A par B.

Proposition 2.17 (Les PGCD sont associés) :
Soit $A, B \in \mathbb{K}[X]$, $(A, B) \neq (0, 0)$.
Tous les PGCD de A et B sont associés.

Démonstration :
Il est clair que si P est un PGCD, alors tous les polynômes associés à P sont également des PGCD.

Soit P et Q deux PGCD de A et B. Alors $\mathrm{Div}(P) = \mathrm{Div}(A, B) = \mathrm{Div}(Q)$. En particulier, $P|Q$ et $Q|P$. Donc P et Q sont associés. □

Proposition 2.18 (Caractérisation des PGCD) :
Soit $A, B, D \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$.

$$D \text{ est un PGCD de } A \text{ et } B \iff \begin{cases} D|A,\ D|B \\ \forall P \in \mathbb{K}[X],\ P|A,\ P|B \implies P|D \end{cases}$$

Donc les PGCD sont les plus grands diviseurs communs de A et B au sens de la divisibilité.

Démonstration :
Le sens directe est évident. Si D est un PGCD, on sait déjà que D est un diviseur commun, par définition. Et également, si P est un autre diviseur commun, alors $P \in \mathrm{Div}(A, B) = \mathrm{Div}(D)$.

Inversement, on a $\mathrm{Div}(A, B) = \mathrm{Div}(D)$. Er $\forall P \in \mathrm{Div}(A, B),\ P|D$, donc $\deg(P) \leq \deg(D)$. Donc $\deg(D)$ est le maximum de $\{\deg(P),\ P \in \mathrm{Div}(A, B)\}$. Et donc, par définition, D est un PGCD de A et B. □

Définition 2.8 ($A \wedge B$) :
Soit $(A, B) \in \mathbb{K}[X]^2 \setminus \{(0, 0)\}$.

On note $A \wedge B$ le PGCD de A et B unitaire. *i.e.* $A \wedge B$ est un diviseur commun de A et B de degré maximal et de coefficient dominant 1.

Remarque :
Tous les PGCD étant associés, ils sont tous proportionnels. *i.e.* l'ensemble des PGCD de A et B forment une droite vectorielle (en y ajoutant 0). Et donc, il n'y en a qu'un de coefficient dominant 1 (prendre l'application $P \mapsto \mathrm{coeff\,dom}(P)$ qui est une forme linéaire sur l'ensemble des PGCD).

Remarque :
Par convention, on pose $0 \wedge 0 = 0$. C'est une convention qui permet d'avoir une définition cohérente avec les propriétés des PGCD. Par exemple, la caractérisation des PGCD fonctionne encore avec cette convention.

Proposition 2.19 (Algorithme d'Euclide [✓]) :
Soit $A, B \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$.

On pose $R_0 = A$ et $R_1 = B$. Pour $n \in \mathbb{N}^*$, si $R_n \neq 0$, on définit R_{n+1} comme le reste de la division euclidienne de R_{n-1} par R_n.

Alors $\exists N \in \mathbb{N}$ tel que $R_N = 0$, de plus $(R_n)_{0 \leq n \leq N}$ est une suite de polynôme strictement décroissante en degré et R_{N-1} est un PGCD de A et B.

Démonstration :
On a $R_{k-1} = Q_k R_k + R_{k+1}$ avec $\deg(R_{k+1}) < \deg(R_k)$. Donc tant qu'on peut effectuer les divisions euclidiennes, la suite des degrés $\deg(R_k)$ fabriquée est une suite d'entier strictement décroissante. Elle est donc stationnaire en 0. Et donc $\exists N \in \mathbb{N}$ tel que $\deg(R_N) = 0$. Alors $R_{N+1} = 0$. Et le processus d'arrête.

De plus, d'après ce qui précède, on a vu $\forall k \in \{0, \dots, N\}$, $\mathrm{Div}(R_k, R_{k+1}) = \mathrm{Div}(R_{k-1}, R_k)$. Donc $\mathrm{Div}(R_N, R_{N+1}) = \mathrm{Div}(R_N) = \mathrm{Div}(R_0, R_1) = \mathrm{Div}(A, B)$. Et donc R_N est un PGCD de A et B. □

Théorème 2.20 (Relation de Bézout) :
Soit $(A, B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$. Alors

$$\exists U, V \in \mathbb{K}[X],\ AU + BV = A \wedge B.$$

Démonstration :
Comme dans $\mathbb{Z}$: il suffit de reprendre l'algorithme d'Euclide, puis de renormaliser à la fin en divisant par le coefficient dominant du PGCD qu'on a trouvé. □

Exemple 2.13 :
$A(X) = X^4 + X^3$ et $B(X) = X^2 + X + 1$. Calculer un PGCD de A et B et déterminer la relation de Bézout associé.

Proposition 2.21 :
Soit $A, B, C \in \mathbb{K}[X]$, $(A, B) \neq (0, 0)$ et $C \neq 0$. Alors

$$(CA) \wedge (CB) = \frac{1}{\mathrm{coeff\ dom}(C)} C(A \wedge B).$$

Démonstration :
Sans perte de généralité, on peut suppose C unitaire. Alors $C(A \wedge B)$ est un diviseur commun de CA et CB. Donc $C(A \wedge B) | (CA) \wedge (CB)$.

De plus, par Bézout, $\exists U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$. Donc $(CA)U + (CB)V =$

$C(A \wedge B)$. Donc $(CA) \wedge (CB) | (C(A \wedge B))$.

Or $(CA) \wedge (CB)$ est unitaire par définition et $C(A \wedge B)$ également. Donc $C(A \wedge B) = (CA) \wedge (CB)$. □

Remarque :
On pourrait rajouter beaucoup de propriété similaire à ce qui c'est passé dans $\mathbb{Z}$. Avec ce qu'on a pour le moment, on peut tout reconstruire. Il faudra donc refaire les mini propriétés en fonction de ce dont on a besoin.

Définition 2.9 (PGCD de plusieurs polynômes) :
Soit $(A_1, \ldots, A_n) \in \mathbb{K}[X]^n \setminus \{(0, \ldots, 0)\}$.

On note $\bigwedge_{k=1}^{n} A_k = A_1 \wedge A_2 \wedge \cdots \wedge A_n$ l'unique polynôme unitaire de degré maximal divisant A_1, A_2, …, A_n.

Proposition 2.22 (Propriété algébriques du PGCD) :
Soit $A, B, C, A_1, \ldots, A_n \in \mathbb{K}[X]$ avec $(A, B, C) \neq (0, 0, 0)$ et $(A_1, \ldots, A_n) \neq (0, \ldots, 0)$.

(i) $A \wedge B \wedge C = (A \wedge B) \wedge C = A \wedge (B \wedge C)$ [*Associativité*]

(ii) $\mathrm{Div}(A_1, \ldots, A_n) = \mathrm{Div}(\bigwedge_{k=1}^{n} A_k)$.

(iii) $\exists U_1, \ldots, U_n \in \mathbb{K}[X]$, $\bigwedge_{k=1}^{n} A_k = \sum_{k=1}^{n} A_k U_k$. [*Bézout*]

Démonstration :
Avec une récurrence, essentiellement. □

2.5 Polynômes premiers entre eux

Définition 2.10 (Polynômes premiers entre eux) :
Soit $(A, B) \in \mathbb{K}[X]^2 \setminus \{(0, 0)\}$.

On dit que A et B sont *premier entre eux* si $A \wedge B = 1$, *i.e.* si le diviseur commun unitaire de A et B est 1.

Théorème 2.23 (Théorème de Bézout) :
Soit $(A, B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$.

$$A \wedge B = 1 \iff \exists U, V \in \mathbb{K}[X],\ AU + BV = 1$$

Démonstration :
La démonstration est essentiellement la même que dans $\mathbb{Z}$. Le sens directe est déjà fait. Réciproquement, si $AU+BV = 1$, alors $(A\wedge B)|1$ et donc $A\wedge B$ est un polynôme constant unitaire, donc $A\wedge B = 1$. □

Proposition 2.24 (Lemme de Gauss) :
Soit $A, B, C \in \mathbb{K}[X]$.
Si $A|BC$ et $A \wedge B = 1$, alors $A|C$.

Démonstration :
C'est la même que dans $\mathbb{Z}$. On a $ACU + BCV = C$ et donc la réciproque à la relation de Bézout précédente. □

Proposition 2.25 (Se ramener à des polynômes premier entre eux) :
Soit $(A, B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$. Soit $D = A \wedge B$.
Alors $\exists A_1, B_1 \in \mathbb{K}[X]$, $A_1 \wedge B_1 = 1$ tel que $A = DA_1$, $B = DB_1$.

Démonstration :
On a $DA_1 = A$ et $DB_1 = B$ par définition de la divisibilité. Soit $P = A_1 \wedge B_1$. Alors $P|A, B$, donc $P|D$. Si $\deg(P) \geq 1$, alors D n'est pas de degré maximal et donc ☠. Donc $\deg(P) = 0$. Et donc, $A_1 \wedge B_1 = 1$. □

Proposition 2.26 ("Transmission de la primalité relative") :
Soit $A, B, C \in \mathbb{K}[X]$. Alors

$$A \wedge (BC) = 1 \iff A \wedge B = 1 = A \wedge C$$

Démonstration :
Si $A \wedge (BC) = 1$, alors $AU + BCV = 1$ et donc $(A \wedge B)|1$ donc $A \wedge B = 1$. De même, $A \wedge C = 1$.
Si $A \wedge B = A \wedge C = 1$, Alors $A(U_1CV_2 + U_2) + BCV_1V_2 = 1$. □

Proposition 2.27 :
Soit $A \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ irréductible.
Alors $P|A$ ou $P \wedge A = 1$.

Démonstration :
Voir $\mathbb{Z}$: si $P \not| A$, alors $D = P \wedge A$ est un diviseur de P irréductible, donc $D = 1$ car D unitaire. □

Proposition 2.28 :
Soit $A, B \in \mathbb{K}[X]$ et P irréductible dans $\mathbb{K}[X]$.
Si $P|AB$, alors $P|A$ ou $P|B$.

Démonstration :
Comme dans $\mathbb{Z}$: si $P \not| A$, alors $P \wedge A = 1$ et donc, par lemme de Gauss, $P|B$. □

Définition 2.11 (Polynômes premiers entre eux dans leur ensemble) :
Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$.
On dit que $A_1, \ldots, A_n$ sont *premiers entre eux dans leur ensemble* si $\bigwedge_{k=1}^{n} A_k = 1$.
$A_1, \ldots, A_n$ sont dit *deux à deux premiers entre eux* si $\forall i, j \in \{1, \ldots, n\}$, $i \neq j$, $A_i \wedge A_j = 1$.

!!! ATTENTION !!!

⚠ Bien sûr, il ne faut pas confondre premier dans leur ensemble et deux à deux premiers entre eux. Le second impliquant le premier. Si des polynômes sont deux à deux premiers eux, ils sont automatiquement premier entre eux dans leur ensemble. Mais la réciproque est fausse. On peut avoir des polynômes premiers entre eux dans leur ensemble, sans qu'ils sont deux à deux premier entre eux.

Contre-exemple :
On prend $A(X) = X + 1$, $B(X) = X - 1$, $C(X) = X^2 - 1$. Alors $A \wedge B \wedge C = 1$ car $A \wedge B = 1$. Donc A, B, C sont premiers dans leur ensembles. Mais $A \wedge C = A$ et $B \wedge C = B$. Donc ils ne sont pas deux à deux premiers entre eux.

Proposition 2.29 (Caractérisation des polynômes premier dans leur ensemble par Bézout) :
Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$.
$A_1, \ldots, A_n$ sont premiers dans leur ensemble si, et seulement si, $\exists U_1, \ldots, U_n \in \mathbb{K}[X]$ tels que $\sum_{k=1}^{n} A_k U_k = 1$.

Démonstration :
Le sens indirecte est évident. Le directe s'obtient par récurrence et par Bézout grâce à l'associativité du PGCD. □

Proposition 2.30 :
Soit $A, B, C \in \mathbb{K}[X]$.
Si $A \wedge B = 1$ et $A|C$ et $B|C$, alors $AB|C$.

Démonstration :
On a $C = AP = BQ$. Donc $A|BQ$. Mais $A \wedge B = 1$, donc $A|Q$. Et donc le résultat. □

Remarque :
Ce résultat se généralise dans le cas de polynômes deux à deux premiers entre eux par récurrence facile.

2.6 PPCM

Définition-Propriété 2.12 (PPCM) :
Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$.
On appelle *plus petit commun multiple* de A et B, tout multiple commun de A et B non nul de degré minimal.

Démonstration :
On note $E = \{\deg(P),\ P \in \mathbb{K}[X],\ A|P,\ B|P\}$. Alors $\deg(A) + \deg(B) \in E$ donc $E \neq \emptyset$ et $E \subset \mathbb{N}$ et $\mathbb{N}$ bien ordonnée donc existence d'un degré minimal et donc de polynôme qui ont ce degré. □

Remarque :
Comme pour les PGCD, il n'y a pas unicité des PPCM. À cause des polynômes inversibles. Comme pour les PGCD, on aurait unicité en imposant quelque chose sur le coefficient dominant.

Proposition 2.31 (Caractérisation des PPCM) :
Soit $A, B \in \mathbb{K}[X]$, $AB \neq 0$ et soit $M \in \mathbb{K}[X]$.
Alors

$$M \text{ est un PPCM de } A \text{ et } B \iff \begin{cases} M \neq 0 \\ A, B \in \mathrm{Div}(M) \\ \forall P \in \mathbb{K}[X],\ A, B|P \implies M|P \end{cases}$$

Démonstration :
Même principe que pour les entiers.

Si M est un PPCM, en faisant une division euclidienne, on a $P = MQ + R$ et R multiple commune de A et B avec $\deg(R) < \deg(M)$. La minimalité nous donne $R = 0$ et donc le résultat.

Inversement, si M vérifie les trois propriétés, alors M est un multiple commun non nul de degré minimal. Donc c'est un PPCM. □

Corollaire 2.32 (Ensemble des multiples communs) :
Soit $A, B \in \mathbb{K}[X]$, $AB \neq 0$. Soit M un PCCM de A et B.
Alors

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Démonstration :
C'est facile par minimalité du degré de M et par définition des ensembles. □

Définition-Propriété 2.13 ($A \vee B$) :
Soit $A, B \in \mathbb{K}[X]$, $AB \neq 0$.
Il existe un unique PPCM de A et B unitaire, noté $A \vee B$. Et donc

$$M = A \vee B \iff \begin{cases} \text{coeff dom}(M) = 1 \\ A|M,\ B|M \\ \forall P \in \mathbb{K}[X],\ A|P,\ B|P \implies M|P \end{cases}$$

Démonstration :
Imposé le coefficient dominant égal à 1 revient à imposé que M est non nul. Donc la deuxième partie est évident.
$A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est une droite vectorielle. Et voila. □

Remarque :
On peut alors prendre comme convention $A \vee 0 = 0$.

Proposition 2.33 (Factorisation de PPCM) :
Soit $A, B, C \in \mathbb{K}[X]$, $ABC \neq 0$. Alors

$$(CA) \vee (CB) = \frac{C}{\text{coeff dom}(C)}(A \vee B).$$

Proposition 2.34 (PPCM et PGCD) :
Soit $A, B \in \mathbb{K}[X]$, $AB \neq 0$. Alors

(i) Si $A \wedge B = 1$, alors $A \vee B = \frac{AB}{\text{coeff dom}(AB)}$

(ii) En général $(A \wedge B)(A \vee B) = \frac{AB}{\text{coeff dom}(AB)}$.

Démonstration :
Posons $M = A \vee B$. On a $A|M$ et $B|M$ et $A \wedge B = 1$, donc $AB|M$. De plus, $M|AB$ par caractérisation de M. Et donc M et AB sont associés. Mais M est unitaire. Donc $AB = \text{coeff dom}(AB)(A \vee B)$.

Ensuite, on se ramène à des polynômes unitaires : on pose A_1, B_1 tel que $A_1 \wedge B_1 = 1$ et $A = DA_1$, $B = DB_1$ avec $D = A \wedge B$. Alors $A \vee B = D(A_1 \vee B_1) = DA_1B_1$. Et donc $D(A \vee B) = AB$. □

Proposition 2.35 (PGCD et PPCM avec décompositions en produit de facteurs irréductibles) :
Soit $A, B \in \mathbb{K}[X]$. Soit $P_1, \ldots, P_n \in \mathbb{K}[X]$ les facteurs irréductibles de A et B. Autrement dit :

$$A(X) = a \prod_{k=1}^{n} P_k(X)^{\alpha_k}, \qquad B(X) = b \prod_{k=1}^{n} P_k(X)^{\beta_k}$$

où $a, b \in \mathbb{K}^*$, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}$ (avec $\alpha_i = 0$ si P_i ne divise pas A et de même $\beta_i = 0$ si $P_i \not| B$).

Alors

$$A \wedge B = \prod_{k=1}^{n} P_k(X)^{\min(\alpha_k, \beta_k)} \qquad \text{et} \qquad A \vee B = \prod_{k=1}^{n} P_k(X)^{\max(\alpha_k, \beta_k)}$$

Remarque :
On retrouve ici que $AB = \text{coeff dom}(AB)(A \wedge B)(A \vee B)$.

Remarque :
Ce théorème provient en fait de la décomposition en produit de facteur irréductibles qui vient dans la suite. On se contente de dire, pour le moment, que si on arrive à écrire A et B sous la forme de produit de facteurs irréductibles, on a une expression des PGCD et PPCM. Mais on a pas l'assurance, pour le moment, que l'ont sait obligatoirement écrire A et B sous la forme d'une produit de facteurs irréductibles. C'est la partie manquante qui arrives plus bas et où l'on va traiter le cas complexe et réel séparément.

3 Racines d'un polynôme, polynômes scindés

On rappelle qu'une racine d'un polynôme $P \in \mathbb{K}[X]$ est un élément $a \in \mathbb{K}$ tel que $\widetilde{P}(a) = 0$.

3.1 Racines et degré

Théorème 3.1 (Caractérisation des racines par la divisibilité [✓]) :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
a est une racine de P si et seulement si $(X - a)|P$.

Démonstration :
Si $(X - a)|P$, alors $\exists Q \in \mathbb{K}[X]$ tel que $P(X) = (X - a)Q(X)$. Alors $\widetilde{P}(a) = (a - a)\widetilde{Q}(a) = 0$ par 1.17 p.26. Donc a racine de P.

Réciproquement, si P est une racine de P. Par division euclidienne, on sait $\exists Q, R \in \mathbb{K}[X]$ tel que $P(X) = (X - a)Q(X) + R(X)$ et $\deg R < \deg(X - a) = 1$. Donc $R \in \mathbb{K}$. Et $\widetilde{P}(a) = 0$ nous donne $\widetilde{R}(a) = 0$. Donc $R = 0$. Donc $P(X) = (X - a)Q(X)$ et donc $(X - a)|P$. □

!!! ATTENTION !!!

⚠ La notion de racine dépend du corps que l'on considère. Un polynôme peut avoir certaines racines dans $\mathbb{R}$ et d'autres dans $\mathbb{C}$. Par exemple, le polynôme $P(X) = X^2 + 1$ n'a aucune racines dans $\mathbb{R}$ mais en a 2 distinctes dans $\mathbb{C}$.

Corollaire 3.2 (Avec plusieurs racines) :
Soit $P \in \mathbb{K}[X]$.
Soit $a_1, \ldots, a_n$ des racines de P deux à deux distinctes. Alors

$$\prod_{k=1}^{n}(X - a_k) = (X - a_1) \times \cdots \times (X - a_n) \Big| P(X)$$

Démonstration :
Par récurrence en utilisant le fait que $(X - a_k) \not| (X - a_j)$ si $k \neq j$, le théorème de Gauss et le fait que $(X - a_i)$ et $(X - a_j)$ sont premiers entre eux ici. □

Théorème 3.3 (Majorant du nombre de racines [✓]) :
Soit $P \in \mathbb{K}[X]$.
Si $P \neq 0$, alors P ne peut pas avoir plus de racines distinctes que son degré.

Ce théorème est fondamental. Il est très utile pour montrer qu'un polynôme est nul. Dès qu'un polynôme a plus de racines que son degré, c'est nécessairement le polynôme nul, par contraposée de ce théorème.

Démonstration :
Soit $P \in \mathbb{K}[X]^*$. Soit également $a_1, \dots, a_n$ ses racines distinctes. Alors, par le corollaire 3.2, on a $(X-a_1)\dots(X-a_n)|P(X)$. Et P non nul. Donc $\exists Q \in \mathbb{K}[X]^*$ tel que $P(X) = Q(X)\prod_{k=1}^{n}(X-a_k)$. Alors dans ce cas, $\deg P = \deg Q + \deg \prod_{k=1}^{n}(X-a_k) \geq \underbrace{1+1+\cdots+1}_{n} = n$. Donc le nombre de racines distinctes de P (ici n) est plus petit que $\deg P$. □

!!! ATTENTION !!!

⚠ Ce théorème ne dit pas qu'un polynôme a forcément des racines. Ni qu'il en a autant que son degré. Il existe des polynômes n'ayant pas de racines (X^2+1 dans $\mathbb{R}[X]$ par exemple) ou d'autres avec moins de racines que leurs degré (par exemple X^5-1 dans $\mathbb{R}[X]$). Ce théorème donne juste un majorant du nombre de racines de P.

On utilise souvent le corollaire suivant pour montrer qu'un polynôme est nul :

Corollaire 3.4 (Caractérisation de nullité par le nombre de racines [✓]) :
Soit $P \in \mathbb{K}[X]$.

$$P = 0 \iff P \text{ a une infinité de racines}$$

Démonstration :
Le sens indirecte est évident. S'il a une infinité de racines, il en a en particulier plus que son degré ... □

Exemple 3.1 :

Soit $P, Q, R \in \mathbb{R}[X]$ avec $P \neq 0$. Montrer que $\exists A > 0$ tel que $\forall x \geq A$, $\widetilde{P}(x) \neq 0$. En déduire que si $\forall x \geq A$, $\frac{\widetilde{Q}(x)}{\widetilde{P}(x)} = \frac{\widetilde{R}(x)}{\widetilde{P}(x)}$, alors $Q = R$.

Corollaire 3.5 (Expression d'un polynôme de degré n ayant n racines distinctes) :
Soit $P \in \mathbb{K}[X]$ avec $n = \deg P \geq 0$, de coefficient dominant $a \in \mathbb{K}^*$ et ayant n racines distinctes $x_1, \ldots, x_n \in \mathbb{K}$.

Alors

$$P(X) = a(X - x_1) \ldots (X - x_n) = a \prod_{k=1}^{n} (X - x_k)$$

Démonstration :
Récurrence sur n et corollaire du théorème de la caractérisation des racines par la divisibilité. □

Ce théorème est le premier pas vers le théorème fondamental de l'arithmétique 4.5 qui est une généralisation de ce théorème. Le but de la suite de cette partie est donc de poursuivre l'étude amorcée ici et d'aboutir à un théorème le plus général possible.

Exemple 3.2 :
Soit $P \in \mathbb{R}_3[X]$ unitaire tel que $\forall k \in \{1, 2, 3\}$, $\widetilde{P}(k) = k$. Déterminer P.

3.2 Racines multiples

Définition 3.1 (Racine multiple [✓]) :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

On dit que a est une racine multiple de P si $(X - a)^2 | P$.

Définition-Propriété 3.2 (Multiplicité [✓]) :
Soit $P \in \mathbb{K}[X]$, $P \neq 0$ et $a \in \mathbb{K}$.

Si a est une racine de P, on appelle multiplicité de a (en tant que racine de P) le plus grand entier $m \in \mathbb{N}$ tel que $(X-a)^m | P$. Autrement dit, la multiplicité de a en tant que racine de P, est

$$m = \max\{n \in \mathbb{N},\ (X-a)^n | P\}.$$

Démonstration :
Si $P = 0$, il n'y a rien à faire. Si $P \neq 0$. L'ensemble $\{k \in \mathbb{N}, (X-a)^k | P\}$ est une partie de $\mathbb{N}$ non vide (0 est dedans) et majoré (par le degré de P). Donc elle admet un maximum dans $\mathbb{N}$ qu'on appelle multiplicité de a. □

Remarque :
On a automatiquement l'unicité de la multiplicité d'une racine a donnée d'un polynôme P donné.

Définition 3.3 (Racine simple, racine double [✓]) :
On appelle racine simple, une racine de multiplicité 1. On appelle racine double, une racine de multiplicité 2.

Proposition 3.6 (Caractérisation des racines multiples par la division [✓]) :
Soit $P \neq 0 \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ une racine de P.

a est une racine multiple de P de multiplicité m si et seulement si $(X-a)^m | P$ et $(X-a)^{m+1} \nmid P$.

Démonstration :
Si a est une racine de multiplicité m de P, alors $m = \max\{k \in \mathbb{N}, (X-a)^k | P\}$. Donc $(X-a)^m | P$ puisque c'est un max et $(X-a)^{m+1} \nmid P$ sinon m ne serait pas un max.

Réciproquement, a est bien sûr une racine de P et on a clairement $m \in \{k \in \mathbb{N}, (X-a)^k | P\}$. Si $n \geq m+1$, alors $(X-a)^{m+1} | (X-a)^n$. Mais $(X-a)^{m+1} \nmid P \implies (X-a)^n \nmid P$. Donc m est la multiplicité de a. □

On peut aussi définir la multiplicité comme

$$m+1 = \min\{k \in \mathbb{N}, (X-a)^k \not| P\}$$

Corollaire 3.7 (Reformulation de la caractérisation des racines multiples par les divisions [✓]) :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est une racine de P de multiplicité m si et seulement si $\exists Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^m Q(X)$ et $\widetilde{Q}(a) \neq 0$.

Démonstration :
Corollaire immédiat de la proposition précédente □

Exemple 3.3 :
Montrer que i est une racine multiple de $(X^4-1)^n$ et déterminer sa multiplicité.

Remarque :
Une racine de multiplicité 0 n'est pas une racine. En effet, cela veut dire que $(X-a)^0 = 1 | P$ et $(X-a)^1 \not| P$. Donc a n'est pas une racine. Mais on utilisera pas (ou peu) ce résultat. La notion de multiplicité n'a d'intérêt que pour une "vraie" racine.

Proposition 3.8 :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ et $m \in \mathbb{N}$ tel que $(X-a)^m | P$.
Alors a est une racine de P de multiplicité au moins m.

Démonstration :
Évident par la définition de la multiplicité □

Remarque :
Attention à l'inégalité sur la multiplicité !

Proposition 3.9 :
Soit $P \in \mathbb{K}[X]$ et $a_1, \dots, a_n \in \mathbb{K}$ des racines de P deux à deux distinctes de multiplicités respectives $\alpha_1, \dots, \alpha_n$. Alors

$$(X - a_1)^{\alpha_1} \dots (X - a_n)^{\alpha_n} | P$$

Démonstration :
On sait que $(X - a_1)^{\alpha_1} | P(X)$. Donc $P(X) = (X - a_1)^{\alpha_1} Q(X)$. Maintenant $(X - a_2)^{\alpha_2} | (X - a_1)^{\alpha_1} Q(X)$. Mais $(X - a_2)^{\alpha_2}$ et $(X - a_1)^{\alpha_1}$ sont premiers entres eux. Donc $(X - a_2)^{\alpha_2} | Q(X)$ grâce au théorème de Gauss.

Et par récurrence, on aboutit au résultat. □

Proposition 3.10 (Nombre de racines comptées avec multiplicité [✓]) :
Soit $P \in \mathbb{K}[X]$, $P \neq 0$.

Le nombre de racines de P compté avec multiplicité est inférieur ou égal au degré de P, *i.e.* Si $a_1, \dots, a_n$ sont les racines de P distinctes de multiplicité respectives $m_1, \dots, m_n$, alors

$$\sum_{k=1}^{n} m_k \leq \deg P$$

Démonstration :
On sait $(X - a_1)^{m_1} \dots (X - a_n)^{m_n} | P$ donc $\sum_{k=1}^{n} m_k \leq \deg P$ en prenant les degré. □

Proposition 3.11 (Polynôme nul par nombre de racines [✓]) :
Soit $P \in \mathbb{K}[X]$ de degré $d \in \mathbb{N} \cup \{-\infty\}$.

Si la somme des multiplicités des racines de P est $> d$, alors $P = 0$.

Démonstration :
Par l'absurde avec la proposition précédente. □

Proposition 3.12 (Racines et conjugaison) :
Soit $P \in \mathbb{C}[X]$ et $a \in \mathbb{C}$ et $m \in \mathbb{N}^*$. On a équivalence entre

(i) a est une racine de P de multiplicité m

(ii) $\overline{a}$ est une racine de $\overline{P}$ de multiplicité m

Démonstration :
On a

$$(X-a)^m | P(X) \iff (X-\overline{a})^m \Big| \overline{P}(X)$$

□

Exemple 3.4 :
Soit $P \in \mathbb{R}_2[X]$ unitaire tel que $\widetilde{P}(i) = 0$. Déterminer P.

Proposition 3.13 (Racines d'un PGCD) :
Soit $A, B \in \mathbb{K}[X]$, $(A, B) \neq (0, 0)$.

Les racines d'un PGCD sont les racines communes de A et B, de multiplicité, le minimum des multiplicité

Démonstration :
Comme un PGCD divise A et B, par transitivité de la divisibilité et par caractérisation des racines par divisibilité, les racines d'un PGCD sont racines de A et de B. Donc des racines communes.

Ensuite, il suffit de regarder les multiplicités. Si m est la multiplicité d'une racine d'un PGCD de A et B, alors $(X-a)^m | A$ et $(X-a)^m | B$. Donc la multiplicité de a en tant que racine de A et de B est supérieure à celle en tant que racine d'un PGCD. Et par maximalité des degrés, on a ce qu'on veut. □

Proposition 3.14 :
Soit $P \in \mathbb{K}[X]$ de degré $d \in \mathbb{N}$.

Si P admet d racines distinctes, alors ce sont toutes les racines de P et elles sont toutes simples.

Démonstration :
P ne pas avoir plus de racines comptés avec multiplicité que son degré. Comme il en a déjà d distinctes, elles ne peuvent pas être de multiplicité plus grande que 1 et donc elles sont toutes simples. Et on en a le nombre maximum. □

Remarque :
Ce théorème est surtout utile pour trouver la factorisation d'un polynôme.

Exemple 3.5 :
Soit $n \in \mathbb{N}^*$. Montrer que

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right)$$

Remarque :
Ce théorème est les prémices des ennuis qui arrivent juste en dessous. C'est aussi le point de départ le point de départ de la construction du théorème fondamental de l'arithmétique.

3.3 Racines multiples et dérivation

Théorème 3.15 :
Soit $P \in \mathbb{K}[X]^*$ et $a \in \mathbb{K}$ une racine de P de multiplicité $m \geq 1$.
Alors a est une racine de P' de multiplicité $m-1$.

Démonstration :
On sait qu'on peut écrire $P(X) = (X-a)^m Q(X)$ avec $\widetilde{Q}(a) \neq 0$. En dérivant, on trouve $P'(X) = m(X-a)^{m-1}Q(X) + (X-a)^m Q'(X) = (X-a)^{m-1}(mQ(X) + (X-a)Q'(X))$. On pose $R(X) = mQ(X) + (X-a)Q'(X)$. Et $\widetilde{R}(a) = m\widetilde{Q}(a) \neq 0$. Donc a est une racine de multiplicité $m-1$ de P'. □

Corollaire 3.16 (Caractérisation des racines simples par la dérivée) :
Soit $P \in \mathbb{K}[X]^*$.
Les racines simples de P sont exactement les racines de P qui ne sont pas des racines de P'.

Démonstration :
La proposition précédente montre que les racines de P de multiplicité ≥ 2 sont également des racines de P'. Et donc les racines simples de P ne sont pas des racines de P'. En effet, si a est une racine simple de P, alors $P(X) = (X-a)Q(X)$ avec $\widetilde{Q}(a) \neq 0$. En dérivant, $P'(X) = Q(X) + (X-a)Q'(X)$. Alors $\widetilde{P'}(a) = \widetilde{Q}(a) \neq 0$. □

Exemple 3.6 :
Montrer que les racines de $P(X) = X^3 + 3X + 1 \in \mathbb{C}[X]$ sont simples (sans les calculer).

Corollaire 3.17 (Caractérisation des racines simples) :
Soit $P \in \mathbb{C}[X]$.
Les racines de P sont simples si, et seulement si, P et P' sont premiers entres eux.

Démonstration :
Cela vient de la proposition précédente. □

Théorème 3.18 (Caractérisation des racines multiples par les dérivées [✓]) :
Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $a \in \mathbb{K}$ et $m \geq 1$. On a équivalence entre :
(i) a est une racine de P de multiplicité m
(ii) $\widetilde{P}(a) = \widetilde{P'}(a) = \widetilde{P''}(a) = \cdots = \widetilde{P^{(m-1)}}(a) = 0$ et $\widetilde{P^{(m)}}(a) \neq 0$.

Démonstration :
$\boxed{(i) \implies (ii)}$ Comme a est une racine d'ordre m de P, on sait qu'il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^m Q(X)$ avec $\widetilde{Q}(a) \neq 0$. En utilisant la formule de Leibniz pour dériver ce produit,

on trouve $P^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \frac{m!}{(m-i)!}(X-a)^{m-i}Q^{(n-i)}(X)$. En particulier, pour $n = m-1$ on a :

$$\begin{aligned} P^{(m-1)}(X) &= \sum_{k=0}^{m-1} \binom{m-1}{k} \frac{m!}{(m-k)!}(X-a)^{m-k}Q^{(m-1-k)}(X) \\ &= (X-a)\sum_{k=0}^{m-1} \binom{m-1}{k} \frac{m!}{(m-k)!}(X-a)^{m-1-k}Q^{(m-1-k)}(X) \\ &= (X-a)\sum_{k=1}^{m} \binom{m-1}{k-1} \frac{m!}{(m-k-1)!}(X-a)^{m-k}Q^{(m-k)}(X) \end{aligned}$$

et pour $n = m$, on a :

$$\begin{aligned} P^{(m)}(X) &= \sum_{k=0}^{m} \binom{m}{k} \frac{m!}{(m-k)!}(X-a)^{m-k}Q^{(m-k)}(X) \\ &= (X-a)\sum_{k=0}^{m-1} \binom{m}{k} \frac{m!}{(m-k)!}(X-a)^{m-k-1}Q^{(m-k)}(X) + m!Q(X) \\ &= (X-a)\sum_{k=1}^{m} \binom{m}{k-1} \frac{m!}{(m-k-1)!}(X-a)^{m-k}Q^{(m-k+1)}(X) + m!Q(X) \end{aligned}$$

Donc $\widetilde{P^{(m-1)}}(a) = 0$ et $\widetilde{P^{(m)}}(a) = m!\widetilde{Q}(a) \neq 0$.

$\boxed{(ii) \implies (i)}$ La formule de Taylor nous donne :

$$\begin{aligned} P(X) &= \sum_{k=0}^{+\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k \\ &= \sum_{k=m}^{+\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k \\ &= (X-a)^m \sum_{k=m}^{+\infty} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^{k-m} \\ &= (X-a)^m \sum_{k=0}^{+\infty} \frac{\widetilde{P^{(m+k)}}(a)}{(m+k)!}(X-a)^k \end{aligned}$$

On pose $Q(X) = \sum_{k=0}^{+\infty} \frac{\widetilde{P^{(m+k)}}(a)}{(m+k)!}(X-a)^k$. Alors $\widetilde{Q}(a) = \frac{\widetilde{P^{(m)}}(a)}{m!} \neq 0$. Donc a est une racine multiple de P d'ordre m. □

Exemple 3.7 :
Montrer que $\forall n \in \mathbb{N}^*$, $(X-1)^3$ divise le polynôme $nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.

4 Polynômes scindés

Dans cette section, on va commencer à faire une distinction entre $\mathbb{R}$ et $\mathbb{C}$. On va d'abord donner quelques résultats généraux (mais ils sont presque tous déjà donnés au dessus). Et on va spécifier l'étude des polynômes selon que l'on se place sur $\mathbb{R}$ ou sur $\mathbb{C}$. Les choses seront assez différentes sur les deux corps. Il faudra faire attention à ne pas mélanger les deux cas (et on aura des résultats qui le feront ...)

4.1 Définition

Définition 4.1 (Polynôme scindé [✓]) :
Un polynôme $P \in \mathbb{K}[X]$ non constant est dit scindé s'il peut s'écrire comme le produit de polynômes de degré 1 de $\mathbb{K}[X]$, *i.e.* si $\exists a \in \mathbb{K}^*$, $\exists n \in \mathbb{N}^*$, $\exists x_1, \dots, x_n \in \mathbb{K}$ deux à deux distincts, $\exists m_1, \dots, m_n \in \mathbb{N}^*$ tel que $P(X) = a(X - x_1)^{m_1} \dots (X - x_n)^{m_n} = a \prod_{k=1}^{n} (X - x_k)^{m_k}$.

Remarque :
Dans ce cas, a est le coefficient dominant de P et $x_1, \dots, x_n$ sont ses racines.

!!! ATTENTION !!!

⚠ La notion de polynôme scindé dépend entièrement du corps sur lequel on se place. Il ne se passe pas la même chose sur $\mathbb{R}$ et sur $\mathbb{C}$. Voir l'exemple suivant. Il est impératif de la garder en tête.

Exemple 4.1 :
Le polynôme $X^2 + 1$ est un polynôme de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$. Vu comme un polynôme de $\mathbb{C}[X]$, c'est un polynôme scindé car $X^2 + 1 = (X + i)(X - i)$ dans $\mathbb{C}[X]$. Mais ce polynôme n'a pas de racines dans $\mathbb{R}$ donc il ne peut pas être scindé dans $\mathbb{R}[X]$.

Théorème 4.1 (Caractérisation des polynômes scindés par les multiplicités [✓]) :
Soit $P \in \mathbb{K}[X]$ un polynôme de degré ≥ 1. On a équivalence entre

(i) P est scindé dans $\mathbb{K}[X]$

(ii) La somme des multiplicité des racines de P est égale à son degré.

Démonstration :
$\boxed{(i) \implies (ii)}$ Comme P est scindé, on peut l'écrire $P(X) = a\prod_{k=1}^{n}(X - x_k)^{m_k}$ avec $a \in \mathbb{K}^*$, $x_1, \dots, x_n \in \mathbb{K}$ et $m_1, \dots, m_n \in \mathbb{N}^*$. On a donc $\deg P = \sum_{k=1}^{n} m_k$.

$\boxed{(ii) \implies (i)}$ Soit $x_1, \dots, x_n \in \mathbb{K}$ les racines de P de multiplicité $m_1, \dots, m_n \in \mathbb{N}^*$. Alors $\prod_{k=1}^{n}(X - x_k)^{m_k} \Big| P(X)$. Donc $P(X) = Q(X)\prod_{k=1}^{n}(X - x_k)^{m_k}$. Alors $\deg P = \deg Q + \sum_{k=1}^{n} m_k$. Mais la somme des multiplicité des racines de P est égale au degré de P, donc $\deg Q = 0$ donc $Q(X) = a \in \mathbb{K}^*$ et donc $P(X) = a\prod_{k=1}^{n}(X - x_k)^{m_k}$. Donc P est scindé. □

Remarque :
Attention, ici on a choisi de décrire les racines de P avec les multiplicités. C'est rarement le cas. On aurait pu aussi dire que P est scindé s'il s'écrit sous la forme $P(X) = a\prod_{k=1}^{n}(X - x_k)$. Dans cette définition on ne précise pas que les x_i sont distincts. Donc la même valeurs peut apparaître plusieurs fois. Et si une racine a une multiplicité, elle va donc devoir apparaître dans la liste $(x_1, \dots, x_n)$ autant de fois que sa multiplicité.

Exemple 4.2 :
Soit $P \in \mathbb{R}[X]$ tel que $\deg(P) = 3$ et $\frac{\widetilde{P}(x)}{x} \xrightarrow[x\to 0]{} 0$. Montrer que P est scindé.

Proposition 4.2 (PGCD avec un polynôme scindé) :
Soit $A, B \in \mathbb{K}[X]$, $(A, B) \neq (0, 0)$. Supposons que A ou B est scindé.
$A \wedge B = 1 \iff A$ et B n'ont pas de racines communes.

Démonstration :
Si $A \wedge B = 1$ alors A et B n'ont pas de racines communes à cause de Bézout (et ça ne dépend pas que l'un des deux soit scindé). Et s'ils n'ont pas de racines communes, comme l'un des deux est scindés, tout ses diviseurs le sera également. En particulier, $A \wedge B$ est scindé. Et donc $A \wedge B$ a les racines communes de A et B qui n'existent pas. Et donc $A \wedge B = 1$. □

4.2 Factorisation dans $\mathbb{C}$

Nous allons essayer de "combler les trous" de la partie précédente dans les deux parties qui suivent.

On a commencé à expliquer comment faire pour factoriser un polynômes. Mais pour cela, on a besoin de connaître toutes les racines d'un polynômes. Mais il faut connaître les racines. Il reste donc à prévoir le nombre de racines qu'il faut chercher. Si l'on arrive à prévoir le nombre de racines d'un polynôme, on peut alors recoller avec les théorèmes précédents pour prévoir si un polynôme est scindé ou pas.

Ensuite, pour le factoriser réellement, factuellement, il faudra alors trouver exactement les racines. Mais comme on saura exactement combien en chercher, la tâche sera plus aisée (dès qu'on en trouve le bon nombre, c'est qu'on les a toutes).

Remarque :
ATTENTION ! Il y a un problème de comptage ici que nous avons déjà touché du doigts dans la partie précédente. Il faut être clair sur ce que l'on entend par "compter les racines". Compter les racines distinctes n'est pas la même chose que compter les racines avec leur multiplicités.

4.2.1 Théorème de D'Alembert-Gauss

Théorème 4.3 (Théorème de D'Alembert-Gauss [✓]) :
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Remarque (HP) :
On dit que $\mathbb{C}$ est un corps algébriquement clos.

On admet ce théorème. La démonstration est officiellement hors programme. Il y a plusieurs démonstrations possibles mais aucune n'est accessible avec le bagage mathématique de première année. Certaines démo seront accessibles en seconde année, notamment avec les fonctions de plusieurs variables ou le théorème d'inversion locale. La méthode la plus simple serait de montrer que la fonction polynomiale associée à un polynôme complexe de degré ≥ 1 admet un minimum en z_0 (il y a une astuce à utiliser et il faut montrer que cette fonction est continue sur un compact, ce qui nécessite d'utiliser des fonctions de plusieurs variables). En raisonnant ensuite par l'absurde, on suppose que z_0 n'est pas une racine de P et on montre qu'il existe $c \in \mathbb{C}$ tel que $\forall t \in \mathbb{R}$, $|P(z_0 + tc)| < |P(z_0)|$, ce qui est clairement absurde. Et on peut alors conclure.

Corollaire 4.4 (Polynôme irréductible sur $\mathbb{C}$ [✓]) :
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1

Ce corollaire est TRÈS important ! Il permet de tout faire. Il est l'alpha et l'oméga dans $\mathbb{C}[X]$.

Démonstration :
Soit $P \in \mathbb{C}[X]$ un polynôme irréductible. Il n'est donc pas constant donc de degré ≥ 1. Supposons qu'il soit de degré $d \geq 2$. Par le théorème de D'Alembert-Gauss, P admet donc au moins une racine

$a \in \mathbb{C}$. Donc $P(X) = (X-a)Q(X)$ avec $\deg Q = d-1$. Donc Q n'est pas une constante. Et donc P est divisible par $X-a$ donc il n'est pas irréductible. Ce qui aboutit clairement à ☠. Donc P n'est pas de degré $d \geq 2$ donc P est de degré 1. □

Remarque :
Dans tous les corps que l'on considère, les polynômes de degré 1 sont toujours des polynômes irréductibles. Mais dans $\mathbb{C}[X]$, ce sont les seuls, on vient de donner la liste de tous les polynômes irréductibles de $\mathbb{C}[X]$. Tous les polynômes de degré sont irréductibles (on le savait déjà), mais on vient de montrer que ce sont les seuls. Or les polynômes irréductibles sont les parpaings élémentaires de la factorisation des polynômes.

Exemple 4.3 :
Montrer que le polynômes $X^4 - 5X^2 + 3$ n'est pas irréductible dans $\mathbb{C}[X]$.

Exemple 4.4 ([✓]) :
Décomposer $X^n - 1$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$, pour $n \geq 1$.

4.2.2 Décomposition en facteurs irréductibles dans $\mathbb{C}[X]$

Théorème 4.5 (Théorème fondamental de l'algèbre dans $\mathbb{C}[X]$ [✓]) :
Soit $P \in \mathbb{C}[X]$ non constant.
Alors $\exists a \in \mathbb{C}^*$, $\exists n \in \mathbb{N}^*$, $\exists x_1, \ldots, x_n \in \mathbb{C}$ deux à deux distincts et $\exists m_1, \ldots, m_n \in \mathbb{N}^*$ tels que

$$P(X) = a \prod_{k=1}^{n} (X - x_k)^{m_k}$$

De plus, cette décomposition est unique à l'ordre des facteurs près

La décomposition est donc unique à une permutation sur l'ensemble des racines près. C'est les valeurs des racines qui est unique, pas l'ordre dans lequel on énumère les racines en questions.

Cette décomposition est le parallèle du théorème fondamental de l'arithmétique qui donne la décomposition d'un entier en produit de facteurs premiers (unique aussi à l'ordre des facteurs premiers près).

Démonstration :
Comme P est non contant, il est de degré $d \geq 1$. Donc, par théorème de D'Alembert-Gauss, il possède au moins une racine $x_1 \in \mathbb{C}$. Cette racine est donc d'une certaine multiplicité $m_1 \in \mathbb{N}^*$. Alors $P(X) = Q(X)(X - x_1)^{m_1}$. Si $m_1 < \deg P$, alors $\deg Q \geq 1$ et on peut appliquer le même raisonnement à Q etc jusqu'à n'obtenir qu'une constante qui sera nécessairement non nul (on a une suite de degré strictement décroissante). □

Remarque :
En fait, ce théorème est équivalent au théorème de D'Alembert-Gauss. Ce théorème est donc une reformulation du théorème de D'Alembert-Gauss.

Corollaire 4.6 ([✓]) :
Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.

C'est juste le théorème précédent formulé différemment.

Ce résultat n'est valable QUE dans $\mathbb{C}[X]$. Penser à $X^2 + 1$.

Corollaire 4.7 (Nombres de racines dans $\mathbb{C}$ [✓]) :
Tout polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}$ possède exactement n racines comptées avec multiplicité.

Ça aussi, c'est une autre reformulation du théorème fondamental de l'algèbre.

Exemple 4.5 :
Factoriser dans $\mathbb{C}[X]$ les polynômes $X^2 - 2X\cos\theta + 1$, $X^n - 1$ et $X^4 + X^2 + 1$.

4.2.3 Arithmétiques et racines dans $\mathbb{C}$

Proposition 4.8 :
Soit $A, B \in \mathbb{C}[X]$. On a équivalence entre

1. $A|B$
2. Les racines de A sont racines de B et leur multiplicité en tant que racine de A est inférieur ou égale à leur multiplicité en tant que racine de B

Si on essaie d'écrire ça, ça donnerait : $\exists a \in \mathbb{C}^*$, $\exists x_1, \dots, x_n \in \mathbb{C}$, $\exists m_1, \dots, m_n, m'_1, \dots, m'_n \in \mathbb{N}^*$, $\exists Q \in \mathbb{C}[X]$ tels que $A(X) = a\prod_{k=1}^{n}(X - x_k)^{m_k}$ et $B(X) = Q(X)\prod_{k=1}^{n}(X - x_k)^{m'_k}$ avec $m_k \leq m'_k$ pour tout $k \in \{1, \dots, n\}$.

Démonstration :
Si A est une constante, il n'y a rien à faire. On suppose donc désormais que A est de degré ≥ 1. Par le théorème de d'Alembert-Gauss, on peut écrire $A(X) = a\prod_{k=1}^{n}(X - x_k)^{m_k}$ pour un certain $a \in \mathbb{C}^*$, $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in \mathbb{C}$, $m_1, \dots, m_n \in \mathbb{N}^*$.

$\boxed{(i) \implies (ii)}$ Si $A|B$, on a facilement que $x_1, \dots, x_n$ sont des racines de B de multiplicité au moins $m_1, \dots, m_n$.

$\boxed{(ii) \implies (i)}$ Si les $x_1, \dots, x_n$ sont des racines B de multiplicité supérieur ou égales à $M_1, \dots, m_n$, alors $\prod_{k=1}^{n}(X - x_k)^{m_k}$ divise B et donc $A|B$. □

Exemple 4.6 :
Montrer que $X^4 + X^2 + 1 | X^{18} - 1$.

Proposition 4.9 (Caractérisation de polynômes premiers entre eux dans $\mathbb{C}[X]$ [✓]) :
Soit $A, B \in \mathbb{C}[X]$. On a équivalence entre :

(i) A et B sont premiers entres eux

(ii) A et B n'ont pas de racines communes.

Démonstration :
On va démontrer ce théorème par contraposée dans les deux sens.

$\boxed{(i) \implies (ii)}$ On suppose donc que A et B ont au moins une racine en commun. Donc $\exists \alpha \in \mathbb{C}$ tel que $\widetilde{A}(\alpha) = \widetilde{B}(\alpha) = 0$. donc $(X - \alpha)|A$ et $(X - \alpha)|B$. Donc A et B ont un diviseur commun dans $\mathbb{C}[X]$ qui n'est pas constants donc A et B ne sont pas premiers entres eux.

$\boxed{(ii) \implies (i)}$ On suppose que A et B ne sont pas premiers entres eux. Donc ils ont un facteurs communs $P \in \mathbb{C}[X]$ de degré ≥ 1. Par théorème de d'Alembert-Gauss, P admet au moins une racine qui sera donc une racine de A et de B aussi, par divisibilité. □

Exemple 4.7 :
Montrer que $X^2 + 1$ et $X^3 + X + 1$ sont premiers entres eux.

!!! ATTENTION !!!

⚠ Ces résultats ne sont valables QUE sur $\mathbb{C}$. C'est la forme particulière des polynômes irréductibles de $\mathbb{C}$ qui fait tout le travail (dû à d'Alembert-Gauss). Mais ailleurs (par ailleurs j'entends particulièrement $\mathbb{R}$) tout ceci est faux. Les choses sont plus compliqués. Donc attention au corps sur lequel vous vous placez.

4.3 Cas réel

4.3.1 Premiers liens avec $\mathbb{C}$

Remarque :
Il est clair que $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Définition 4.2 (Racine complexe) :
Soit $P \in \mathbb{R}[X]$.
On appelle racine complexe de P toute racine de P vu dans $\mathbb{C}[X]$.

Remarque :
La définition précise des racines complexes d'un polynôme réel n'est pas très clair. L'intérêt est d'étendre le corps de base pour rajouter des racines et donc de considérer les racines complexes non réelles. Mais avec uniquement ces racines, on ne peut pas faire grand chose. Il faut toutes les racines

de P (réelles et complexes non réelles) pour pouvoir le factoriser correctement dans $\mathbb{C}[X]$ par le théorème fondamental de l'arithmétique. Donc a priori, les racines complexes devraient plutôt être toutes les racines de P vu comme polynôme de $\mathbb{C}[X]$. Seulement, comme $P \in \mathbb{R}[X]$, on a souvent déjà calculer les racines réelles et le but est donc d'étudier les racines "qui manque", donc les racines non réelles. Etc.

Bref, les deux sont intéressants. Ça dépend un peu du contexte. Comme il est usuel de changer de corps régulièrement (ce que nous sommes en train d'amorcer), selon le corps dans lequel on se place, on considère l'une ou l'autre définition. Si on garde $P \in \mathbb{R}[X]$ et qu'on le traite en tant que tel, on peut chercher ses racines non réelles (on fait une petite incartade timide dans le monde des complexes). Mais on peut aussi décider de faire les chose un peu brutalement et voir P dans $\mathbb{C}[X]$ pour pouvoir utiliser les outils dont on dispose dans $\mathbb{C}[X]$. Auquel cas, les racines complexes de P feraient plutôt référence à toutes les racines de P, réelles ou non réelles.

Exemple 4.8 :
On a $X^2 + X + 1 \in \mathbb{R}[X]$ et j est une racine complexe de ce polynôme.

Proposition 4.10 (Nombres de racines complexes [✓]) :
Soit $P \in \mathbb{R}[X]$ de degré $n \in \mathbb{N}$
P possède exactement n racines complexes comptées avec multiplicité.

Démonstration :
Si $P \in \mathbb{R}[X]$, alors $P \in \mathbb{C}[X]$ et on a 4.7. □

La force des polynômes réels (donc leurs intérêts et donc leurs embêtements) est que l'on peut les voir comme des polynômes complexes et leur appliquer la batterie de résultats sympathiques qu'on a dans le cas complexes. Il faut juste ne pas oublier de repasser dans $\mathbb{R}$ donc de transposer ces résultats dans $\mathbb{R}$. C'est à cette étape qu'il faut prendre des gants.

Proposition 4.11 (Racines non réelles d'un polynôme réel [✓]) :
Les racines complexes non réelles d'un polynôme réel sont deux à deux conjuguées et deux racines complexes conjuguées ont même multiplicité.

Démonstration :
Soit $P \in \mathbb{R}[X]$. Si $a \in \mathbb{C} \setminus \mathbb{R}$ est une racine de P de multiplicité m, alors $\overline{a}$ est une racine de multiplicité m du polynôme $\overline{P} = P$. □

Exemple 4.9 :
Soit $P \in \mathbb{R}[X]$ unitaire de degré 3 tel que $\widetilde{P}(2i) = 0$ et $\widetilde{P}(0) = 1$. Déterminer P.

4.3.2 Décomposition en facteurs irréductibles dans $\mathbb{R}[X]$

Lemme 4.12 (Relations de divisibilité sur $\mathbb{R}$ vu dans $\mathbb{C}$) :
Soit $A, B \in \mathbb{R}[X]$. Alors

$$A|B \text{ dans } \mathbb{R}[X] \iff A|B \text{ dans } \mathbb{C}[X]$$

Démonstration :
$\boxed{\Rightarrow}$ Donc il existe $P \in \mathbb{R}[X]$ tel que $B = AP$. Mais $A, B, P \in \mathbb{C}[X]$ aussi, donc on a $A|B$ dans $\mathbb{C}[X]$.

$\boxed{\Leftarrow}$ On suppose que $\exists P \in \mathbb{C}[X]$ tel que $B = AP$. Par décomposition en facteurs irréductibles dans $\mathbb{C}[X]$, on sait que $\exists n \in \mathbb{N}$, $\exists x_1, \dots, x_n \in \mathbb{C}$, $\exists m_1, \dots, m_n \in \mathbb{N}^*$ et $a \in \mathbb{C}^*$ tel que $P(X) = a\prod_{k=1}^{n}(X-x_k)^{m_k}$. Donc $B(X) = aA(X)\prod_{k=1}^{n}(X-x_k)^{m_k}$. Donc les x_k sont des racines de B. Mais étant réels, ses racines complexes (non réelles) sont deux à deux conjuguées et de même multiplicité. Donc $\forall k \in \{1, \dots, n\}$, soit $x_k \in \mathbb{R}$, soit $\exists j \in \{1, \dots, n\} \setminus \{k\}$ tel que $x_j = \overline{x_k}$ et $m_j = m_k$. Et dans ce cas $\prod_{k=1}^{n}(X - x_k)^{m_k} \in \mathbb{R}[X]$. Enfin, comme $A, B, \prod_{k=1}^{n}(X - x_k)^{m_k} \in \mathbb{R}[X]$, on en déduit que $a \in \mathbb{R}^*$ également sinon on aboutirait à ☠ (observer le coefficients dominant de B par exemple). Donc $P(X) = a\prod_{k=1}^{n}(X - x_k)^{m_k} \in \mathbb{R}[X]$ et donc la relation de divisibilité est valable dans $\mathbb{R}[X]$ donc $A|B$ dans $\mathbb{R}[X]$. □

Remarque :
On rappel que la notion de divisibilité est intrinsèquement lié au corps de base. Pour que ce soit plus clair, on aurait pu (dû ?) noté la relation de divisibilité dans $\mathbb{K}[X]$ par $|_{\mathbb{K}}$ (ou mieux $|_{\mathbb{K}[X]}$) pour insister sur le fait que cette relation n'est valable que dans $\mathbb{K}[X]$. Mais cela aurait alourdi les notations. Et cette notation n'est pas canonique, alors ....

Cependant, vous pouvez parfaitement la définir en début de problème et l'utiliser comme bon vous semble si ça peut vous aider à garder l'esprit clair.

Exemple 4.10 :
Montrer que $(X^2 + 1)|(X^3 - X^2 + X - 1)$ dans $\mathbb{R}[X]$.

Théorème 4.13 (Polynômes irréductibles de $\mathbb{R}[X]$ [✓]) :
Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

(i) Les polynômes de degré 1

(ii) Les polynômes de degré 2 de discriminant < 0.

Ce théorème est fondamental. C'est de lui que viennent les ennuis et donc toute la suite de cette partie. C'est plus particulièrement les polynômes irréductibles du second types qui causent toutes les perturbations.

Démonstration :
Montrons d'abord que ce sont des polynômes irréductibles. Soit $P \in \mathbb{R}[X]$. Si $\deg P = 1$, alors P est irréductible dans $\mathbb{C}[X]$ donc il l'est forcément dans $\mathbb{R}[X]$. En effet, s'il ne l'était pas dans $\mathbb{R}[X]$ il aurait un diviseur non trivial dans $\mathbb{R}[X]$ mais qui serait également un élément de $\mathbb{C}[X]$ (puisque $\mathbb{R}[X] \subset \mathbb{C}[X]$) et ne serait donc pas irréductibles dans $\mathbb{C}[X]$ ce qui aboutit à ☠ avec un corollaire de d'Alembert-Gauss.

Supposons maintenant que $\deg P = 2$ et qu'il est de discriminant < 0. Il n'a donc pas de racines réelles et ses deux racines complexes sont conjuguées. Considérons $D \in \mathbb{R}[X]$ un diviseur de P. Donc nécessairement, $\deg D \leq 2$. Si $\deg D = 2$ ou 0 c'est un diviseur trivial de P. Mais si $\deg D = 1$, alors D a nécessairement une racine dans $\mathbb{R}$ qui sera donc aussi une racine réelle de P. Et là, ☠. Donc $\deg D \neq 1$ et donc c'est un diviseur trivial. Donc P est irréductible.

Réciproquement, montrons que tout polynôme irréductible est de cette forme. Soit donc $P \in \mathbb{R}[X]$ irréductible. Donc $\deg P \geq 1$ car P est non constant. Donc en tant que polynôme de $\mathbb{C}[X]$, on peut lui appliquer le théorème de d'Alembert-Gauss et donc il admet au moins une racine α dans $\mathbb{C}$. Donc $(X-\alpha)|P(X)$ dans $\mathbb{C}[X]$. Si $\alpha \in \mathbb{R}$, alors $(X-\alpha)|P(X)$ dans $\mathbb{R}[X]$. Mais comme P est irréductible, $X-\alpha$ doit être un diviseurs trivial de P et donc P est de degré 1. Si $\alpha \notin \mathbb{R}$, alors $\overline{\alpha}$ est également racines de P. Donc $(X-\alpha)(X-\overline{\alpha})|P(X)$. Mais $(X-\alpha)(X-\overline{\alpha})$ est un polynôme à coefficient réel. Donc c'est un diviseurs de $P(X)$ dans $\mathbb{R}[X]$. Mais comme P est irréductible dans $\mathbb{R}[X]$, le polynôme $(X-\alpha)(X-\overline{\alpha})$ est un diviseurs trivial de P et donc P est de degré 2 sans racines réelles, *i.e.* il est de degré 2 de discriminant < 0. □

Exemple 4.11 :
Donner des exemples de polynômes irréductibles dans $\mathbb{R}[X]$. Quand est-il de $X^2 - 3X + 2$?

Théorème 4.14 (Théorème fondamental de l'algèbre dans $\mathbb{R}[X]$ [✓]) :
Soit $P \in \mathbb{R}[X]$ non constant. Alors $\exists \lambda \in \mathbb{R}^*$, $\exists n_1, n_2 \in \mathbb{N}$, $\exists a_1, \dots, a_{n_1} \in \mathbb{R}$ deux à deux distincts, $\exists (p_1, q_1), \dots, (p_{n_2}, q_{n_2}) \in \mathbb{R}^2$ deux à deux distincts tels que $\forall j \in \{1, \dots, n_2\}$, $\Delta_j = p_j^2 - 4q_j < 0$ et $\exists \alpha_1, \dots, \alpha_{n_1}, \beta_1, \dots, \beta_{n_2} \in \mathbb{N}^*$ tels que

$$P(X) = \lambda \prod_{k=1}^{n_1} (X - a_k)^{\alpha_k} \prod_{j=1}^{n_2} (X^2 + p_j X + q_j)^{\beta_j}$$

et cette décomposition est unique à l'ordre des facteurs près.

Démonstration :
Si $P(X) \in \mathbb{R}[X]$ de degré ≥ 1, c'est en particulier un polynôme non constant de $\mathbb{C}[X]$. Donc on peut lui appliquer la décomposition en facteurs irréductibles dans $\mathbb{C}[X]$. Puis on regroupe les facteurs de degré 1 avec des racines complexes conjuguées (dès qu'il y a une racines complexes non réelles, son conjuguée apparaît nécessairement avec la même multiplicité puisque P est à coefficient réel) ce qui nous donne la forme voulue. □

Remarque :
Avec cette décomposition on a également

$$\deg P = \sum_{k=1}^{n_1} \alpha_k + \sum_{j=1}^{n_2} 2\beta_j$$

donc le degré de P et la somme des multiplicités de ses facteurs irréductibles de degré 1 et du doubles des multiplicités de ses facteurs irréductibles de degré 2.

Remarque :
On rappelle qu'il y a toujours une légère ambiguïté lors du calcul du nombre de racine d'un polynôme. Soit on sous-entend qu'on s'intéresse aux racines distinctes, ou alors on prend en compte *toute* les racines et il faut alors les comptés avec leur multiplicité (une racine double compte 2 fois, une racine triple compte 3 fois etc).

Les théorèmes donnent des informations sur le nombre de racines comptés avec multiplicité. Mais avant de déterminer les multiplicités, il faut déjà trouver toutes les racines distinctes.

Corollaire 4.15 :
Tout polynôme réel de degré impair a au moins une racine réelle.

Démonstration :
On le montre par contraposée : si P n'a pas de racines réelles, alors, dans sa décomposition en

facteurs irréductibles dans $\mathbb{R}$, on a $n_1 = 0$ et donc $\deg P = \sum_{j=1}^{n_2} 2\beta_j$ donc P est de degré pair. □

Exemple 4.12 :
Factoriser dans $\mathbb{R}[X]$ le polynôme $X^5 - 1$.

Proposition 4.16 (Polynôme premiers entre eux) :
Soit $A, B \in \mathbb{R}[X]$.
Si $A \wedge B = 1$, alors A et B n'ont pas de racines communes.

Démonstration :
C'est le sens facile avec Bézout. □

!!! ATTENTION !!!

La réciproque est fausse dans $\mathbb{R}$. Il faut imposer d'avoir A ou B scindé pour que ça fonctionne.

Contre-exemple :
Prendre $A(X) = (X^2+1)(X^2+3)$ et $B(X) = (X^2+1)(X^2+2)$. Alors $A \wedge B = X^2 + 1$ et pourtant A et B n'ont pas de racines *réelles* communes.

4.4 Relations Racines / Coefficients

On retourne ici dans $\mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Proposition 4.17 (Relations coefficients/racines [✓]) :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ scindé dans $\mathbb{K}[X]$ et de degré $n \in \mathbb{N}^*$. Soit $x_1, \dots, x_n \in \mathbb{K}$ ses racines comptées avec multiplicités. Alors

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

Démonstration :
On a $P(X) = a_n \prod_{k=1}^{n} (X - x_k)$ car P est scindé sur $\mathbb{K}$. Le coefficient constant de P est alors donné par

$$a_0 = \widetilde{P}(0) = a_n \prod_{k=1}^{n} (0 - x_k) = (-1)^n \prod_{k=1}^{n} x_k$$

d'où la formule annoncée.

Le coefficient a_{n-1} est obtenu par le développement de la forme factorisée de P en ne sélectionnant qu'une seule parenthèse parmi les n disponible de laquelle on extrait la racine et les autres parenthèse donnant l'indéterminée X. La formule est alors obtenue en faisant varier la parenthèse fournissant la racine parmi toutes les parenthèse disponible.

$$a_{n-1} = a_n \sum_{k=1}^{n} -x_k = -a_n \sum_{k=1}^{n} x_k$$

□

Proposition 4.18 (Cas des polynômes de degré 2) :
Soit $P(X) = aX^2 + bX + c \in \mathbb{K}[X]$ scindé dans $\mathbb{K}[X]$ de racines x_1 et x_2. Alors

$$\frac{b}{a} = -x_1 - x_2 \qquad \text{et} \qquad \frac{c}{a} = x_1 x_2$$

Proposition 4.19 :
Soit $\alpha, \beta \in \mathbb{K}$. Les solutions du systèmes

$$\begin{cases} x + y = \alpha \\ xy = \beta \end{cases}$$

sont exactement les racines du polynômes $X^2 - \alpha X + \beta$.

Démonstration :
Si le système des solutions x et y dans $\mathbb{K}$, on considère le polynôme $P(X) = (X - x)(X - y)$. Alors

$P(X) = X^2 - (x+y)X + xy = X^2 - \alpha X + \beta$. Donc les solutions du systèmes sont bien les racines de ce polynômes.

Réciproquement, on considère le polynôme $P(X) = X^2 - \alpha X + \beta$. Si ce polynôme à une racine de $\mathbb{K}$, il en a nécessairement un deuxième et donc il est scindé dans $\mathbb{K}$. On note a et b ses racines. Donc on $P(X) = (X-a)(X-b)$ car P est unitaire. Et les relations racines/coefficients nous donne alors $a+b = \alpha$ et $ab = \beta$. Donc a et b sont bien des solutions du système. Et si P n'a pas de racines dans $\mathbb{K}$, le système n'a pas de solutions non plus par contraposée du premier paragraphe. □

Exemple 4.13 :
Résoudre les systèmes

$$\begin{cases} x + y = 5 \\ xy = -1 \end{cases}$$

et

$$\begin{cases} x - y = 2 \\ x^2 + y^2 = -2 \end{cases}$$

En fait, on peut définir des fonctions permettant d'éxprimer tous les coefficients en fonctions des racines pour un polynômes scindés. C'est ce qu'on appelle les fonctions symétriques élémentaires :

Définition (HP) 4.3 (*Fonctions symétriques élémentaires*)

Pour $n \in \mathbb{N}^*$ et $x_1, \dots, x_n \in \mathbb{K}$, on appelle fonctions symétriques élémentaires en les $x_1, \dots, x_n$ les fonctions

$$\sigma_1 = \sum_{k=1}^{n} x_k, \quad \sigma_2 = \sum_{1 \le i < j \le n} x_i x_j, \quad \sigma_3 = \sum_{1 \le i < j < k \le n} x_i x_j x_k,$$

et plus généralement,

$$\forall p \in \{1, \dots, n\},\ \sigma_p = \sum_{1 \le i_1 < \dots < i_p \le n} x_{i_1} x_{i_2} \dots x_{i_p}$$

et en particulier

$$\sigma_n = \prod_{k=1}^{n} x_k$$

Remarque :
σ_k contient $\binom{n}{k}$ termes dans la somme.

Avec ces notations, on a

Propriété (HP) 4.20 (*Relations coefficients/racines complètes*)

Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ scindé de degré $n \in \mathbb{N}^*$ et de racines $x_1, \ldots, x_n \in \mathbb{K}$ comptés avec multiplicité. Alors

$$\forall k \in \{0, \ldots, n\},\ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

En particulier, un polynôme unitaire de degré 2 avec deux racines et donné par $X^2 - \sigma_1 X + \sigma_2$. Un polynôme scindé unitaire de degré 3 est donné par $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$. Etc. On peut donc écrire

$$P(X) = a_3 X^3 + a2X^2 + a_1 X + a_0 = a_3(X - x_1)(X - x_2)(X - x_3)$$

dont on déduit en développant

$$-a_3 x_1 x_2 x_3 = -a_3\sigma_3 = a_0, \qquad a_3(x_1x_2 + x_1x_3 + x_2x_3) = a_3\sigma_2 = a_1,$$

$$-a_3(x_1 + x_2 + x_3) = -a_3\sigma_1 = a_2.$$

Exemple 4.14 :
Résoudre le système

$$\begin{cases} x + y + z = 2 \\ xy + xz + yz = -5 \\ xyz = -6 \end{cases}$$

Remarque :
En fait, on peut montrer que tout polynôme en $x_1, \ldots, x_n$ symétrique en $x_1, \ldots, x_n$ peut s'exprimer comme un polynôme en les $\sigma_1, \ldots, \sigma_n$.

Par exemple, $S_1 = \sum_{k=1}^{n} x_k = \sigma_1$; $S_2 = \sum_{k=1}^{n} x_k^2 = \sigma_1^2 - 2\sigma_2$; $S_3 = \sum_{k=1}^{n} x_k^3 = \sigma_1^3 - \sigma_1\sigma_2 - 3\sigma_3$. Etc.

4.5 Interpolation de Lagrange

L'interpolation est le principe de trouver une courbe passant par des points fixés du plan. En l'occurrence, on peut montrer qu'on peut toujours interpoler n'importe quel nuage de point deux à deux non alignés verticalement par un polynôme.

Définition 4.4 (Polynômes interpolateurs de Lagrange) :
Soit $n \in \mathbb{N}^*$ et soit $x_0, \dots, x_n \in \mathbb{K}$ deux à deux distincts.
On appelle le k-ème polynôme interpolateur de Lagrange en $(x_0, \dots, x_n)$ le polynôme

$$L_k(X) = \frac{\prod_{\substack{i=0 \\ i \neq k}}^{n} (X - x_i)}{\prod_{\substack{i=0 \\ i \neq k}}^{n} (x_k - x_i)}$$

Proposition 4.21 (Polynômes interpolateurs de Lagrange) :
Soit $n_i n \mathbb{N}^*$ et $x_0, \dots, x_n \in \mathbb{K}$ deux à deux distincts. On note $(L_0, \dots, L_n)$ les polynômes interpolateurs de Lagrange en $(x_0, \dots, x_n)$. Alors :

(i) $\forall i \in \{0, \dots, n\}$, $\deg(L_i) = n$.

(ii) $\forall i, j \in \{0, \dots, n\}$, $\widetilde{L_i}(x_j) = \delta_{i,j}$.

(iii) $(L_0, \dots, L_n)$ est une base de $\mathbb{K}_n[X]$.

Démonstration :
Il suffit de faire les calculs : Pour tout $i \in \{0, \dots, n\}$, $\deg(L_i) = \sum_{\substack{k=0 \\ k \neq i}}^{n} 1 = n$.

Le calcule montre aussi

$$\widetilde{L_i}(x_j) = \frac{\prod_{\substack{k=0 \\ k \neq i}}^{n} (x_j - x_k)}{\prod_{\substack{k=0 \\ k \neq i}}^{n} (x_i - x_k)} = \begin{cases} 0 & \text{si } i \neq j \\ 1 \text{si } i = j \end{cases}$$

Finalement, si $\lambda_0, \dots, \lambda_n \mathbb{K}$ tels que $\sum_{k=0}^{n} \lambda_k L_k = 0$, alors en évaluant en les x_i, on a $\lambda_i = 0$. Et donc la famille est libre. Or $\mathbb{K}_n[X]$ est de dimension $n+1$, donc par caractérisation des bases en dimension finie, $(L_0, \dots, L_n)$ est une base de $\mathbb{K}_n[X]$. □

Proposition 4.22 (Interpolation de Lagrange) :
Soit $n \in \mathbb{N}^*$ est $x_0, \dots, x_n, y_0, \dots, y_n \in \mathbb{K}$ avec $x_0, \dots, x_n$ deux à deux distincts.
Alors $\exists! P \in \mathbb{K}_n[X]$ tel que $\forall i \in \{0, \dots, n\}$, $\widetilde{P}(x_i) = y_i$ et c'est le polynôme

$$P(X) = \sum_{k=0}^{n} y_k L_k(X).$$

Démonstration :
On pose le polynôme P comme au dessus. Le calcul montre facilement $\widetilde{P}(x_i) = y_i$. L'unicité est

apporté par la liberté de la famille $(L_0, \dots, L_n)$. Sinon, on peut la voir autrement : Si P et Q ont les mêmes propriétés, alors $P - Q$ est un polynômes de degré $\leq n$ et ayant $n + 1$ racines distinctes. Donc $P - Q = 0$. □

Exemple 4.15 :
Soit $a_1, \dots, a_n \in \mathbb{R}_+$. Montrer qu'il existe un polynôme P tel que $\forall i \in \{1, \dots, n\}$, $\widetilde{P}(a_i) = \sqrt{a_i}$.