Chapitre 17

Polynômes

I Polynômes à coefficients réels

1) Ensemble $\mathbb{R}[X]$ des polynômes à coefficients réels

a) Définition

a_n n'est pas supposé non nul ! On le supposera parfois dans la suite, quand on supposera que P est de degré n (et donc a_n sera son coefficient dominant), mais, pour l'instant, les a_k sont quelconques, et éventuellement nuls.

Définition. *Une application $P : \mathbb{R} \longrightarrow \mathbb{R}$ est un polynôme, ou application polynomiale, à coefficients réels si il existe $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{R}^{n+1}$ tels que*

$$\forall x \in \mathbb{R}, \qquad P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k.$$

Les réels $a_0, \dots, a_n$ sont appelés les coefficients du polynôme P.

Pour tout $k \in \mathbb{N}$, on note X^k l'application polynomiale $x \in \mathbb{R} \longmapsto x^k$ (avec les conventions d'écriture $X^0 = 1$ et $X^1 = X$). Le polynôme

$$P : x \longmapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

s'écrit donc plus simplement

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

On note $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels.

Dans ce cours nous avons choisi d'appeler $X : x \mapsto x$ mais on aurait pu utiliser n'importe quelle lettre : si on utilise Y, on note $\mathbb{R}[Y]$ l'ensemble des polynômes, si on choisit x , on note $\mathbb{R}[x]$ l'ensemble des polynômes. C'est le choix du programme mais nous pensons que cela peut créer une confusion entre x la fonction et x l'un des choix naturel pour nommer un réel.

Ne faut pas confondre les nombres x et $P(x)$ et les applications X et P.

Remarques :

- Le polynôme P est parfois noté $P(X)$. Il faut comprendre cette notation comme la composée $P \circ X$, qui est bien l'application P puisque X est l'identité de $\mathbb{R}$. Ainsi P et $P(X)$ représentent bien la même application.
- On dit qu'on évalue un polynôme P en un point $x \in \mathbb{R}$ quand on donne la valeur de $P(x)$.
- On dit que $P \in \mathbb{R}[X]$ est un monôme si il existe $a \in \mathbb{R}$ et $n \in \mathbb{N}^*$ tels que $P = aX^n$.

Exemples :

b) Unicité des coefficients

L'écriture $P = \sum_{k=0}^{n} a_k X^k$ n'est pas unique : en effet on peut toujours rajouter un nombre fini p de termes nuls et écrire $P = \sum_{k=0}^{n+p} a_k X^k$ en posant $a_{n+1} = a_{n+2} = \cdots = a_{n+p} = 0$.
Par contre les coefficients de P sont uniquement déterminés :

Théorème (unicité des coefficients d'un polynôme). *Les coefficients d'un polynôme de $\mathbb{R}[X]$ sont définis de manière unique, c'est-à-dire si $P \in \mathbb{R}[X]$ est tel qu'il existe $(p,n) \in \mathbb{N}^2$ avec $p \leqslant n$, $(a_0,\dots,a_n) \in \mathbb{R}^{n+1}$ et $(b_0,\dots,b_p) \in \mathbb{R}^{p+1}$ tels que*

$$P = \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{p} b_k X^k,$$

alors $a_0 = b_0$, $a_1 = b_1$, …, $a_p = b_p$ et $a_{p+1} = a_{p+2} = \cdots = a_n = 0$.

En particulier, la fonction constante égale à 0 est l'unique polynôme dont tous les coefficients sont nuls. On l'appelle le polynôme nul et on le note encore 0.

Démonstration. Posons $b_{p+1} = b_{p+2} = \cdots = b_n = 0$. On a alors $\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} b_k X^k$ et donc, pour tout $x \in \mathbb{R}$, $\sum_{k=0}^{n} (a_k - b_k) x^k = 0$. Pour conclure il nous suffit de démontrer, pour tout $n \in \mathbb{N}$, la propriété

$$H_n : \text{« Si } (c_0,\dots,c_n) \in \mathbb{R}^{n+1} \text{ est tel que } \sum_{k=0}^{n} c_k X^k = 0 \text{ alors } c_0 = \cdots = c_n = 0 \text{ »}$$

□

c) Degré d'un polynôme

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

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

- *Si P n'est pas le polynôme nul, alors on appelle degré de P, et on note $\deg(P)$, le plus grand des indices des coefficients non nuls de P :*

$$\deg(P) = \max\{k \in [\![0\,;n]\!] \mid a_k \neq 0\}.$$

  Si $p = \deg(P)$, alors a_p (resp. $a_p X^p$) est appelé le coefficient (resp. le terme) dominant de P. Si $a_p = 1$, alors on dit que P est unitaire.
- *Si P est le polynôme nul, alors on adopte la convention $\deg(0) = -\infty$.*

Si $P \in \mathbb{R}[X]$ n'est pas le polynôme nul et si $p = \deg(P)$, alors P s'écrit de manière unique sous la forme $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$.

Exemples :

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

Définition. *Pour tout $n \in \mathbb{N}$, on note $\mathbb{R}_n[X]$ l'ensemble des polynômes P de $\mathbb{R}[X]$ tels que $\deg(P) \leqslant n$.*

La proposition découle de la définition du degré d'un polynôme et de l'unicité de ses coefficients.

Insistons bien : un polynôme de $\mathbb{R}_n[X]$ est de degré **au plus** n mais pas forcément de degré exactement n. En effet, si $P = \sum_{k=0}^{n} a_k X^k$, alors rien ne dit que $a_n \neq 0$. En général, pour montrer qu'un polynôme est de degré inférieur ou égal à n, on utilise les opérations sur le degré (cf. paragraphe suivant). Pour montrer qu'un polynôme est de degré exactement n, on doit généralement calculer le terme de plus haut degré et vérifier qu'il n'est pas nul.

Proposition. *On a $P \in \mathbb{R}_n[X]$ si et seulement si il existe un unique $(a_0, \dots, a_n) \in \mathbb{R}^{n+1}$ tel que $P = \sum_{k=0}^{n} a_k X^k$. De plus $\deg(P) = n$ si et seulement si $a_n \neq 0$.*

Remarques :

- $\mathbb{R}_0[X]$ est l'ensemble des polynômes de degré au plus 0, c'est-à-dire l'ensemble des polynômes constants. Par conséquent on identifie $\mathbb{R}_0[X]$ avec $\mathbb{R}$.
- Pour tout $k \in \mathbb{N}$, $\mathbb{R}_n[X] \subset \mathbb{R}_{n+1}[X] \subset \mathbb{R}[X]$. De plus $\bigcup_{n \in \mathbb{N}} \mathbb{R}_n[X] = \mathbb{R}[X]$.

2) Opérations sur les polynômes

Pour les règles de calcul sur le degré, on convient que, pour tout $a \in \mathbb{N} \cup \{-\infty\}$,

$$(-\infty) + (-\infty) = a + (-\infty) = (-\infty) + a = -\infty \qquad \text{et} \qquad \max(a, -\infty) = a.$$

Soient $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ dans $\mathbb{R}[X]$ de degrés respectifs $p \in \mathbb{N} \cup \{-\infty\}$ et $q \in \mathbb{N} \cup \{-\infty\}$.

a) Opérations algébriques

Proposition.

1. *Si $\lambda \in \mathbb{R}$, alors $\lambda P \in \mathbb{R}[X]$. Si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$ et le coefficient dominant de λP est λa_p.*
2. *$P + Q \in \mathbb{R}[X]$ et $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$. Plus précisément :*
   - *Si $p \neq q$, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$ et le coefficient dominant est a_p (resp. b_q) si $p > q$ (resp. $p < q$).*
   - *Si $p = q$ et $a_p \neq -b_p$, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$ et le coefficient dominant est $a_p + b_q$.*
   - *Si $p = q$ et $a_p = -b_q$, alors $\deg(P+Q) < \max(\deg(P), \deg(Q))$ et aucune formule générale ne donne le coefficient dominant de $P+Q$.*
3. *$PQ \in \mathbb{R}[X]$ et $\deg(PQ) = \deg(P) + \deg(Q)$ et le coefficient dominant de PQ est $a_p b_q$.*

Démonstration. Supposons que P et Q sont non nuls (sinon c'est immédiat).

1. On a $\lambda P = \sum_{k=0}^{p} (\lambda a_k) X^k \in \mathbb{R}[X]$. D'où le résultat dans le cas où $\lambda \neq 0$.
2. Supposons que $p \leqslant q$ (le cas où $p > q$ se traite de façon analogue).

Posons $a_{p+1} = \cdots = a_q = 0$. On a alors

$$P + Q = \sum_{k=0}^{q} (a_k + b_k) X^k \in \mathbb{R}[X].$$

- Si $p < q$, alors $a_q + b_q = b_q \neq 0$ et donc $\deg(P+Q) = q = \max(\deg(P), \deg(Q))$.
- Si $p = q$ et $a_q \neq -b_q$, alors $a_q + b_q \neq 0$ et donc

$$\deg(P + Q) = q = \max(\deg(P), \deg(Q)).$$

- Si $p = q$ et $a_q = -b_q$, alors $a_q + b_q = 0$ et donc

$$\deg(P + Q) < q = \max(\deg(P), \deg(Q)).$$

3. On a $PQ = \left(a_p X^p + \sum_{k=0}^{p-1} a_k X^k \right) \left(b_q X^q + \sum_{j=0}^{q-1} b_j X^j \right)$.

$$= a_p b_q X^{p+q} + \underbrace{\sum_{j=0}^{q-1} b_j X^{p+j}}_{\text{de degré} \leqslant p+q-1} + \underbrace{\sum_{k=0}^{p-1} a_k X^{k+q}}_{\text{de degré} \leqslant q+p-1} + \underbrace{\sum_{k=0}^{p-1} \sum_{j=0}^{q-1} a_k b_j X^{k+j}}_{\text{de degré} \leqslant p-1+q-1}$$

Ainsi PQ est la somme de $a_p b_q X^{p+q}$ et de trois polynômes de degré inférieur strictement à $p + q$. D'où le résultat. □

Exemples :

- *Si* $P = 3X^2 + 2X$ *et* $Q = 7X^3 - 1$, *alors*
- *Si* $P = 2X^5 - 4X^2 + 1$ *et* $Q = -2X^5 + 7X^4$, *alors*
- *Si* $P = 8X^3 + 5X^2 - 3X - 1$ *et* $Q = X$, *alors*
- *Si* $P = X + 7$ *et* $Q = -1 + 3X + X^2$, *alors*

Par récurrence, nous obtenons

Corollaire. *Soient* $P_1, \ldots, P_k$ *dans* $\mathbb{R}[X]$. *On a :*

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

Le coefficient dominant du produit est égal au produit des coefficients dominants.

Si $P \in \mathbb{R}[X]$ *et* $k \in \mathbb{N}$, *alors* $P^k \in \mathbb{R}[X]$, $\deg(P^k) = k \deg(P)$ *et le coefficient dominant de* P^k *est la puissance* $k^{\text{ième}}$ *de celui de* P.

Corollaire. *Soit* $n \in \mathbb{N}$. *Si* $(\lambda, \mu) \in \mathbb{R}^2$ *et* $(P, Q) \in (\mathbb{R}_n[X])^2$, *alors* $\lambda P + \mu Q \in \mathbb{R}_n[X]$.

Remarque : De nombreuses propriétés sur les polynômes héritent naturellement des propriétés de l'addition et de la multiplication sur $\mathbb{R}$. Notamment, si P, Q, R sont dans $\mathbb{R}[X]$, alors

- $P + Q = Q + P$ (commutativité de l'addition),
- $P + (Q + R) = (P + Q) + R$ (associativité de l'addition),
- $P + 0 = 0 + P = P$ (0 est l'élément neutre pour l'addition),
- $P - P = 0$ ($-P$ est l'opposé de P, ou symétrique de P pour l'addition).

Nous reverrons ces propriétés lors du chapitre *Introduction aux espaces vectoriels*. Il y en a d'autres encore (mais qui ne sont pas des propriétés d'espaces vectoriels) :

- $PQ = QP$ (commutativité du produit),
- $P(QR) = (PQ)R$ (associativité du produit),
- $P \times 1 = 1 \times P = P$ (1 est l'élément neutre pour le produit).

Qu'en est-il de l'inverse d'un polynôme ?

Proposition (polynôme inversibles). *Soient P et Q dans $\mathbb{R}[X]$. On a $PQ = 1$ si et seulement si P et Q sont des polynômes constants non nuls inverses l'un de l'autre.*

Démonstration.

□

Lorsque le produit de deux fonctions est nul, il est faux de conclure que l'une des deux est nulle. Par contre c'est le cas pour des polynômes.

Proposition (intégrité). *Soient P et Q dans $\mathbb{R}[X]$. On a $PQ = 0$ si et seulement si $P = 0$ ou $Q = 0$.*

Démonstration.

□

b) Composition d'un polynôme

Proposition. *Soient P et Q des polynômes non constants de $\mathbb{R}[X]$. On a $P \circ Q \in \mathbb{R}[X]$, $\deg(P \circ Q) = \deg(P)\deg(Q)$ et le coefficient dominant de $P \circ Q$ est $a_p(b_q)^p$.*

Démonstration. Reprenons les notations des propositions précédentes. Pour tout $k \in [\![0\,;p]\!]$, $Q^k \in \mathbb{R}[X]$ donc $a_k Q^k \in \mathbb{R}[X]$ est de degré au plus k. On a

$$P \circ Q = a_p Q^p + \sum_{k=0}^{p-1} a_k Q^k \in \mathbb{R}[X].$$

Le polynôme Q^p est de degré pq et de coefficient dominant b_q^p. Puisque $a_p \neq 0$, $a_p Q^p$ est de degré pq et de coefficient dominant $a_p b_q^p$. Pour tout $k \in [\![0\,;p-1]\!]$, $a_k Q^k$ est de degré au plus $kq < pq$. Par somme $P \circ Q$ est donc de degré $pq = \deg(P)\deg(Q)$ et de coefficient dominant $a_p(b_q)^p$. □

Exemple :

c) Dérivée d'un polynôme

L'appellation dérivée d'un polynôme n'est pas un hasard : on constate qu'il s'agit de la dérivée de la fonction P, au sens défini dans le chapitre 13. Néanmoins il s'agit d'une autre définition (dite formelle) de la dérivée dans le cas d'un polynôme uniquement et qui n'utilise pas de notion de limite. Notamment un polynôme est dérivable et il n'y a pas besoin de le dire avant de le dériver.

Définition. *Soit $P \in \mathbb{R}[X]$. On définit le polynôme dérivé P' de P par :*

- *Si P est constant, alors on pose $P' = 0$.*
- *Si $P = \sum_{k=0}^{n} a_k X^k$ avec $n \in \mathbb{N}$ et $a_n \neq 0$, alors*

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

Exemples :

Il est immédiat que :

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

Cette proposition est immédiate en utilisant des arguments d'analyse (le fait que la dérivée d'un polynôme est.... la dérive de la fonction polynomiale associée à ce polynôme). Mais on peut la montrer exclusivement en utilisant la définition formelle de la dérivée d'un polynôme (cf. TD).

Proposition. *Soient P et Q dans $\mathbb{R}[X]$. Soit $\lambda \in \mathbb{R}$. On a*

$$(P+Q)' = P'+Q', \quad (\lambda P)' = \lambda P', \quad (PQ)' = P'Q+QP', \quad (P\circ Q)' = Q' \times (P' \circ Q).$$

Définition (dérivées successives). *Soit $P \in \mathbb{R}[X]$ et $k \in \mathbb{N}$. On appelle polynôme dérivé d'ordre k du polynôme P le polynôme noté $P^{(k)}$ défini par récurrence de la manière suivante :*

$$P^{(0)} = P \qquad \text{et} \qquad \forall k \in \mathbb{N}^*, \quad P^{(k+1)} = (P^{(k)})'.$$

On a $P' = P^{(1)}$ et on note aussi $P'' = P^{(2)} = (P')'$.

Exemple :

Remarques :

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

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

- Si P est un polynôme de degré $p \in \mathbb{N}^*$ et de coefficient dominant λ, alors :
  - Si $j \in [\![0\,;p-1]\!]$, le coefficient dominant de $P^{(j)}$ est

$$p(p-1)(p-2)\cdots(p-j+1)\lambda = \frac{p!}{(p-j)!}\lambda.$$

  - $P^{(p)}$ est un polynôme constant égal à $p!\lambda$.
  - Si $j \geqslant p+1$, $P^{(j)}$ est le polynôme nul.

Proposition. *Si $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k$ alors, pour tout $k \in [\![0\,;n]\!]$, $a_k = \frac{P^{(k)}(0)}{k!}$.*

Démonstration.

□

Théorème (formule de Taylor pour les polynômes). *Si $P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$, alors*

Démonstration.

□

II Division euclidienne de polynômes

1) Le théorème de la division euclidienne

Rappelons le théorème de la division euclidienne dans $\mathbb{Z}$ (vu à l'école primaire... pas tout à fait sous cette forme certes) : si $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $r \in [\![0\,;|b|-1]\!]$. Voici l'analogue de ce théorème dans $\mathbb{R}[X]$.

On fait des divisions euclidiennes de polynômes comme des divisons euclidiennes d'entiers. Commençons par un exemple : effectuons la division euclidienne du polynôme $A = 5X^4 - 2X^3 + 16X^2 - X - 1$ par $B = X^2 + 3$. On la pose comme la division euclidienne dans $\mathbb{Z}$:

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

Démonstration. *Unicité.*

Existence. Notons $p = \deg(B) \geqslant 0$ et $B = \sum_{j=0}^{p} b_j X^j$ (on a donc $b_p \neq 0$). Nous allons montrer par récurrence que, pour tout $n \in \mathbb{N}$,

$$H_n : \text{« Pour tout } A \in \mathbb{R}_n[X], \text{ il existe } (B,Q) \in \mathbb{R}[X] \text{ tel que } A = BQ + R \text{ et } \deg(Q) < \deg(B) \text{ »}$$

est vraie.

- Soit $A \in \mathbb{R}_0[X]$, c'est-à-dire A est constant. Il suffit de poser

$$(Q,R) = \begin{cases} (0,A) & \text{si} \quad p = \deg(B) \geqslant 1, \\ (A/b_0, 0) & \text{si} \quad p = \deg(B) = 0. \end{cases}$$

  Ainsi H_0 est vraie.
- Soit $n \in \mathbb{N}$. Supposons que H_n soit vraie. Soit $A = \sum_{k=0}^{n+1} a_k X^k \in \mathbb{R}_{n+1}[X]$. Si $n+1 < p$, alors $A = B \cdot 0 + A$ donc on prend $(Q,R) = (0,A)$ et on a $A = BQ + R$ et $\deg(R) < \deg(B)$. Supposons que $n+1 \geqslant p$.
  - Si $a_{n+1} = 0$, alors $A \in \mathbb{R}_n[X]$ et alors on applique l'hypothèse de récurrence à A et c'est fini.
  - Supposons que $a_{n+1} \neq 0$, i.e A est de degré $n+1$. Considérons

$$\widetilde{A} = A - \frac{a_{n+1}}{b_p} X^{n+1-p} B.$$

    Le polynôme $\widetilde{A}$ est la somme de deux polynômes de degré $n+1$ dont les coefficients dominants sont opposés donc $\deg(\widetilde{A}) \leqslant n$. Par hypothèse de récurrence, il existe alors des polynômes $\widetilde{Q}$ et $\widetilde{R}$ tels que $\widetilde{A} = B\widetilde{Q} + \widetilde{R}$ et $\deg(\widetilde{R}) < \deg(B)$. On a alors

$$A = \underbrace{\left(\widetilde{Q} + \frac{a_{n+1}}{b_p} X^{n+1-p}\right)}_{=Q} B + \widetilde{R}.$$

    On pose alors $R = \widetilde{R}$ et on a bien $\deg(R) < \deg(B)$. Ainsi H_{n+1} est vraie.

Par récurrence, la propriété H_n est donc vraie pour tout $n \in \mathbb{N}$. Cela prouve l'existence. □

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

Proposition. *Soient $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$. Le reste de la division euclidienne de P par $X - a$ est $P(a)$.*

Démonstration.

□

Exemples :

Technique ultra classique lorsqu'on ne demande que le reste. S'il y a des racines multiples (cf. paragraphe III.2), on dérive et on évalue en la racine.

2) Divisibilité dans $\mathbb{R}[X]$

Définition (diviseur et multiple). *Soit $(A, B) \in \mathbb{R}[X]^2$. On dit que A est divisible par B (ou que B divise A, ou que B est un diviseur de A ou encore que A est un multiple de B) dans $\mathbb{R}[X]$ si le reste de la division euclidienne de A par B est le polynôme nul, c'est-à-dire si il existe $Q \in \mathbb{R}[X]$ tel que $A = BQ$. On note alors $B|A$.*

Remarque : Le théorème de la division euclidienne nous assure que, si $A = BQ$, alors Q est unique.

Exemples :

- $X - 1$ *divise* $X^3 - 1$ *car*
- $2X + 2$ *divise* $X + 1$ *car*
- $X^2 + 1$ *divise* $X^4 - 1$ *car*
- $X^3 + 2X + 3$ *divise* $X^5 + 3X^2 - 4X - 6$ *car* $X^5 - X^2 - 6 = (X^3 + 2X + 3)(X^2 - 2)$.

Remarquons l'analogie entre les notions de division euclidienne et de diviseurs entre $\mathbb{Z}$ et $\mathbb{R}[X]$. Il existe également un analogue des nombres premiers dans $\mathbb{R}[X]$ (mais c'est à la limite du programme), la notion de polynôme irréductible : un polynôme $P \in \mathbb{R}[X]$ est dit irréductible dans $\mathbb{R}[X]$ s'il est non constant et si les seuls polynômes qui le divisent sont les polynômes constants et les polynômes λP, avec $\lambda \in \mathbb{R}^*$.

Proposition. *Soient A, B et C des polynômes non nuls de $\mathbb{R}[X]$.*

1. *Si $B|A$, alors $\deg(B) \leqslant \deg(A)$, avec égalité si et seulement si il existe $\lambda \in \mathbb{R}^*$ tel que $A = \lambda B$.*
2. *(réflexivité) $A|A$.*
3. *(antisymétrie) Si $A|B$ et $B|A$, alors il existe $\lambda \in \mathbb{R}^*$ tel que $A = \lambda B$.*
4. *(transitivité) Si $C|B$ et $B|A$, alors $C|A$.*
5. *Si $B|A$, alors $BC|AC$.*

Démonstration.

1. Si $B|A$, alors il existe $Q \in \mathbb{R}[X]$ tel que $A = BQ$ et donc $\deg(A) = \deg(B) + \deg(Q) \geqslant \deg(B)$. Il y a égalité si et seulement si $\deg(Q) = 0$, c'est-à-dire Q est constant.
2. On a $A = 1 \times A$ donc $A|A$.
3. Si $A|B$ et $B|A$, alors il existe U et V dans $\mathbb{R}[X]$ tels que $A = BU$ et $B = AV$. On a donc $A = AVU$ donc $\deg(A) = \deg(A) + \deg(U) + \deg(V)$. Comme $\deg(A) \neq -\infty$, on a $\deg(U) + \deg(V) = 0$ donc $\deg(U) = \deg(V) = 0$. En particulier U est constant, disons égal à λ, et donc $A = \lambda B$.

4. Si $C|B$ et $B|A$, alors il existe U et V dans $\mathbb{R}[X]$ tels que $A = BU$ et $B = CV$. Ainsi $A = C(VU)$, c'est-à-dire $C|A$.
5. Si $B|A$, il existe Q tel que $A = BQ$ donc $AC = BCQ$ et donc $BC|AC$. □

III Racines d'un polynôme et factorisation

1) Définition et caractérisation

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

Exemples :

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

Théorème. *Soient $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$. Alors a est une racine de P si et seulement si $X - a$ divise P, c'est-à-dire si et seulement si il existe $Q \in \mathbb{R}[X]$ tel que $P = (X - a)Q$. Le polynôme Q est alors unique.*

Démonstration.

□

Proposition. *Soient $P \in \mathbb{R}[X]$, $n \geqslant 1$, $a_1, \dots, a_n$ deux à deux distincts dans $\mathbb{R}$. Si $a_1, \dots, a_n$ sont des racines de P, alors P est divisible par $\prod_{j=1}^{n}(X - a_j)$.*

Démonstration. Procédons par récurrence sur $n \geqslant 1$.

- Si a_1 est une racine de P, alors $X - a_1$ divise P. La proposition est donc vraie pour $n = 1$.
- Supposons la proposition vraie au rang $n \geqslant 1$. Soit $P \in \mathbb{R}[X]$ tel que $a_1, \dots, a_{n+1}$ sont des racines distinctes de P. Il existe Q tel que $P = (X - a_{n+1})Q$. Pour tout $j \in [\![1\,;n]\!]$, nous avons
$$Q(a_j) = \frac{P(a_j)}{a_j - a_{n+1}} = 0,$$
c'est-à-dire a_j est racine de Q. L'hypothèse de récurrence entraîne alors l'existence de $Q_1 \in \mathbb{R}[X]$ tel que $Q = (X - a_1)\dots(X - a_n)Q_1$. Par conséquent $P = (X - a_1)\dots(X - a_n)(X - a_{n+1})Q_1$. Ainsi la proposition est vraie au rang $n + 1$. □

C'est le théorème le plus important de ce chapitre !

Théorème. *Soit $n \in \mathbb{N}$. Si $P \in \mathbb{R}_n[X]$ admet au moins $n + 1$ racines deux à deux distinctes dans $\mathbb{R}$, alors $P = 0$. Autrement dit tout polynôme non nul de degré n admet au plus n racines deux à deux distinctes.*

Démonstration.

□

La fonction $\sin$ n'est pas un polynôme. En effet elle s'annule une infinité de fois (en tous les $k\pi$, $k \in \mathbb{Z}$) donc, si elle en était un, il s'agirait du polynôme nul. Ce n'est pas le cas puisque $\sin(\pi/2) = 1 \neq 0$. Même remarque pour la fonction $\cos$.

Corollaire. *Si un polynôme de $\mathbb{R}[X]$ possède une infinité de racines dans $\mathbb{R}[X]$, alors il s'agit du polynôme nul.*

Corollaire.

1. *Soit $n \in \mathbb{N}$. Soient P et Q dans $\mathbb{R}_n[X]$. On a $P = Q$ si et seulement si P et Q coïncident en au moins $n+1$ valeurs distinctes.*
2. *Soient P et Q dans $\mathbb{R}[X]$. On a $P = Q$ si et seulement si P et Q coïncident en une infinité de valeurs distinctes.*

Démonstration. C'est une conséquence du théorème précédent et de son corollaire puisque $P = Q$ si et seulement si $P - Q = 0$. □

Exemple : *On peut montrer par récurrence (cf. DM) que, pour tout $n \in \mathbb{N}^*$, il existe $T_n \in \mathbb{R}[X]$ tel que*

$$\forall \theta \in \mathbb{R}, \qquad \cos(n\theta) = T_n(\cos(\theta)).$$

Mais, à n fixé, T_n est-il unique ?

Corollaire. *Soit P est un polynôme de degré $n \geqslant 1$ et de coefficient dominant $a_n \neq 0$. Si P admet n racines deux à deux distinctes $\alpha_1, \ldots, \alpha_n$, alors $P = a_n \prod_{k=1}^{n} (X - \alpha_k)$.*

Démonstration.

□

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

2) Ordre de multiplicité d'une racine

Soient $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$.

- On dit que a est une racine simple de P si $X - a$ divise P mais $(X-a)^2$ ne divise pas P.
- On dit que a est une racine multiple de P si $(X-a)^2$ divise P.
- On dit que a est une racine double de P si $(X-a)^2$ divise P mais $(X-a)^3$ ne divise pas P.

Plus généralement :

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

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

Proposition. *Soient $P \in \mathbb{R}[X]$ un polynôme non nul et $k \in \mathbb{N}^*$. Le nombre $a \in \mathbb{R}$ est une racine d'ordre k de P si et seulement si il existe $Q \in \mathbb{R}[X]$ tel que $P = (X-a)^k Q$ et $Q(a) \neq 0$. Le polynôme Q est alors unique.*

Démonstration.

□

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

Proposition. *Soit $P \in \mathbb{R}[X]$ admettant $p \geqslant 1$ racines $a_1, \dots, a_p$ deux à deux distinctes de P d'ordres de multiplicité respectifs $k_1, \dots, k_p$. Alors*

$$\sum_{m=1}^{p} k_m \leqslant \deg(P) \qquad \text{et} \qquad \prod_{m=1}^{p} (X-a_m)^{k_m} \Big| P.$$

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

$$\sum_{m=1}^{p} k_m = \deg(P) \qquad \Longleftrightarrow \qquad P = \lambda \prod_{m=1}^{p} (X - a_m)^{k_m}.$$

Démonstration.

- Pour tout $p \in \mathbb{N}^*$, notons $H(p)$ la propriété « Si P est un polynôme qui admet $a_1, \dots, a_p$ pour racines deux à deux distinctes de multiplicité $k_1, \dots, k_p$, alors $\prod_{m=1}^{p} (X - a_m)^{k_m} \Big| P$ ». Montrons-la par récurrence.
  - Soit P un polynôme admettant une racine a_1 d'ordre de multiplicité k_1, alors on a $(X - a_1)^{k_1} | P$, par définition. Ainsi $H(1)$ est vraie.
  - Soit $p \geqslant 1$. Supposons $H(p)$ vraie. Soit P un polynôme admettant $a_1, \dots, a_{p+1}$ pour racines deux à deux distinctes d'ordre de multiplicités $k_1, \dots, k_{p+1}$. Il existe un polynôme Q tel que $Q(a_{p+1}) \neq 0$ et $P = (X - a_{p+1})^{k_{p+1}} Q$.

    Montrons que $a_1, \dots, a_p$ sont racines de Q d'ordres de multiplicité $k_1, \dots, k_p$. Soit $i \in [\![1\,;p]\!]$. On a $0 = P(a_i) = (a_i - a_{p+1})^{k_{p+1}} Q(a_i)$ et $a_i \neq a_{p+1}$ donc $Q(a_i) = 0$. Notons ℓ_i l'ordre de multiplicité de a_i dans Q. Il existe alors R_i tel que $R_i(a_i) \neq 0$ et $Q = (X - a_i)^{\ell_i} R_i$ et donc $P = (X - a_i)^{\ell_i} \underbrace{(X - a_{p+1})^{k_{p+1}} R_i}_{=Q_i}$. Puisque $Q_i(a_i) \neq 0$, on en déduit que ℓ_i est l'ordre de multiplicité de a_i dans P et donc $\ell_i = k_i$. On vient bien de montrer que $a_1, \dots, a_p$ sont racines de Q d'ordre de multiplicité $k_1, \dots, k_p$. Par hypothèse de récurrence, on a donc $\prod_{m=1}^{p} (X - a_i)^{k_i} \Big| Q$. On en déduit que $\prod_{m=1}^{p+1} (X - a_i)^{k_i} \Big| P$. Ainsi $H(p+1)$ est vraie.

  Par récurrence, pour tout $p \in \mathbb{N}^*$, $H(p)$ est vraie.
- Soit $p \in \mathbb{N}^*$. Si $P \in \mathbb{R}[X]$ admet pour racines $a_1, \dots, a_p$ d'ordres de multiplicité $k_1, \dots, k_p$, alors on vient de montrer que $\prod_{m=1}^{p} (X - a_m)^{k_m} \Big| P$. Ainsi

$$\deg(P) \geqslant \deg\left(\prod_{m=1}^{p} (X - a_m)^{k_m} \right) = \sum_{m=1}^{p} \deg\left((X - a_m)^{k_m} \right) = \sum_{m=1}^{p} k_m.$$

  De plu il y a égalité si et seulement si P et $\prod_{m=1}^{p} (X - a_m)^{k_m}$ sont égaux à une constante multiplicative près. Dans ce cas, cette constant est forcément λ puisque $\prod_{m=1}^{p} (X - a_m)^{k_m}$ est unitaire. □

Ce théorème n'est pas explicitement au programme mais c'est un outil formidable et simple (bien plus simple que de factoriser tant qu'on ne puisse plus) pour déterminer la multiplicité d'une racine. De plus c'est l'utilité principale de la formule de Taylor pour les polynômes.

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

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

Démonstration. Notons $n = \deg(P) \in \mathbb{N}^*$. La formule de Taylor pour les polynômes entraîne que

$$P = \sum_{j=0}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^j = \sum_{j=k}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^j + \sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j$$
$$= (X-a)^k \underbrace{\sum_{j=k}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^{j-k}}_{=Q} + \underbrace{\sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j}_{=R}$$

Ainsi a est une racine d'ordre k de P si et seulement si $R = 0$ et $Q(a) \neq 0$ (d'après le critère précédent).

On a $Q(a) = \dfrac{P^{(k)}(a)}{k!}$. Enfin $R = 0$ si et seulement si $R \circ (X+a) = 0$ si et seulement si, pour tout $j \in [\![0\,;k-1]\!]$, $\dfrac{P^{(j)}(a)}{j!} = 0$. D'où le théorème. □

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

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

On vient de voir que la recherche de racines, puis de leur ordre de multiplicité permet de factoriser les polynômes ? Mais que faire lorsqu'il n'y a pas de racines ? Ou lorsqu'on ne les trouve pas ? Jusqu'où s'arrêter dans la factorisation ?

On sait très bien le faire dans le cas des polynômes de degré 2. Rappelons le résultat vu dans le chapitre 2 :

Théorème. *Soit* $P = aX^2 + bX + c$ *avec* $(a,b,c) \in \mathbb{R}^* \times \mathbb{R}^2$. *Notons* $\Delta = b^2 - 4ac$ *son discriminant.*

- *Si* $\Delta = 0$, *alors* $P = a\big(X - \alpha\big)^2$ *avec* $\alpha = -\dfrac{b}{2a}$.

- *Si* $\Delta > 0$, *alors* $P = a(X - r_1)(X - r_2)$ *avec* $r_1 = \dfrac{-b + \sqrt{\Delta}}{2a}$ *et* $r_2 = \dfrac{-b - \sqrt{\Delta}}{2a}$.
- *Si* $\Delta < 0$, *alors* P *ne peut pas s'écrire comme le produit de deux polynômes de* $\mathbb{R}[X]$ *de degré* 1.

On a vu dans le chapitre 14 que tout polynôme de degré impair admet au moins une racine réelle.

Pour les polynômes de degré 3, il existe forcément une racine a. On peut donc l'écrire sous la forme $X - a$ fois un polynôme du second degré que l'on sait de nouveau factoriser ou non selon le signe de son discriminant. Problème : comment trouver une racine ? Et bien on peut toujours y arriver (il y a des formules mais elles sont hors-programme) mais en ECG, ou bien la racine est évidente (0, 1, -1, 2, -2) ou bien elle sera fournie.

Plus généralement on dispose d'un théorème qui nous dit quand s'arrêter, c'est-à-dire à partir de quand une factorisation est maximale.

Un polynôme n'admettant aucune racine n'admet donc que des polynômes de degré 2 dans sa factorisation (s'il y a un polynôme de degré 1, alors il admet une racine) et donc son degré est un multiple de 2. Ainsi, par contraposée, on retrouve le fait que tout polynôme réel de degré impair admet au moins une racine réelle.

Théorème (Factorisation dans $\mathbb{R}[X]$). *Tout polynôme non constant de* $\mathbb{R}[X]$ *s'écrit comme le produit de polynômes de degré* 1 *et de polynômes de degré* 2 *de discriminants strictement négatifs.*

Plus précisément, donnons-nous $P \in \mathbb{R}[X]$ *non constant. Notons* λ *le coefficient dominant de* P. *Il existe* $p \in \mathbb{N}^*$, $q \in \mathbb{N}^*$, $(a_1, \dots, a_p) \in \mathbb{R}^p$, $(k_1, \dots, k_p) \in (\mathbb{N}^*)^p$, $(\ell_1, \dots, \ell_q) \in (\mathbb{N}^*)^q$, $(u_1, \dots, u_q) \in \mathbb{R}^q$, $(v_1, \dots, v_q) \in \mathbb{R}^q$ *tels que, pour tout* $j \in [\![1\,;q]\!]$, $u_j^2 - 4v_j < 0$ *tels que*

$$P = \lambda \left(\prod_{j=1}^{p} (X - \alpha_j)^{k_j} \right) \left(\prod_{j=1}^{q} (X^2 + u_j X + v_j)^{\ell_j} \right).$$

De plus $\deg(P) = \sum_{j=1}^{p} k_j + 2 \sum_{j=1}^{q} \ell_j$.

Démonstration. Admis □

Ce théorème nous dit quand on doit s'arrêter mais pas comment faire. Dans la pratique factoriser un polynôme est un problème extrêmement difficile et on ne sait le faire que dans des cas particuliers. En ECG, cela sera toujours guidé. Nous disposons essentiellement de trois outils :

Les nombres complexes sont un précieux outil pour factoriser des polynômes mais ils sont hors-programme.

- La recherche de racines et de leurs ordres de multiplicité.
- L'utilisation d'un trinôme du second degré ou d'identité remarquables.
- La division euclidienne (lorsqu'on connaît une partie de la factorisation).

Exemples :