17 Polynômes

Depuis le lycée, vous êtes familiers des polynômes de degré 2, qui sont des fonctions de la forme $ax^2 + bx + c$, avec $a \neq 0$.
Et vous avez déjà rencontré des polynômes de degré 3, 4 voire plus, et avez probablement déjà une bonne intuition de ce dont il s'agit.
Ce chapitre a pour objectif de redéfinir toutes ces notions de façon plus formelle, et d'en étudier les propriétés.

Dans tout le chapitre, $\mathbf{K}$ est un corps quelconque.
Vous pouvez bien entendu imaginer que $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$, mais sauf mention explicite du contraire, ces résultats restent valables pour $\mathbf{K} = \mathbf{Q}$ ou encore $\mathbf{K} = \mathbf{Z}/7\mathbf{Z}$.

Rappel
Nous avons mentionné que pour p premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps.

17.1 L'algèbre $\mathbf{K}[X]$ des polynômes

Nous ne définirons pas véritablement ce qu'est une $\mathbf{K}$-algèbre A, mais disons qu'il s'agit d'un anneau muni en plus d'une structure d'espace vectoriel (que nous définirons bientôt).
Autrement dit, au delà des deux opérations qui existent dans un anneau, il en existe une troisième qui est la possibilité de multiplier les éléments de A par des éléments de $\mathbf{K}$ (les scalaires), avec certaines compatibilités entre toutes ces opérations.
Vous connaissez déjà un exemple de $\mathbf{K}$-algèbre, il s'agit de l'ensemble $\mathcal{M}_n(\mathbf{K})$.

17.1.1 Définition de $\mathbf{K}[X]$ et de ses opérations

Le principe de la définition qui suit est simple : nous avons déjà prouvé[1] que sur $\mathbf{R}$, une fonction polynomiale est entièrement déterminée par la suite de ses coefficients.
Définissons donc un polynôme comme une suite finie de nombres (ici des éléments de $\mathbf{K}$).

[1] Dans le chapitre 7.

Définition 17.1 – On note $\mathbf{K}[X]$ la partie de $\mathbf{K}^{\mathbf{N}}$ formée des suites nulles à partir d'un certain rang.
Les éléments de $\mathbf{K}[X]$ sont appelés **polynômes à coefficients dans $\mathbf{K}$**.
Pour $k \in \mathbf{N}$, on note X^k l'élément $(u_n)_{n\in\mathbf{N}}$ de $\mathbf{K}[X]$ défini par $u_n = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases} =$ $(0, 1, 0, 0, \dots)$.

Danger !
Le rang à partir duquel la suite est nulle dépend bien sûr de la suite choisie !

Donc intuitivement, dans le cas où $\mathbf{K} = \mathbf{R}$, on fait correspondre à $x \mapsto a_0 + a_1 x + \cdots + a_n x^n$ la suite $(a_0, a_1, \dots, a_n, 0, 0, \dots)$.

Définition 17.2 – Soit $P = (a_k)_{k\in\mathbf{N}}$ un élément de $\mathbf{K}[X]$.
Pour tout $k \in \mathbf{N}$, on dit que a_k est le **coefficient de degré k de P**.
Le polynôme dont tous les coefficients sont nuls est appelé polynôme nul, et on le note $0_{\mathbf{K}[X]}$, ou plus simplement 0.
Le **degré** d'un polynôme non nul $P = (a_k)_k$ est $\deg(P) = \max\{k \in \mathbf{N},\ a_k \neq 0\}$.
Par convention, le degré du polynôme nul est égal à $-\infty$.

Autrement dit
Un polynôme de degré n est un polynôme dont le coefficient de degré n est **non nul** et dont tous les coefficients de degré supérieur sont nuls.

Remarque. Notons que **par définition**, deux polynômes $P = (a_0, a_1, \dots)$ et $Q = (b_0, b_1, \dots)$ sont égaux si et seulement si tous leurs coefficients sont égaux : $\forall k \in \mathbf{N},\ a_k = b_k$.

Nous allons à présent définir plusieurs opérations sur $\mathbf{K}[X]$.

Définition 17.3 – Soient $P = (a_n)_{n\in\mathbf{N}}$ et $Q = (b_n)_{n\in\mathbf{N}}$ deux polynômes de $\mathbf{K}[X]$.
On définit :

- pour $\lambda \in \mathbf{K}$, le polynôme $\lambda \cdot P = (\lambda a_0, \lambda a_1, \dots, \lambda a_n, \dots)_n$
- la somme $P + Q$ de P et Q comme étant le polynôme

$$P + Q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, \dots)_n.$$

  Notons qu'il s'agit bien d'un polynôme, puisque pour $n > \max(\deg P, \deg Q)$, $a_n = b_n = 0$ et donc $a_n + b_n = 0$.
- le produit PQ de P et Q comme étant le polynôme $PQ = (c_n)_n$ où pour tout $n \in \mathbf{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Loi de composition
On n'a pas ici une loi de composition interne : elle n'associe pas un polynôme à deux polynômes, mais ce que nous nommerons plutôt une loi de composition externe : à un polynôme et un scalaire (= un élément de $\mathbf{K}$) elle associe un polynôme.

La définition de la somme n'appelle pas à davantage de commentaires, mais celle du produit mérite quelques explications.
Prenons deux fonctions polynomiales $f : x \mapsto a_0 + a_1 x + \cdots + a_p x^p$ et $g : x \mapsto b_0 + b_1 x + \cdots + b_q x^q$, et développons le produit $f(x)g(x)$:

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1 x + a_2 x^2 + \cdots + a_p x^p) \times (b_0 + b_1 x + \cdots + b_q x^q) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_p b_q x^{p+q}. \end{aligned}$$

En particulier, le terme constant[2] est donné par $a_0 b_0$, le terme en x est donné par $a_0 b_1 + a_1 b_0$, ..., le terme de degré n est $a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}$, ce qui coïncide bien avec notre définition.
Plus formellement : quitte à ajouter un certain nombre de coefficients nuls à l'un ou l'autre des polynômes, on peut supposer que $p = q$, de sorte que pour tout $x \in \mathbf{R}$, on a

[2] Sans x.

$$\begin{aligned} P(x)Q(x) &= \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{k=0}^{n} b_\ell x^\ell\right) = \sum_{k=0}^{n}\left(a_k x^k \sum_{\ell=0}^{n} b_\ell x^\ell\right) \quad \text{Distributivité.} \\ &= \sum_{k=0}^{n}\sum_{\ell=0}^{n} a_k b_\ell x^{\ell+k} = \sum_{k=0}^{n}\sum_{j=k}^{n+k} a_k b_{\ell-k} x^j \quad \text{Chgt d'indice } j = \ell + k. \\ &= \sum_{j=0}^{2n}\sum_{k=0}^{j} a_k b_{j-k} x^j = \sum_{j=0}^{2n}\left(\sum_{k=0}^{j} a_k b_{j-k}\right) x^j. \quad \text{Permutation de sommes.} \end{aligned}$$

Notons au passage que pour $n > p + q$, on a

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{p} a_k \underbrace{b_{n-k}}_{=0 \text{ car } n-k>p+q-p=q} + \sum_{k=p+1}^{n} \underbrace{a_k}_{=0 \text{ car } k>p} b_{n-k} = 0.$$

Remarque
Notons au passage que nous venons de prouver que
$\deg(PQ) \leqslant \deg(P) + \deg(Q)$.

Et donc PQ est bien un polynôme puisque tous ses coefficients sont nuls à partir d'un certain rang. Et donc le produit définit bien une loi de composition interne sur $\mathbf{K}[X]$.

Puisqu'on a noté $X^n = (\underbrace{0, \dots, 0}_{n \text{ fois}}, 1, 0, \dots)$, un polynôme $P = (a_0, a_1, a_2, \dots, a_n, 0, \dots)$ s'écrit encore

$$\begin{aligned} P &= a_0(1, 0, \dots) + a_1(0, 1, 0, \dots) + a_2(0, 0, 1, 0, \dots) + \cdots + a_n(0, \dots, 0, 1, 0, \dots) \\ &= a_0 \times X^0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k \end{aligned}$$

où $n = \deg P$.

Cette écriture est unique puisque si $P = \sum_{k=0}^{n} a_k X^k = \sum_{i=0}^{p} b_i X^i$, alors $P = (a_0, a_1, \dots, a_n, 0, \dots) = (b_0, b_1, \dots, b_p, 0, \dots)$, et donc par définition même de l'égalité de deux suites, $\forall i \in \mathbf{N}$,

$a_i = b_i$.

On s'autorisera aussi à noter $P = \sum_{k=0}^{+\infty} a_k X^k$, en gardant à l'esprit qu'il ne s'agit pas d'une vraie somme jusqu'à $+\infty$, et que seul un nombre fini de termes sont non nuls.

Pour $\lambda \in \mathbf{K}$, on notera parfois $\widetilde{\lambda}$ le polynôme dont le seul coefficient non nul est celui de degré 1, qui vaut λ : $\widetilde{\lambda} = (1, 0, 0, \dots)$, mais la plupart du temps, nous le noterons[3] tout simplement λ. En particulier, $\widetilde{0} = 0_{\mathbf{K}[X]}$.
Ces polynômes, à savoir ceux dont le degré est inférieur ou égal à 0, sont appelés polynômes **constants.**

[3] Abusivement.

Danger !
Je n'ai pas dit de degré 0, mais de degré **inférieur** ou égal à 0. Le polynôme nul est constant

Définition 17.4 – Si P est un polynôme non nul, alors son coefficient de degré $\deg(P)$ est appelé **coefficient dominant**.
Un polynôme est **unitaire** si son coefficient dominant vaut 1.
Enfin, un polynôme dont un seul coefficient est non nul est appelé un **monôme**.

Autrement dit
Le coefficient dominant est le dernier terme non nul de la suite des coefficients.

Exemple 17.5

Le coefficient dominant de $P = -2X^3 + X^2 - 1$ est -2.
Ce polynôme n'est pas unitaire, mais $\frac{P}{-2}$ l'est.
De manière générale, si P est non nul, alors en le divisant par son coefficient dominant, on obtient un polynôme unitaire proportionnel à P.

17.1.2 Propriétés des opérations

Proposition 17.6 : *Soit $P = \sum_{k=0}^{p} a_k X^k$, $Q = \sum_{k=0}^{q} b_k X^k$ et $R = \sum_{k=0}^{r} c_k X^k$ trois éléments de $\mathbf{K}[X]$. Alors :*

1. $P + Q = Q + P$. *(commutativité de l'addition)*
2. $(P + Q) + R = P + (Q + R)$. *(associativité de l'addition)*
3. $P + 0_{\mathbf{K}[X]} = 0_{\mathbf{K}[X]} + P = P$ *($0_{\mathbf{K}[X]}$ neutre pour $+$)*
4. *P possède un inverse pour l'addition, qu'on note $-P$ et qui est donné par*

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

Autrement dit, $(\mathbf{K}[X], +)$ est un groupe commutatif.

Remarque
Nous avons prouvé que $(\mathbf{K}^{\mathbf{N}}, +, \times)$ est un anneau, donc en particulier, $(\mathbf{K}^{\mathbf{N}}, +)$ est un groupe commutatif.

Démonstration. Plutôt que de prouver qu'il s'agit d'un groupe, prouvons qu'il s'agit d'un sous-groupe de $(\mathbf{K}^{\mathbf{N}}, +)$.
Il suffit pour cela de remarquer que la suite nulle (qui est le polynôme nul) est nulle à partir d'un certain rang, et que la différence de deux suites nulles à partir d'un certain rang est encore nulle à partir d'un certain rang.
Le point 4 nécessite toute de même une petite précision : si nous avons déjà prouvé que l'inverse d'une suite $P = (a_0, a_1, \dots)$ dans $\mathbf{K}^{\mathbf{N}}$ est la suite que nous avons donc notée $-P$, et qui est $(-a_0, -a_1, \dots)$, l'énoncé précise ici qu'il s'agit également du polynôme $(-1) \cdot P$.
Et donc $-P$ et $(-1) \cdot P$ désignent bien le même objet, ce qui est plutôt rassurant car cela va dans le sens de nos habitudes, mais n'avait rien d'une évidence au vu des définitions. □

Proposition 17.7 : *Soient* $P=\sum_{k=0}^{p} a_kX^k, Q=\sum_{k=0}^{q} b_kX^k$ *et* $R=\sum_{k=0}^{r} c_kX^k$ *trois éléments de* $\mathbf{K}[X]$*. Alors :*

1. $\forall (P,Q)\in\mathbf{K}[X]^2$, $PQ=QP$ *(commutativité du produit)*
2. $\forall (P,Q,R)\in\mathbf{K}[X]^3$, $(PQ)R=P(QR)$ *(associativité du produit)*
3. $\forall (P,Q,R)\in\mathbf{K}[X]^3$, $P(Q+R)=PQ+PR$ *(distributivité)*
4. $\forall P\in\mathbf{K}[X]$, $\widetilde{1}\times P=P$ *($\widetilde{1}$ est élément neutre pour la multiplication)*
5. $\forall \lambda\in\mathbf{K}$, $\forall (P,Q)\in\mathbf{K}[X]^2$, $\lambda\cdot(P+Q)=\lambda\cdot P+\lambda\cdot Q$
6. $\forall (\lambda,\mu)\in\mathbf{K}^2$, $\forall P\in\mathbf{K}[X]$, $(\lambda+\mu)\cdot P=\lambda\cdot P+\mu\cdot P$
7. $\forall (\lambda,\mu)\in\mathbf{K}^2$, $\forall P\in\mathbf{K}[X]$, $\lambda\cdot(\mu\cdot P)=(\lambda\mu)\cdot P$
8. $\forall \lambda\in\mathbf{K}$, $\forall (P,Q)\in\mathbf{K}[X]^2$, $(\lambda\cdot P)Q=\lambda\cdot(PQ)=P(\lambda\cdot Q)$

Un peu de jargon

Vous connaissez déjà les 4 premiers points : couplés au fait qu'on ait un groupe commutatif, ils signifient que $\mathbf{K}[X]$ possède une structure d'*anneau*.
Les 3 suivants (toujours couplés à la structure de groupe) signifient qu'on a ce que nous nommerons bientôt un *espace vectoriel*.
Tous ensemble, et couplés au dernier point (qui garantit une certaine compatibilité entre le produit de $\mathbf{K}[X]$ et celui de $\mathbf{K}$) ils donnent à $\mathbf{K}[X]$ une structure d'*algèbre* dont vous parlerez l'an prochain.

Démonstration. Notons que cette fois, nous n'allons pas pouvoir utiliser le fait que $(\mathbf{K}^{\mathbf{N}},+,\times)$ est un anneau, puisque le produit sur $\mathbf{K}[X]$ n'est pas le même que celui sur $\mathbf{K}^{\mathbf{N}}$ (qui était le produit terme à terme).

Dans toute la suite, notons $P=\sum_{k=0}^{p} a_kX^k, Q=\sum_{k=0}^{q} b_kX^k$ et $R=\sum_{k=0}^{r} c_kX^k$.

1. Pour tout $n\in\mathbf{N}$, le changement d'indice $i=n-k$ prouve que
$$\sum_{k=0}^{n} a_kb_{n-k}=\sum_{i=0}^{n} a_{n-i}b_i=\sum_{i=0}^{n} b_ia_{n-i}.$$
Donc le coefficient de degré n de PQ est égal à celui de QP. Ceci étant vrai pour tout $n\in\mathbf{N}$, ces deux polynômes sont égaux.
2. Le coefficient de degré n de $(PQ)R$ est $\sum_{k=0}^{n}\left(\sum_{i=0}^{k} a_ib_{k-i}\right)c_{n-k}$ et celui de $P(QR)$ est $\sum_{k=0}^{n} a_k\left(\sum_{j=0}^{n-k} b_jc_{n-k-j}\right)$. Or, on a
$$\begin{aligned}\sum_{k=0}^{n}\left(\sum_{i=0}^{k} a_ib_{k-i}\right)c_{n-k}&=\sum_{i=0}^{n}\sum_{k=i}^{n} a_ib_{k-i}c_{n-k}\\&=\sum_{i=0}^{n} a_i\sum_{k=i}^{n} b_{k-i}c_{n-k}\\&=\sum_{i=0}^{n} a_i\sum_{j=0}^{n-i} b_jc_{n-i-j}.\end{aligned}$$
Interversion de sommes.

Chgt d'indice

On a posé
$$j=k-i\Leftrightarrow i=j+k.$$

Et donc les coefficients de $(PQ)R$ sont égaux à ceux de $P(QR)$.
3. Le coefficient de degré n de $P(Q+R)$ est
$$\sum_{k=0}^{n} a_k(b_{n-k}+c_{n-k})=\sum_{k=0}^{n} a_kb_{n-k}+\sum_{k=0}^{n} a_kc_{n-k}.$$
On reconnaît là le coefficient de degré n de $PQ+PR$.
4. Le coefficient de degré n de $\widetilde{1}\times P$ est $1\times a_n+0\times a_{n-1}+\cdots+0\times a_0=a_n$.
5. Pour les points 5 à 8, notons que pour $\lambda\in\mathbf{K}$, la multiplication de P par le *polynôme* $\widetilde{\lambda}$ et la multiplication de P par le *scalaire* λ produisent le même effet : elles multiplient tous les coefficients de P par λ.
Or les propriétés déjà prouvées sur le produit permettent facilement, dans le cas particulier de polynômes constants, de retrouver les points 5 à 8.

Par exemple le point 5 découle directement de la distributivité : pour $\lambda \in \mathbf{K}$ et $P, Q \in \mathbf{K}[X]$, on a

$$\lambda \cdot (P+Q) = \widetilde{\lambda}(P+Q) = \widetilde{\lambda}P + \widetilde{\lambda}Q = \lambda \cdot P + \lambda \cdot Q.$$

Les points 6 et 7 nécessitent en plus de remarquer que $\widetilde{\lambda+\mu} = \widetilde{\lambda} + \widetilde{\mu}$ et $\widetilde{\lambda\mu} = \widetilde{\lambda}\widetilde{\mu}$.

□

Notons que toutes ces vérifications, bien que fastidieuses étaient indispensables. Les résultats ne doivent en rien vous surprendre, puisqu'on retrouve des règles de calcul qu'on manipule depuis toujours sans se poser de questions.

Dans la suite, nous ne distinguerons plus la multiplication par un scalaire de la multiplication par un polynôme constant, et nous noterons généralement λP plutôt que $\lambda \cdot P$ ou $\widetilde{\lambda}P$.

Enfin, il est temps de remarquer que la notation X^k que nous avons définie est bien cohérente avec les puissances multiplicatives de X.
Déjà, $X^0 = (1, 0, 0, \dots)$ est l'élément neutre de $\times$.

> **Remarque**
> Ces puissances ne sont bien définies, que parce que $\times$ est associative.

Lemme 17.8. Soit $P = (a_0, a_1, \dots, a_n, 0, \dots)$ un polynôme de $\mathbf{K}[X]$ de degré inférieur ou égal à n. Alors $P \times X = (0, a_0, a_1, a_2, \dots, a_n, 0, \dots)$.

Démonstration. Notons $(b_k)_{k\in\mathbf{N}}$ les coefficients de X et $(c_k)_{k\in\mathbf{N}}$ ceux de PX. On a alors, pour tout $k \in \mathbf{N}^*$,

$$c_k = \sum_{i=0}^{k} a_i \underbrace{b_{k-i}}_{=0 \text{ si } i\neq k-1} = a_{k-1} \times 1 = a_{k-1}.$$

Et $c_0 = a_0 \underbrace{b_0}_{=0} = 0$. □

Donc en particulier, pour tout $k \in \mathbf{N}^*$, $\underbrace{X \times X \times \cdots \times X}_{k \text{ fois}} = (\underbrace{0, \dots, 0}_{k \text{ fois}}, 1, 0, \dots)$.
Et donc la notation X^k est bien cohérente avec les puissances.
On a donc tout de suite : $\forall (k, \ell) \in \mathbf{N}^2$, $X^k X^\ell = X^{k+\ell}$, comme pour toute loi associative possédant un élément neutre.

⚠ On ne notera pas de puissances négatives de X, X n'a aucune raison d'être inversible dans $\mathbf{K}[X]$, et de fait nous prouverons plus loin qu'il ne l'est pas. Donc vous ne pourrez pas noter ni X^{-1} ni $\frac{1}{X}$, ils ne sont pas définis dans $\mathbf{K}[X]$.

17.1.3 Degré, ensemble $\mathbf{K}_n[X]$

Définition 17.9 – Soit $n \in \mathbf{N}$. On note $\mathbf{K}_n[X] = \{P \in \mathbf{K}[X] : \deg(P) \leqslant n\}$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$ de degré **inférieur ou égal à n.**

> **⚠ Attention !**
> Ne pas dire que $\mathbf{K}_n[X]$ est l'ensemble des polynômes de degré n, mais bien de degré inférieur à n.

Notons en particulier que $\mathbf{K}_0[X]$ est l'ensemble des polynômes constants (polynôme nul inclus) et que si $p \leqslant q$, alors $\mathbf{K}_p[X] \subset \mathbf{K}_q[X]$.

Proposition 17.10 : *Soient $P, Q \in \mathbf{K}[X]$. Alors :*

1. *pour tout $\lambda \neq 0$,* $\deg(\lambda P) = \deg(P)$
2. $\deg(PQ) = \deg(P) + \deg(Q)$
3. $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.
   Si de plus $\deg(P) \neq \deg(Q)$, *alors l'inégalité est une égalité :* $\deg(P+Q) = \max(\deg P, \deg Q)$.

Démonstration. Notons $P = \sum_{k=0}^{p} a_k X^k$, avec $a_p \neq 0$ et $Q = \sum_{k=0}^{q} b_k X^k$, avec $b_q \neq 0$. On a donc $\deg P = p$ et $\deg Q = q$.

1. Le coefficient de degré n de λP est λa_n, qui est donc nul si et seulement si $a_n = 0$. Donc $\lambda a_p \neq 0$ et pour $n > p$, $\lambda a_p = 0$, de sorte que $\deg(\lambda P) = p = \deg P$.
2. Nous avons déjà prouvé que si P et Q sont non nuls, alors $\deg(PQ) \leqslant \deg(P) + \deg(Q)$. De plus, le coefficient de degré $p+q$ de PQ est $a_p b_q \neq 0$, et donc $\deg(PQ) = \deg(P) + \deg(Q)$. Si l'un des deux polynômes P et Q est nul, alors $PQ = 0$ est de degré $-\infty = \deg(P) \times \deg(Q)$.
3. Le coefficient de degré n de $P + Q$ est $a_n + b_n$. Si $n > \max(p, q)$, il est donc nul, prouvant que $\deg(P + Q) \leqslant \max(p, q) = \max(\deg P, \deg Q)$.

   ⚠ On n'a pas prouvé que $\deg(P + Q) = \max(\deg P, \deg Q)$, car il se peut encore que le coefficient de degré $\max(\deg P, \deg Q)$ soit nul, auquel cas $\deg(P + Q) < \max(\deg P, \deg Q)$. C'est par exemple le cas si $P = -X^2 + 1$ et $Q = X^2 + X$. On a alors $P + Q = X + 1$, qui est de degré 1.
   En revanche si $\deg P \neq \deg Q$, les termes de plus haut degré ne peuvent plus s'annuler.
   Supposons par exemple que $p < q$. Alors le coefficient de degré $\max(p, q) = q$ de $P + Q$ est $a_p + b_q = b_q \neq 0$, et donc $P + Q$ est bien de degré $\max(\deg P, \deg Q)$.

□

Rappel

Pour tout réel p,

$$-\infty + p = -\infty$$

et

$$-\infty + (-\infty) = -\infty.$$

Corollaire 17.11 – *Pour $n \in \mathbf{N}$, $\mathbf{K}_n[X]$ est un sous-groupe de $\mathbf{K}[X]$, stable par la multiplication par un scalaire. Autrement dit, $\forall (P, Q) \in \mathbf{K}_n[X]^2$ et $\forall \lambda \in \mathbf{K}$, λP et $P - Q$ sont dans $\mathbf{K}_n[X]$.*

En revanche

Notons que le produit de deux éléments de $\mathbf{K}_n[X]$ n'est pas toujours dans $\mathbf{K}_n[X]$ (qui n'est donc pas un sous-anneau de $\mathbf{K}[X]$), mais toujours dans $\mathbf{K}_{2n}[X]$.

Proposition 17.12 : *L'anneau $\mathbf{K}[X]$ est intègre. Autrement dit,*

$$\forall (P, Q) \in \mathbf{K}[X]^2,\ PQ = 0_{\mathbf{K}[X]} \Rightarrow (P = 0_{\mathbf{K}[X]} \textbf{ ou } Q = 0_{\mathbf{K}[X]}).$$

Démonstration. Si $P \neq 0$ et $Q \neq 0$, alors $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$, donc PQ n'est pas nul. □

Plus généralement

Dans un anneau intègre, tout élément non nul est régulier pour la multiplication.
Ce qui ne veut pas dire qu'il soit inversible pour autant.

Corollaire 17.13 – $\forall (P, Q, R) \in \mathbf{K}[X]^3$, $(PQ = PR \textbf{ et } P \neq 0_{\mathbf{K}[X]}) \Rightarrow Q = R$.

Démonstration. $PQ = PR \Leftrightarrow P(Q - R) = 0_{\mathbf{K}[X]}$.
Et puisque $P \neq 0$, nécessairement $Q - R = 0_{\mathbf{K}[X]} \Leftrightarrow Q = R$. □

17.1.4 Composition de polynômes

Définition 17.14 – Soient $P, Q \in \mathbf{K}[X]$ deux polynômes, avec $P = \sum_{k=0}^{n} a_k X^k$.

On définit alors un polynôme noté $P \circ Q$ par

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

Proposition 17.15 : *Soient $P, Q \in \mathbf{K}[X]$, avec Q non constant. Alors*

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

Démonstration. Notons $P = \sum_{k=0}^{n} a_k X^k$, avec $n = \deg(P)$.
Alors pour tout $k \in \mathbf{N}$, Q^k est de degré $k \times \deg(Q)$.

Donc $\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right) \leqslant (n-1)\deg Q$.

Et puisque $\deg(a_n Q^n) = n\deg Q$ est différent de $\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right)$, alors le degré de la somme est $n\deg Q$. □

Exemples 17.16

Les coefficients d'un polynôme composé $P \circ Q$ ne sont pas faciles à obtenir directement à partir de ceux de P et Q, même si le binôme de Newton peut partiellement nous aider.

Par exemple, si $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$, avec $p = \deg P$ et $q = \deg Q$, alors le terme de degré pq provient uniquement de

$$a_p Q^p = a_p\left(b_q X^q + \sum_{k=0}^{q-1} b_k X^k\right)^p = a_p b_q^p X^{pq} + \underbrace{\star}_{\in \mathbf{K}_{pq-1}[X]}.$$

Donc le coefficient dominant de $P \circ Q$ est $a_p b_q^p$.

⚠ Les composées de polynômes sont[4] rarement notées avec $\circ$, et on note par exemple $P(X+1)$ pour désigner le polynôme P composé avec $X+1$.
Le risque de confusion avec le produit $P \times (X+1)$ est alors important...
Partons du principe que si on avait souhaité parler de ce produit, on l'aurait plutôt noté $(X+1)P$ ou alors carrément $P \times (X+1)$ ou $P \cdot (X+1)$.

[4] Par habitude plus que par convention.

17.1.5 Dérivation des polynômes

Nous définissons ici la notion de polynôme dérivé, pour l'instant sans rapport avec la dérivation des fonctions.

Définition 17.17 – Soit $P = \sum_{k=0}^{p} a_k X^k \in \mathbf{K}_p[X]$. On définit alors le **polynôme dérivé** de P, noté P' par

$$P' = \sum_{k=1}^{p} k a_k X^{k-1} \in \mathbf{K}_{p-1}[X]$$

Plus généralement, on note $P^{(0)} = P$ et pour tout $n \in \mathbf{N}$, $P^{(n+1)} = \left(P^{(n)}\right)'$.

Cette dérivation correspond bien à ce que vous connaissez des dérivées des fonctions polynômiales dans $\mathbf{R}$.
En revanche, soyons conscients qu'il s'agit là d'une définition : à aucun moment on ne parle de limite[5] de taux d'accroissement.
La bonne nouvelle, c'est que P' est toujours défini, il n'y aura jamais besoin de se poser la question de la dérivabilité de P : à tout polynôme P est associé un autre polynôme P'. Et tous les polynômes dérivés d'ordre supérieur : P'', $P^{(3)}$, etc sont eux aussi toujours définis.

[5] Ce qui n'aurait de sens que dans $\mathbf{R}$.

Proposition 17.18 : *Soient* $P = \sum_{k=0}^{p} a_k X^k$ *et* $Q = \sum_{k=0}^{q} b_k X^k$ *deux polynômes, et soit* $\lambda \in \mathbf{K}$. *Alors*

1. *Si* $\deg(P) \geqslant 1$, *alors* $\deg(P') = \deg(P) - 1$.
   En revanche, si P *est constant, alors* $P' = 0$, *de degré* $-\infty$.
2. $(\lambda P + Q)' = \lambda \cdot P' + Q'$ *(linéarité de la dérivation)*
3. $(PQ)' = P'Q + PQ'$
4. $(P \circ Q)' = Q' \times (P' \circ Q)$

Démonstration.

1. Si P est constant, alors la somme définissant P' est vide, donc P' est nul.
   En revanche, si $P = \sum_{k=0}^{p} a_k X^k$ est de degré p, donc avec $a_p \neq 0$, alors $P' = \sum_{k=1}^{p} a_k X^{k-1}$ est de degré au plus $p-1$, et son coefficient de degré $p-1$ est $pa_p \neq 0$. Donc $\deg(P') = p - 1$.
2. Trivial.
3. Commençons par le vérifier pour des monômes.
   Soient donc $k, \ell \in \mathbf{N}$. Si k et ℓ sont tous deux non nuls, alors
   $$\left(X^k X^\ell\right)' = \left(X^{k+\ell}\right)' = (k+\ell)X^{k+\ell-1} = kX^{k-1}X^\ell + \ell X^k X^{\ell-1} = \left(X^k\right)' X^\ell + X^k \left(X^\ell\right)'.$$
   Il est aisé de se convaincre que ceci reste vrai si $k = 0$ ou $\ell = 0$ (l'une des dérivées est alors nulle).
   Dès lors, la linéarité de la dérivée prouvée ci-dessus nous permet d'en déduire la formule dans le cas général :
   $$\begin{aligned}
   (PQ)' &= \left(\sum_{k=0}^{p} a_k X^k Q\right)' = \left(\sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell X^k X^\ell\right)' \\
   &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell \left(X^k X^\ell\right)' \\
   &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell \left(\left(X^k\right)' X^\ell + X^k \left(X^\ell\right)'\right) \\
   &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell \left(X^k\right)' X^\ell + \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell X^k \left(X^\ell\right)' \\
   &= \sum_{k=0}^{p}\left[a_k \left(X^k\right)'\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right)\right] + \sum_{k=0}^{p}\left[a_k X^k \left(\sum_{\ell=0}^{q} b_\ell \left(X^\ell\right)'\right)\right] \\
   &= \left(\sum_{k=0}^{p} a_k \left(X^k\right)'\right)\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right) + \left(\sum_{k=0}^{p} a_k X^k\right)\left(\sum_{\ell=0}^{q} b_\ell \left(X^\ell\right)'\right) \\
   &= \left(\sum_{k=0}^{p} a_k X^k\right)'\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right) + \left(\sum_{k=0}^{p} a_k X^k\right)\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right)' = P'Q + PQ'.
   \end{aligned}$$
   C'est encore la linéarité de la dérivation.
4. Une récurrence facile à l'aide de la formule ci-dessus prouve que pour tout $k \in \mathbf{N}$, le polynôme dérivé de Q^k est $kQ'Q^{k-1}$.
   Et alors
   $$(P \circ Q)' = \left(\sum_{k=0}^{p} a_k Q^k\right)' = \sum_{k=1}^{p} a_k k Q' Q^{k-1} = Q' \times \sum_{k=1}^{p} k a_k Q^{k-1} = Q' \times (P' \circ Q).$$

□

Corollaire 17.19 (Propriétés de la dérivée $n^{\text{ème}}$) – *Soient $P, Q \in \mathbf{K}[X]$, soit $\lambda \in \mathbf{K}$ et soit $n \in \mathbf{N}$.*

1. $\deg P^{(n)} = \begin{cases} \deg(P) - n & si\ \deg(P) \geqslant n \\ -\infty & sinon \end{cases}$
2. $(\lambda P + Q)^{(n)} = \lambda P^{(n)} + Q^{(n)}$

La dérivée $n^{\text{ème}}$ d'un produit est un peu plus complexe, mais il existe tout de même une formule.

Proposition 17.20 (Formule de Leibniz) : *Soient $P, Q \in \mathbf{K}[X]$ et soit $n \in \mathbf{N}$. Alors*

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

Danger !
Il s'agit bien de dérivées $k^{\text{èmes}}$ et $(n-k)^{\text{èmes}}$, et pas de puissances.

Démonstration. Prouvons le résultat par récurrence sur n.

Pour $n = 0$, il n'y a rien à dire : $PQ = \sum_{k=0}^{0} \binom{0}{k} P^{(k)} Q^{(n-k)}$.

Supposons la formule vraie au rang n. Alors

$$\begin{aligned}
(PQ)^{(n+1)} &= \left((PQ)^{(n)}\right)' \\
&= \left(\sum_{k=0}^{n} \binom{k}{n} P^{(k)} Q^{(n-k)}\right)' && \text{Hypothèse de récurrence.} \\
&= \sum_{k=0}^{n} \binom{k}{n} \left(P^{(k)} Q^{(n-k)}\right)' && \text{Linéarité de la dérivation.} \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n-k+1)}\right) && \text{Dérivée d'un produit.} \\
&= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k+1)} \\
&= \sum_{i=1}^{n+1} \binom{n}{i-1} P^{(i)} Q^{(n+1-i)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\
&= PQ^{(n+1)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) P^{(k)} Q^{(n+1-k)} + P^{(n+1)} Q \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)}.
\end{aligned}$$

Donc par le principe de récurrence, la formule est valable pour tout $n \in \mathbf{N}$. □

17.1.6 Évaluation en un point, fonctions polynomiales

Définition 17.21 – Si $P = \sum_{k=0}^{n} a_k X^k$, alors pour $\lambda \in \mathbf{K}$, on note $P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k \in \mathbf{K}$.

Proposition 17.22 : *Pour $P, Q \in \mathbf{K}[X]$, et $\lambda \in \mathbf{K}$, on a*

$$(P+Q)(\lambda) = P(\lambda) + Q(\lambda) \text{ et } (PQ)(\lambda) = P(\lambda)Q(\lambda).$$

Définition 17.23 – Soit $P \in \mathbf{K}[X]$. On appelle **fonction polynomiale associée à** P la fonction $\widetilde{P} : \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ \lambda & \longmapsto & P(\lambda) \end{array} \right.$.

Proposition 17.24 : *Soient $P, Q \in \mathbf{K}[X]$. Alors :*

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q},\ \widetilde{PQ} = \widetilde{P}\widetilde{Q},\ \widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$$

et dans le cas où $\mathbf{K} = \mathbf{R}$, alors $\widetilde{P'} = \left(\widetilde{P}\right)'$.

K = R ?

La restriction sur **K** vient tout simplement du fait que la notion de fonction dérivable, qui nécessite une notion de limite, n'a été définie que pour les fonctions définies sur **R** (même si on pourrait sans grandes difficultés le faire également pour les fonctions d'une variable complexe).

17.2 Divisibilité dans K[X]

17.2.1 Divisibilité

Définition 17.25 – Soient $P, Q \in \mathbf{K}[X]$. On dit que P **divise** Q, ou que Q est un multiple de P, et on note $P \mid Q$ s'il existe $\mathbf{R} \in \mathbf{K}[X]$ tel que $Q = PR$.

Exemple 17.26

Le polynôme $X^2 + 3X - 4$ est divisible par $X + 4$ puisque $X^2 + 3X - 4 = (X + 4)(X - 1)$.

Remarque. Un fait souvent utile est que si $P \mid Q$, avec $Q = PR$, alors $\deg P + \deg R = \deg Q$, et en particulier, $\deg P \leqslant \deg Q$.

Proposition 17.27 : *Comme sur **Z**, la relation de divisibilité est réflexive et transitive. Elle n'est pas antisymétrique, mais, pour $P, Q \in \mathbf{K}[X]$, on a*

$$(P \mid Q \text{ et } Q \mid P) \Leftrightarrow (P = Q = 0_{\mathbf{K}[X]} \text{ ou } \exists \lambda \in \mathbf{K}^*,\ P = \lambda Q).$$

De plus, si $P \mid A$ et $P \mid B$, alors $\forall (U, V) \in \mathbf{K}[X]^2$, $P \mid AU + BV$ et si $P \mid Q$, alors $\forall R \in \mathbf{K}[X]$, $PR \mid QR$.

Démonstration. Pour $P \in \mathbf{K}[X]$, on a $P = 1P$, donc P est réflexive.
Et si $P \mid Q$ et $Q \mid R$, alors il existe $A, B \in \mathbf{K}[X]$ tels que $Q = AP$ et $R = BQ$, donc $R = B(AP) = (AB)P$, de sorte que $P \mid R$.
Supposons que $P \mid Q$ et $Q \mid P$. Alors il existe $R_1, R_2 \in \mathbf{K}[X]$ tel que $Q = PR_1$ et $P = QR_2$.
Donc en particulier, $\deg P \leqslant \deg Q$ et $\deg Q \leqslant \deg P$, donc $\deg P = \deg Q$ et donc $\deg R_1 = \deg R_2 = 0$.
Donc R_1 est une constante $\lambda \neq 0$.
Inversement, si $P = \lambda Q$ avec $\lambda \in \mathbf{K}^*$, alors $Q = \dfrac{1}{\lambda} P$, et on a donc à la fois $P \mid Q$ et $Q \mid P$.

Les deux derniers points se prouvent exactement comme dans **Z**. □

Notons également que multiplier un polynôme par un scalaire non nul ne change rien à l'ensemble de ses diviseurs.
Autrement, quel que soit $\lambda \in \mathbf{K}^*$, $P \mid Q \Leftrightarrow P \mid \lambda Q$.
En effet, s'il existe $R \in \mathbf{K}[X]$ tel que $Q = PR$, alors $\lambda Q = P\lambda R$.
Et inversement, si $\lambda Q = PR$, alors $Q = \left(\frac{1}{R}\right) P$, donc $P \mid Q$.

17.2.2 Division euclidienne

Justifions à présent un résultat évoqué dans un chapitre antérieur : l'existence d'une division euclidienne dans l'anneau des polynômes.

Théorème 17.28 (Division euclidienne dans K[X]) : *Soient $A, B \in \mathbf{K}[X]$, avec $B \neq 0$. Alors il existe un unique couple $(Q,R) \in \mathbf{K}[X]^2$, avec $\deg R < \deg B$ tel que $A = BQ + R$.*
Notons que ceci s'écrit encore $(Q,R) \in \mathbf{K}[X] \times \mathbf{K}_{(\deg B)-1}[X]$.

Démonstration. L'unicité est la plus facile : supposons que $A = BQ_1 + R_1 = BQ_2 + R_2$, avec $\deg R_1 < \deg B$ et $\deg R_2 < \deg B$.
Alors $R_1 - R_2 = B(Q_2 - Q_1)$. Si $Q_1 \neq Q_2$, alors $B(Q_2 - Q_1) \neq 0$, et donc $\deg B(Q_2 - Q_1) \geqslant \deg B$.
Or, $\deg(R_1 - R_2) < \deg B$, ce qui est absurde.
Donc $Q_1 = Q_2$, et par conséquent, $R_1 = R_2$.

Pour l'existence, le cas le plus facile est celui où B divise A : il existe $Q \in \mathbf{K}[X]$ tel que $A = BQ = BQ + 0$.
On suppose donc désormais que $B \nmid A$.
Soit alors $\mathscr{P} = \{\deg(A - BQ),\ Q \in \mathbf{K}[X]\}$.
Puisque tous les $A - BQ$ sont non nuls, $\mathscr{P}$ est une partie de $\mathbf{N}$, non vide puisqu'elle contient $\deg(A) = \deg(A - B \times 0)$.
Elle possède donc un plus petit élément p.
Soit alors $Q \in \mathbf{K}[X]$ tel que $\deg(A - BQ) = p$, et montrons que p est strictement inférieur à $\deg B$.
Supposons au contraire que $R = A - BQ$ soit de degré supérieur$p$ ou égal à $\deg B$, et notons alors $n = \deg B$, $B = \sum_{i=0}^{n} b_i X^i$ et $R = \sum_{i=0}^{p} r_i X^i$.
Alors $R - \dfrac{r_p}{b_n} X^{p-n} B$ est encore de la forme $A - BQ$, et

$$R - \frac{r_p}{b_n} X^{p-n} B = \sum_{i=0}^{p} r_i X^i - \frac{r_p}{b_n} X^{n-p} \sum_{i=0}^{n} b_i X^i = \underbrace{\sum_{i=0}^{p} r_i X^i - r_p X^p}_{\in \mathbf{K}_{p-1}[X]} - \underbrace{\sum_{i=0}^{n-1} \frac{r_p}{b_n} b_i X^{p-n+i}}_{\in \mathbf{K}_{p-1}[X]} \in \mathbf{K}_{p-1}[X].$$

Donc $\deg\left(R - \dfrac{r_p}{b_n} X^{n-p} B\right)$ est un élément de $\mathscr{P}$ strictement inférieur à p, contredisant la définition de p.
On en déduit bien que $A = BQ + R$, avec $\deg R < \deg B$. □

La pratique de la division euclidienne n'a pas changé par rapport à ce que nous avions dit plus tôt dans l'année.
On retrouve bien entendu, comme pour les entiers[6] le fait que B divise A si et seulement si le reste de la division de A par B est nul.

Remarque
Notons que les hypothèses faites sur les degrés impliquent que $a_n \neq 0$ et $b_p \neq 0$.

Explication
Ce polynôme ne sort pas de nulle part : on souhaite retirer à R un multiple de B de manière à faire baisser le degré de r, c'est-à-dire à annuler son terme de plus haut degré ($r_p X^p$).

[6] Et nous verrons dans un chapitre ultérieur que l'analogie ne s'arrête pas là, et qu'à partir du moment où on a une division euclidienne, on peut reconstruire une notion de PGCD, retrouver Bézout, etc. Bref, faire de l'arithmétique.

17.3 Racines d'un polynôme

17.3.1 Racines et multiplicités

Définition 17.29 – Soit $P \in \mathbf{K}[X]$ et soit $a \in \mathbf{K}$. On dit que a est **racine** de P si $P(a) = 0$.

Remarques. ▶ Il est bon de préciser dans quel corps on se place lorsqu'on parle de racines. Par exemple, le polynôme $X^2 + 1$ n'a pas de racines dans $\mathbf{R}$, mais en a deux dans $\mathbf{C}$.
De même, $X^3 - 2 \in \mathbf{Q}[X]$ n'a aucune racine dans $\mathbf{Q}$, en a une dans $\mathbf{R}$ et trois dans $\mathbf{C}$.
▶ Si $P \mid Q$, alors toute racine de P est une racine de Q. En effet, si $Q = PR$ et $P(a) = 0$, alors $Q(a) = P(a)R(a) = 0$.

Exemple 17.30 **Application des racines au calcul d'une division euclidienne**

Calculons le reste de la division euclidienne (dans $\mathbf{R}[X]$) de X^n par $X^2+X-2=(X-1)(X+2)$.
Cette division est de la forme $X^n=(X-1)(X+2)Q_n+R_n \qquad (\star)$, avec $\deg R_n<2$.
Autrement dit, il existe deux réels a_n et b_n tels que $R_n=a_nX+b_n$.
Évaluons alors $(\star)$ en 1 :

$$1^n=(1-1)(1+2)Q_n(1)+R_n(1)=a_n+b_n.$$

Et de même, par évaluation en -2, $(-2)^n=-2a_n+b_n$.
On en déduit, par résolution d'un système, que $R_n=\frac{1}{3}\left((1-(-2)^n)X+2+(-2)^n\right)$.

Proposition 17.31 : *Soit $P\in\mathbf{K}[X]$ et soit $a\in\mathbf{K}$. Alors a est racine de P si et seulement si $X-a$ divise P.*

Démonstration. Si $X-a$ divise P, soit alors Q tel que $P(X)=Q(X)(X-a)$.
Alors en évaluant en a, il vient $P(a)=Q(a)(a-a)=0$.

Inversement, supposons que $P(a)=0$. Soit alors $P=(X-a)Q+R$ la division euclidienne de P par $X-a$, avec $\deg R<\underbrace{\deg(X-a)}_{=1}$.
Alors R est un polynôme constant λ. Mais en évaluant en a,

$$P(a)=(a-a)Q(a)+\lambda \Leftrightarrow P(a)=\lambda.$$

Et donc si $P(a)=0$, alors $\lambda=0$, et donc $P=(X-a)Q$ est divisible par $X-a$. □

Proposition-définition Soit $P\in\mathbf{K}[X]$ non nul, et soit $a\in\mathbf{K}$. Alors $\{k\in\mathbf{N}$ tel que $(X-a)^k\mid P\}$ possède un plus grand élément, qu'on appelle la **multiplicité de** a dans P.
Si cette multiplicité est nulle, alors a n'est pas racine de P.
Si elle vaut 1, alors P est divisible par $X-a$ mais pas par $(X-a)^2$, on dit que a est racine simple de P.
Si elle vaut 2, alors P est divisible par $(X-a)^2$ mais pas par $(X-a)^3$, on dit alors que a est racine double de P, etc.

Remarques. Plus généralement, a est racine de multiplicité m de P si $(X-a)^m\mid P$ et $(X-a)^{m+1}\nmid P$.
Ceci s'écrit encore : il existe $Q\in\mathbf{K}[X]$ tel que $P=(X-a)^mQ(X)$ et $Q(a)\neq 0$.

Démonstration. L'ensemble $\{k\in\mathbf{N},\ (X-a)^k\mid P\}$ est non vide puisqu'il contient toujours 0.
Et il est majoré puisque si $(X-a)^k\mid P$, alors $\deg\left((X-a)^k\right)\leqslant\deg P$, et donc $k\leqslant\deg P$.
Par conséquent, comme toute partie non vide et majorée de $\mathbf{N}$, il possède un plus grand élément m. □

Corps contenant Q.
Si je vous dis «corps qui contient $\mathbf{Q}$», vous pensez évidemment à $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$.
Mais nous en avons déjà rencontré au moins un autre : $\mathbf{Q}(\sqrt{2})$.
En revanche, ne pas en déduire trop rapidement que ce qui suit n'est valable que dans des corps infinis : il existe des corps infinis sur lesquels elle n'est pas valable.

17.3.2 Multiplicité et dérivées

La formule qui suit est un exemple de formule qui n'est plus valable dans les corps finis. La raison en est que, par exemple, dans $\mathbf{Z}/p\mathbf{Z}$, $p!=0$, et donc n'est pas inversible.
Nous énonçons donc les résultats pour $\mathbf{R}$ ou $\mathbf{C}$, mais plus généralement ceci reste valable dans n'importe quel corps qui contient $\mathbf{Q}$.

Proposition 17.33 (Formule de Taylor pour les polynômes) : *Soit $P \in \mathbf{R}[X]$ ou $\mathbf{C}[X]$, et soit $n = \deg P$. Alors* $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

En particulier, pour $a = 0$, on obtient

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

de sorte que le coefficient de degré k de P est $\frac{P^{(k)}(0)}{k!}$.

Démonstration. ▶ Commençons par le cas $a = 0$.
Il est facile de prouver par récurrence sur k que la dérivée $k^{\text{ème}}$ de X^i est
$i(i-1)\cdots(i-k+1)X^{i-k} = \frac{i!}{(i-k)!}X^{i-k}$ si $k \leqslant i$ et est nulle si $k > i$.
Donc si $P = \sum_{i=0}^{+\infty} a_i X^i$, $P^{(k)} = \sum_{i=k}^{+\infty} a_i \frac{i!}{(i-k)!}X^{i-k}$ et donc $P^{(k)}(0) = a_k k!$.
Soit encore $a_k = \frac{P^{(k)}(0)}{k!}$ et donc $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!}X^k$.

Remarque

On a là une composée de polynômes : c'est P composé par le polynôme (unitaire, de degré 1) $X + a$.

▶ Dans le cas général, posons $Q(X) = P(X + a)$.
On a alors $Q'(X) = P'(X + a)$, puis $Q''(X) = P''(X + a)$, et une récurrence rapide prouve que pour tout $k \in \mathbf{N}$, $Q^{(k)}(X) = P^{(k)}(X + a)$.
Et donc

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

En composant à droite par $X - a$, on a donc

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

□

Si a est une racine double de P, il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-a)^2 Q$, et Q n'est pas divisible par $X - a$, donc $Q(a) \neq 0$.
On a alors $P' = 2(X-a)Q + (X-a)^2 Q'$, de sorte que $P'(a) = 0$.
Et alors $P'' = 2Q + 2(X-a)Q' + 2(X-a)Q' + (X-a)^2 Q''$, de sorte que $P''(a) = 2Q(a) \neq 0$.
En fait, il s'agit là ($P(a) = P'(a) = 0$ et $P''(a) \neq 0$) est une caractérisation des racines doubles, ce que prouve et généralise la proposition suivante.

Proposition 17.34 : *Soit $P \in \mathbf{K}[X]$, et soit $a \in \mathbf{K}$, avec $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$. Alors a est racine de multiplicité $m \in \mathbf{N}^*$ de P si et seulement si*

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

Démonstration. Notons $n = \deg P$.
Si $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$, alors par la formule de Taylor polynomiale,

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

est bien divisible par $(X-a)^m$.
Donc déjà la multiplicité de a est supérieure ou égale à m.
Et alors $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$. Donc la multiplicité de a est égale à m.

Inversement, supposons que a soit une racine de multiplicité m de P.
Alors $P = (X-a)^m Q$, avec $Q(a) \neq 0$.
Mais par la formule de Taylor,

$$P = (X-a)^m \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} + \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k}_{\in \mathbf{K}_{m-1}[X]}.$$

Détails
L'écriture
$P = (X-a)^m Q + 0_{\mathbf{K}[X]}$
satisfait les conditions d'une division euclidienne : par unicité, c'est donc **la** division euclidienne de P par $(X-a)^m$.

Par unicité de la division euclidienne de P par $(X-a)^m$, on a donc

$$\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} = Q \text{ et } \sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k = 0.$$

Composons cette dernière relation à droite par $X+a$, de sorte que

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

Par identification des coefficients, on a donc pour tout $k \in [\![0, m-1]\!]$, $\dfrac{P^{(k)}(a)}{k!} = 0$, et donc $P^{(k)}(a) = 0$.
Et en évaluant la première relation en $X = a$, il vient

$$\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(a-a)^{k-m} = Q(a) \Leftrightarrow \frac{P^{(m)}(a)}{m!} = Q(a) \Leftrightarrow P^{(m)}(a) = m!Q(a) \neq 0.$$

□

Exemples 17.35

2 est racine double de $P = X^4 - 3X^3 + X^2 + 4$.
En effet, on a $P(2) = 0$, puis $P'(X) = 4X^3 - 9X^2 + 2X$, donc $P'(2) = 0$, et $P'' = 12X^2 - 18X + 2$ et donc $P''(2) = 14 \neq 0$.

L'utilisation des dérivées permet de calculer des restes dans des divisions euclidiennes par un polynôme possédant une racine multiple.
Par exemple, cherchons le reste de la division euclidienne de $X^n + 1$ par $(X+1)^2$.
Nous savons que la division euclidienne cherchée est de la forme
$(\star)$ $X^n + 1 = (X+1)^2 Q_n + R_n$, avec $\deg R_n \leqslant 1$.
Autrement dit, il doit exister deux réels a_n et b_n tels que $R_n = a_n X + b_n$.
Et alors en évaluant en $X = -1$,

$$(-1)^n + 1 = (-1+1)^2 Q_n(-1) + (b_n - a_n) \Leftrightarrow b_n - a_n = (-1)^n + 1.$$

En l'absence d'autre racine de $(X+1)^2$, on ne peut pas en tirer une seconde solution.
Mais en dérivant $(\star)$, il vient,

$$nX^{n-1} = 2(X+1)Q_n + (X+1)^2 Q_n' + R_n'$$

qui après évaluation en $X = -1$ nous donne $n(-1)^{n-1} = a_n$ et donc $R_n = n(-1)^{n-1}X + (-1)^n(n-1) + 1$.

Corollaire 17.36 – *Si a est racine de P de multiplicité $m \geqslant 2$, alors a est racine de P' de multiplicité $m-1$.*

Démonstration. On a $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.
Donc en particulier,

$$P'(a) = (P')'(a) = \cdots = (P')^{(m-2)}(a) = 0 \text{ et } (P')^{(m-1)}(a) \neq 0.$$

Donc a est racine de P' de multiplicité $m-1$. □

17.3.3 Factorisation par les racines

Proposition 17.37 : *Soit $P \in \mathbf{K}[X]$ **non nul**, et soient $\lambda_1, \dots, \lambda_r$ des racines deux à deux distinctes de P, de multiplicités respectives $m_1, \dots m_r$.*
Alors $(X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}$ divise P.

Démonstration. Prouvons par récurrence sur $k \in [\![1, r]\!]$ que $\mathscr{P}(k)$: $(X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k}$ divise P.
Pour $k = 1$, ceci découle de ce qui a été dit précédemment : λ_1 est racine d'ordre m_1 de P, qui est donc divisible par[7] $(X-\lambda_1)^{m_1}$.
Supposons donc $\mathscr{P}(k)$ soit vraie.
Alors il existe $Q_k \in \mathbf{K}[X]$ tel que $P = (X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k} Q_k$.
Puisque λ_{k+1} est racine de P d'ordre m_{k+1}, $P = (X-\lambda_{k+1})^{r_{k+1}} A$, pour un certain $A \in \mathbf{K}[X]$ tel que $A(\lambda_{k+1}) \neq 0$.
Notons par ailleurs n_{k+1} la multiplicité de λ_{k+1} en tant que racine de Q_k : $Q_k = (X-\lambda_{k+1})^{n_{k+1}} B$, avec $B(\lambda_{k+1}) \neq 0$.
Puisque Q_k divise P, $n_{k+1} \leqslant m_{k+1}$. Et alors on a

$$P = (X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k} (X-\lambda_{k+1})^{n_{k+1}} B = (X-\lambda_{k+1})^{m_{k+1}} A.$$

Mais nous avons déjà mentionné que $\mathbf{K}[X]$ étant un anneau intègre, il est possible de simplifier par $(X-\lambda_{k+1})^{n_{k+1}}$. Et alors

$$(X-\lambda_1)^{n_1} \cdots (X-\lambda_k)^{n_k} B = (X-\lambda_{k+1})^{m_{k+1}-n_{k+1}} A.$$

Puisque λ_{k+1} n'est pas racine du membre de gauche, elle n'est pas non plus racine du membre de droite, donc $m_{k+1} - n_{k+1} = 0 \Leftrightarrow m_{k+1} = n_{k+1}$.
Donc $(X-\lambda_{k+1})^{m_{k+1}}$ divise Q_k, et donc P est multiple de $(X-\lambda_1)^{m_1} \cdots (X-\lambda_{k+1})^{m_{k+1}}$.
Par le principe de récurrence, blablabla. □

[7] C'est là la définition de la multiplicité d'une racine.

Kids, don't try this !
Ces récurrences ont été rédigées par un professionnel expérimenté, il est dangereux d'essayer de reproduire de telles rédactions dans vos copies.

Exemple 17.38

Cherchons pour quelles valeurs de $n \in \mathbf{N}$ le polynôme $X^n + 1$ est divisible par $X^2 + 1$.
On $X^2 + 1 \mid X^n + 1 \Leftrightarrow i$ et $-i$ sont racines de $X^n + 1$.
Ce qui est le cas si et seulement si $i^n = -1$ et $(-i)^n = -1$.
Soit si et seulement si n est pair et $i^n = -1$ donc ssi $n \equiv 2$ [4].

Corollaire 17.39 – *Avec les notations précédentes, on a $\sum_{k=1}^{r} m_k \leqslant \deg P$.*
Donc un polynôme non nul ne peut avoir plus de racines (comptées avec multiplicité) que son degré.

⚠ Ne pas confondre le nombre de racines et le nombre de racines **comptées avec multiplicité**.
Par exemple, $X^3(X+1)^4(X-2)(X+2)$ est un polynôme de degré 9, qui ne possède que 4 racines, mais qui en possède $9 = 3 + 4 + 1 + 1$ si on les compte avec multiplicités.

Par contraposée, on en déduit que :

Corollaire 17.40 – *Soit $P \in \mathbf{K}_n[X]$. Si P possède $n+1$ racines distinctes, alors $P = 0$.*

Une formulation un peu différente du même résultat, et qui ne nécessite pas d'information sur le degré de P est la suivante :

Proposition 17.41 : *Un polynôme qui possède une infinité de racines est nécessairement le polynôme nul.*

Exemple 17.42 **La racine carrée n'est pas une fonction polynomiale**

Il n'existe pas de polynôme $P \in \mathbf{C}[X]$ tel que pour tout $x \in \mathbf{R}_+$, $P(x) = \sqrt{x}$.
En effet, supposons par l'absurde qu'un tel polynôme existe, et soit $Q = P^2 - X$.
Alors pour tout $n \in \mathbf{N}$, $Q(n) = P^2(n) - n = \left(\sqrt{n}\right)^2 - n = n - n = 0$.
Donc Q possède une infinité de racines, et par conséquent est nul.
Donc $\deg P^2 = \deg X \Leftrightarrow 2\deg P = 1$, ce qui n'est pas possible.

Définition 17.43 – Un polynôme $P \in \mathbf{K}[X]$ est dit **scindé** (sur $\mathbf{K}$) s'il est non constant et possède autant de racines (comptées avec multiplicité) que son degré.

Autrement dit
Les polynômes scindés sont ceux qui possèdent le nombre maximal de racines.

Proposition 17.44 : *Un polynôme $P \in \mathbf{K}[X]$ est scindé sur $\mathbf{K}$ si et seulement si et seulement si il existe $\lambda_1, \dots, \lambda_n \in \mathbf{K}$ et $m_1, \dots, m_n \in \mathbf{N}^*$, ainsi que $\alpha \in \mathbf{K}^*$ tel que $P = \alpha \prod_{i=1}^{n} (X - \lambda_i)^{m_i}$.*
Et alors :

- *α est le coefficient dominant de P*
- *les λ_i sont les racines de P, de multiplicité m_i.*

Démonstration. Si P est scindé, alors il existe $\lambda_1, \dots, \lambda_r$ des racines de multiplicités $m_1, \dots, m_r$, avec $\sum_{i=1}^{r} m_i = \deg P$.

Donc[8] P se factorise par $\prod_{i=1}^{r} (X - \lambda_i)^{m_i}$, qui a même degré que P.
Donc le quotient est de degré nul : c'est une constante non nul $\alpha \in \mathbf{K}^*$.
Puisque $\prod_{i=1}^{r} (X - \lambda_i)^{m_i}$ est unitaire, le coefficient dominant de P est nécessairement α.

Inversement, si $P = \alpha \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$, avec $\lambda_1, \dots, \lambda_r$ sont des racines de P, λ_i étant de multiplicité n_i, avec $n_i \geqslant m_i$.
Mais puisque $\sum_{i=1}^{r} m_i = \deg P$, et $\sum_{i=1}^{r} n_i \leqslant \deg P$, nécessairement, pour tout $i \in [\![1, r]\!]$, $m_i = n_i$.
Et P ne peut évidemment pas posséder d'autres racines que $\lambda_1, \dots, \lambda_r$. □

[8] C'est la proposition 17.37.

⚠ Attention à ne pas oublier le α, qui correspond au coefficient dominant dans la factorisation en produit de facteurs de degré 1.

Par exemple, $P(X) = 2X^3 - 4X^2 + 2X$ possède 0 comme racine simple[9] et 1 comme racine double.
On n'en déduit pas que $P(X) = X(X-1)^2$, mais bien que $P(X) = 2X(X-1)^2$.

[9] Il est divisible par X et pas par X^2.

Proposition 17.45 : *Soient $P, Q \in \mathbf{K}[X]$ **avec** P **scindé**. Alors P divise Q si et seulement si toutes les racines de P sont racines de Q, avec une multiplicité en P inférieure ou égale à la multiplicité en Q.*

Démonstration. Notons $\lambda_1, \dots, \lambda_r$ les racines de P, de multiplicités respectives $m_1, \dots, m_r$, de sorte que $P = \alpha \prod_{i=1}^{n} (X - \lambda_i)^{m_i}$.
Il est évident[10] que si P divise Q, alors les λ_i sont des racines de Q de multiplicité supérieure ou égale à m_i.

[10] Et ne nécessite pas que P soit scindé.

Inversement, si tous les λ_i sont des racines de Q, avec une multiplicité n_i supérieure ou égale à m_i. Alors il existe $R \in \mathbf{K}[X]$ tel que

$$Q = \prod_{i=1}^{r} (X - \lambda_i)^{n_i} R = \underbrace{\alpha \prod_{i=1}^{r} (X - \lambda_i)^{m_i}}_{=P} \times \frac{1}{\alpha} \prod_{i=1}^{r} (X - \lambda_i)^{n_i - m_i} R$$

et donc Q est divisible par P. □

17.3.4 Le théorème de d'Alembert-Gauss

Il est bien connu que certains polynômes à coefficients réels, par exemple $X^2 + 1$, ne possèdent pas de racine dans $\mathbf{R}$, mais possèdent des racines dans $\mathbf{C}$.
Par ailleurs, nous avons déjà vu que tout polynôme de degré 2 à coefficients complexes possède deux racines complexes si on les compte avec leur multiplicité, et que tout nombre complexe a non nul possède exactement n racines $n^{\text{èmes}}$, c'est-à-dire que $X^n - a$ est scindé.
Le résultat suivant vient généraliser largement ceci.

Théorème 17.46 (de d'Alembert-Gauss) : *Soit $P \in \mathbf{C}[X]$ non constant. Alors P possède une racine.*

Démonstration. Admis. □

[11] Il en existe des dizaines de nature parfois très très différentes.

La preuve n'est pas au programme de MPSI, même si certaines preuves[11] nous sont abordables.
Ce résultat, parfois appelé théorème fondamental de l'algèbre[12] a connu une première tentative de démonstration par d'Alembert, mais la première preuve vraiment rigoureuse[13] est dûe à Gauss, qui en donna au moins quatre preuves différentes.

[12] Bien qu'il s'agisse essentiellement d'un théorème d'analyse...

[13] Et presque complète.

Exemple 17.47

Si $P \in \mathbf{C}[X]$ est non constant, alors la fonction polynomiale $\widetilde{P}$ induit une surjection de $\mathbf{C}$ sur $\mathbf{C}$.
En effet, pour tout $\lambda \in \mathbf{C}$, $P - \lambda$ est un polynôme non constant, donc possède au moins une racine complexe.
Or une telle racine est un antécédent de λ par P.

Corollaire 17.48 – *Tout polynôme non constant de $\mathbf{C}[X]$ est scindé sur $\mathbf{C}$.*

Terminologie
On dit aussi que $\mathbf{C}$ est un corps **algébriquement clos**.

Démonstration. La preuve se fait par récurrence sur le degré de P.
Pour $\deg P = 1$, c'est exactement le théorème de d'Alembert-Gauss.
Supposons que tout polynôme de degré n soit scindé, et soit $P \in \mathbf{C}[X]$ un polynôme de degré $n + 1$.
Alors par le théorème de d'Alembert-Gauss, P possède une racine λ_1, et donc est divisible par $X - \lambda_1$: il existe $Q \in \mathbf{C}[X]$ tel que $P = (X - \lambda_1)Q$.
Mais Q est de degré n, et donc par hypothèse de récurrence est scindé.
On en déduit que P est scindé car produit de deux polynômes scindés. Par le principe de récurrence, tout polynôme non constant est scindé. □

Corollaire 17.49 – *Soient $P, Q \in \mathbf{C}[X]$, avec P non nul. Alors P divise Q si et seulement si toutes les racines de P sont des racines de Q, avec une multiplicité dans Q supérieure ou égale à la multiplicité dans P.*

Sur $\mathbf{R}$ un tel théorème n'est plus valable. Mais en notant qu'un polynôme à coefficients réels est un cas particulier de polynôme à coefficients complexes, on dispose tout de même du résultat suivant :

Proposition 17.50 : *Soit $P \in \mathbf{R}[X]$ non constant. Alors P possède une racine complexe.*

La racine de la proposition précédente peut tout à fait être réelle, par exemple dans le cas d'un polynôme scindé sur $\mathbf{R}$.
Par contre, pour les racines non réelles des polynômes à coefficients réels, notons qu'elles vont toujours par deux :

Proposition 17.51 : *Soit $P \in \mathbf{R}[X]$, et soit $\alpha \in \mathbf{C}$ une racine complexe de P. Alors $\overline{\alpha}$ est racine de P, de même multiplicité que α.*

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

Alors pour $z \in \mathbf{C}$, $P(\overline{z}) = \sum_{k=0}^{+\infty} a_k \overline{z}^k = \sum_{k=0}^{+\infty} \overline{a_k} \overline{z^k} = \overline{\sum_{k=0}^{+\infty} a_k z^k} = \overline{P(z)}$.
En particulier, α est racine de P si et seulement si $\overline{\alpha}$ est racine de P.
Et comme le même raisonnement vaut pour $P', P'', \dots$, alors α est racine d'ordre m de P si et seulement si

$$P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \text{ et } P^{(m)}(\alpha) \neq 0.$$

Et donc si et seulement si :

$$P(\overline{\alpha}) = P'(\overline{\alpha}) = \cdots = P^{(m-1)}(\overline{\alpha}) = 0 \text{ et } P^{(m)}(\overline{\alpha}) \neq 0.$$

Donc si et seulement si $\overline{\alpha}$ est racine d'ordre m de P. □

Proposition 17.52 : *Soit $P \in \mathbf{R}[X]$, et soit $\lambda \in \mathbf{C} \setminus \mathbf{R}$ une racine de P.*
Alors P est divisible dans $\mathbf{R}[X]$ par $(X-\lambda)(X-\overline{\lambda}) = X^2 - 2\operatorname{Re}(\lambda)X + |\lambda|^2$.

Démonstration. Nous avons déjà dit que $\overline{\lambda}$ est racine de P.
Puisque λ et $\overline{\lambda}$ sont deux racines distinctes de P, celui-ci est donc divisible, dans $\mathbf{C}[X]$, par $(X-\lambda)(X-\overline{\lambda})$.
Autrement dit, il existe $Q \in \mathbf{C}[X]$ tel que $P = (X-\lambda)(X-\overline{\lambda})Q$.
Mais alors, en conjuguant cette relation , il vient $\overline{P} = \overline{(X-\lambda)(X-\overline{\lambda})}\,\overline{Q}$.
Or P et $(X-\lambda)(X-\overline{\lambda})$ étant à coefficients réels, ils sont égaux à leurs conjugués.
Et donc $P = (X-\lambda)(X-\overline{\lambda})Q = (X-\lambda)(X-\overline{\lambda})\overline{Q}$.
Après simplification[14], on a donc $Q = \overline{Q}$, donc $Q \in \mathbf{R}[X]$.
Et donc P est bien divisible **dans** $\mathbf{R}[X]$ par $(X-\lambda)(X-\overline{\lambda})$. □

Conjugué ?
Je n'ai pas défini ce qu'est le conjugué d'un polynôme complexe, mais disons qu'il s'agit de ce que vous pensez (on conjugue chacun des coefficients), et qu'il a les propriétés que vous imaginez (en tous cas il est compatible à la somme et au produit).

[14] $\mathbf{C}[X]$ est intègre.

17.3.5 Factorisation irréductible

Définition 17.53 – Un polynôme $P \in \mathbf{K}[X]$ est dit **irréductible** s'il n'est pas constant et si ses seuls diviseurs sont les polynômes constants et les λP, $\lambda \in \mathbf{K}^*$.

Un autre moyen de le dire est le suivant : P est irréductible si et seulement si

$$\forall (Q,R) \in \mathbf{K}[X]^2,\ P = QR \Rightarrow (\deg Q = 0 \textbf{ ou } \deg R = 0).$$

Remarque
Ces polynômes sont les analogues dans $\mathbf{K}[X]$ des nombres premiers dans $\mathbf{Z}$.

Proposition 17.54 : *Tout polynôme non constant de* $\mathbf{K}[X]$ *est produit d'irréductibles.*

Démonstration. Par récurrence forte sur le degré n de P.
Pour $n = 1$, c'est évident : un diviseur d'un polynôme P de degré 1 est de degré inférieur ou égal à 1. Soit il est constant, soit il est de degré 1, mais alors doit être de la forme λP, $\lambda \in \mathbf{K}^*$.
Supposons à présent que tout polynôme de degré au plus n est produit de facteurs irréductibles et soit P de degré $n+1$.
Si P est irréductible, alors il n'y a rien à dire.
Sinon, soit Q un diviseur de P, qui ne soit ni constant, ni égal à un multiple scalaire de P, et soit $R \in \mathbf{K}[X]$ tel que $P = QR$.
Alors $\deg Q \in [\![1, n]\!]$, et de même pour $\deg R$. Et donc par hypothèse de récurrence, et Q et R sont produits de polynômes irréductibles, et donc il en est de même de P.
Par le principe de récurrence forte, tout polynôme non constant est produit de facteurs irréductibles. □

Autrement dit
Les polynômes de degré 1 sont toujours irréductibles, et ce indépendamment du corps $\mathbf{K}$ sur lequel on se place.

Théorème 17.55 (Factorisation irréductible sur C) :

1. *Les polynômes irréductibles de* $\mathbf{C}[X]$ *sont les polynômes de degré* 1.
2. *Si* $P \in \mathbf{C}[X]$ *est non constant, alors sa factorisation en produit de facteurs irréductibles unitaires est unique (à l'ordre des facteurs près) et vaut*

$$P = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{r_k}$$

où $\lambda_1, \dots, \lambda_r$ *sont les racines distinctes de* P, r_k *est la multiplicité de* λ_k *et* α *est le coefficient dominant de* P.

Coeff dominant
Quitte à regrouper tous les coefficients dominants dans une même constante, nous pouvons supposer que tous les facteurs irréductibles sont unitaires, et que P s'écrit comme produit d'une constante et de polynômes irréductibles unitaires.

Démonstration.
1. Nous savons déjà que les polynômes de degré 1 sont irréductibles (comme sur tout corps).
   Et par ailleurs, si $P \in \mathbf{C}[X]$ est irréductible, alors il existe $\lambda \in \mathbf{C}$ racine de P. Donc P est divisible par $X - \lambda$.
   Par irréductibilité de P, il existe donc $\alpha \in \mathbf{C}^*$ tel que $P = \alpha(X - \lambda)$.
2. Si P est non constant, alors il est scindé, et donc de la forme annoncée.
   L'unicité vient tout simplement du premier point et de la proposition 17.44, qui dit que les λ_k et les r_k sont uniquement déterminés : ce sont les racines de P et leurs multiplicités.

□

Remarque. Cet énoncé est quelque peu imprécis[15] : on prouve en fait que tout polynôme s'écrit de manière unique comme le produit d'une constante non nulle (son coefficient dominant) et de facteurs irréductibles unitaires.
Si on oublie la constante, alors $2X - 2$ n'est pas produit d'irréductibles unitaires, et si on ne demande pas aux facteurs d'être unitaires, alors $2X - 2 = 2(X - 1) = \frac{1}{4}(4X - 4)$ s'écrit de plusieurs manières différentes comme produit d'une constante par un irréductible.

[15] Et le reformulerons et le reprouverons dans un corps quelconque en fin d'année lorsque nous étudierons l'arithmétique des polynômes.

Théorème 17.56 (Factorisation irréductible sur R) :

1. *les polynômes irréductibles de* $\mathbf{R}[X]$ *sont les polynômes de degré* 1 *et les polynômes de degré* 2 *de discriminant strictement négatif.*
2. *si* $P \in \mathbf{R}[X]$ *est non constant, alors sa factorisation en produit de facteurs irréductibles*

Autrement dit
Les polynômes irréductibles de degré 2 sont ceux qui n'ont pas de racine réelle.

unitaires est unique[16] *et est de la forme*

$$P = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k} \prod_{j=1}^{p} \left[\underbrace{(X - \mu_j)(X - \overline{\mu_j})}_{= X^2 - 2\operatorname{Re}(\mu_j)X + |\mu_j|^2 \in \mathbf{R}[X]} \right]^{n_j}$$

où :

- α *est le coefficient dominant de* P
- $\lambda_1, \dots, \lambda_r$ *sont les racines* ***réelles*** *de* P *de multiplicités respectives* $m_1, \dots, m_r$
- $(\mu_1, \overline{\mu_1}), (\mu_2, \overline{\mu_2}), \dots, (\mu_p, \overline{\mu_p})$ *sont les paires de racines complexes non réelles conjuguées*[17] *de* P*, de multiplicités respectives* $n_1, n_2, \dots, n_k$

[16] À l'ordre des facteurs près.

[17] Rappelons que λ et $\overline{\lambda}$ ont même multiplicité.

Démonstration. 1. Si $P \in \mathbf{R}[X]$ est irréductible, alors il possède une racine λ complexe.
Si $\lambda \in \mathbf{R}$, alors P est divisible par $X - \lambda$, et étant irréductible, il existe $\alpha \in \mathbf{R}^*$ tel que $P = \alpha(X - \lambda)$.
Si $\lambda \in \mathbf{C} \setminus \mathbf{R}$, alors nous avons déjà dit que P est divisible (dans $\mathbf{R}[X]$) par $(X - \lambda)(X - \overline{\lambda}) = X^2 - 2\operatorname{Re}(\lambda)X + |\lambda|^2$.
Puisque P est irréductible, il existe donc $\alpha \in \mathbf{R}^*$ tel que

$$P = \alpha \left(X^2 - 2\operatorname{Re}(\lambda)X + |\lambda|^2 \right)$$

qui est évidemment de discriminant négatif.

Inversement si P est un polynôme de degré 2 de discriminant strictement négatif, alors il ne possède pas de racine réelle, et donc n'est pas divisible par aucun polynôme de degré 1.
Et donc tout diviseur de P est soit de degré 0, soit de degré 2, donc P est irréductible.

2. Si $P \in \mathbf{R}[X]$ est non constant, il possède une unique factorisation scindée sur $\mathbf{C}$.
Et alors en regroupant les racines réelles conjuguées, on obtient bien la factorisation souhaitée.
Celle-ci est unique faute de quoi on aurait plusieurs formes scindées sur $\mathbf{C}$.

□

17.3.6 Relations racines-coefficients

Nous avons déjà vu que les coefficients d'un polynôme du second degré s'expriment aisément en fonction des racines.
Les relations qui suivent généralisent largement cet énoncé.

Définition 17.57 – Soit $P = \alpha \prod_{k=1}^{n} (X - \lambda_k)$ un polynôme **scindé** de degré $n \geqslant 1$.
On note alors $\sigma_1 = \lambda_1 + \cdots + \lambda_n$,

$$\sigma_2 = (\lambda_1\lambda_2 + \cdots + \lambda_1\lambda_n) + (\lambda_2\lambda_3 + \cdots + \lambda_2\lambda_n) + \cdots + \lambda_{n-1}\lambda_n$$

et plus généralement, pour $k \in [\![1, n]\!]$,

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

Notons qu'en particulier, $\sigma_n = \lambda_1 \cdots \lambda_n$.

⚠ Attention !
On ne suppose pas ici que les λ_i soient distincts, il peut y avoir des racines multiples.

Exemple 17.58

Dans le cas d'un polynôme de degré 3, qui possède trois racines $\lambda_1, \lambda_2, \lambda_3$, éventuellement confondues, alors

$$\sigma_1 = \lambda_1 + \lambda_2 + \lambda_3,\ \sigma_2 = \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3$$

Ainsi, σ_2 est la somme de tous les produit de deux racines, etc, σ_k est la somme de tous les produit de k racines (**attention** : je n'ai pas dit de racines distinctes !)

Exemple 17.59

Si P possède une racine double λ, alors σ_2 contiendra un terme égal à λ^2.
Si P possède une racine triple λ, alors σ_2 contiendra trois fois λ^2.

Proposition 17.60 (Relation entre racines et coefficients) : *Soit* $P = \sum_{k=0}^{n} a_k X^k$ *un polynôme* ***scindé*** *de degré* n. *Alors*

$$\forall k \in [\![1, n]\!],\ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Démonstration. Il s'agit d'identifier des coefficients de $\sum_{k=0}^{n} a_k X^k = \alpha \prod_{k=1}^{n} (X - \lambda_k)$.
Pour le coefficient dominant, notons que celui du produit est α, car la seule manière d'obtenir un terme en X^n en développant le produit est de multiplier tous les termes en X.
Donc déjà, $\alpha = a_n$.
Quitte à diviser P par a_n, ce qui ne change pas les racines, on peut donc supposer P unitaire.
Alors le coefficient de degré $n-1$ de $\prod_{k=1}^{n}(X-\lambda_k)$ est obtenu lorsqu'en développant le produit, on choisit tous les termes égaux à X, sauf un, égal à l'un des $-\lambda_k$.
Donc $a_{n-1} = -\lambda_1 - \cdots - \lambda_n = -\sigma_1$.
Puis pour le terme de degré $n-2$, c'est le même principe : il faut choisir $n-2$ fois X et deux des $-\lambda_i$.
Le coefficient en X^{n-2} est donc $\sum_{1 \leqslant i_1 < i_2 \leqslant n} \lambda_i \lambda_j$.
Etc. □

Exemple 17.61

Si $P(X) = X^n - 1$. Alors les racines de P sont les $e^{i\frac{2k\pi}{n}}$, $k \in [\![0, n-1]\!]$.
Nous savons déjà que $\sum_{k=0}^{n-1} e^{2i\frac{k\pi}{n}} = 0$, mais on a également
$\sigma_2 = \sum_{1 \leqslant k < \ell \leqslant n-1} e^{2i\frac{(k+\ell)\pi}{n}} = 0$, puis $\sigma_3 = 0$, etc jusqu'à

$$\sigma_n = \prod_{\omega \in \mathbf{U}_n} \omega = (-1)^{n+1}.$$

17.3.7 Retour sur les fonctions polynomiales

La distinction entre fonctions polynomiales et polynômes n'est pas vraiment importante lorsqu'on travaille sur $\mathbf{R}$ ou sur $\mathbf{C}$.

Pourtant, dans certains contextes, elle peut s'avérer fondamentale.
Par exemple, dans $\mathbf{Z}/p\mathbf{Z}[X]$, où p est premier, les polynômes $P = X$ et $Q = X^p$ sont distincts, puisque de degré distincts.
Pourtant, par le petit théorème de Fermat, pour tout $x \in \mathbf{Z}/p\mathbf{Z}$, $x^p = x$.
Et donc les fonctions polynomiales $\tilde{P}$ et $\tilde{Q}$ sont égales, bien que les polynômes soient différents.

Proposition 17.62 : *Si $\mathbf{K}$ est infini, alors l'application $P \mapsto \tilde{P}$ est une bijection entre l'ensemble $\mathbf{K}[X]$ des polynômes et l'ensemble des fonctions polynomiales sur $\mathbf{K}$.*

Démonstration. La surjectivité est immédiate par définition d'une fonction polynomiale.
Soient donc P et Q deux polynômes tels que $\widetilde{P} = \widetilde{Q}$.
Alors en particulier, tout élément λ de $\mathbf{K}$ vérifie $\widetilde{P}(\lambda) - \widetilde{Q}(\lambda) = 0$, donc est racine de $P - Q$.
Si $\mathbf{K}$ est infini, $P - Q$ possède une infinité de racines, et donc est nul.
Et donc $P = Q$, de sorte que $P \mapsto \widetilde{P}$ est injective. □

Plus généralement, si A est une partie infinie de $\mathbf{K}$, alors $P \mapsto \widetilde{P}_{|A}$ est une bijection de $\mathbf{K}[X]$ sur l'ensemble des fonctions polynomiales sur A.
Par exemple on peut identifier $\mathbf{R}[X]$ à l'ensemble des fonctions polynomiales sur $\mathbf{R}_+$ ou sur $[0, 1]$.

17.4 Polynômes interpolateurs de Lagrange

Remarque
On dispose donc de $n + 1$ scalaires.

Dans cette partie, on considère $\lambda_0, \lambda_1, \dots, \lambda_n$ des éléments de $\mathbf{K}$ **deux à deux distincts.**
La question est alors la suivante : connaissant les valeurs que prend $P \in \mathbf{K}[X]$ en les λ_i, est-il possible de déterminer P ?

La réponse est clairement non dans le cas général, puisque si on ajoute un multiple de $\prod_{i=0}^{n}(X - \lambda_i)$ à un polynôme, on ne change pas sa valeur en les λ_i.
Toutefois, nous allons voir que la réponse est oui pour des polynômes de degré au plus n.

Définition 17.63 – Soient $\lambda_0, \lambda_1, \dots, \lambda_n$ des éléments de $\mathbf{K}$ deux à deux distincts.
Pour $i \in [\![0, n]\!]$, on appelle $i^{\text{ème}}$ polynôme de Lagrange associé à $(\lambda_0, \dots, \lambda_n)$ le polynôme

$$L_i = \prod_{\substack{k=0 \\ k \neq i}}^{n} \frac{X - \lambda_k}{\lambda_i - \lambda_k} = \frac{X - \lambda_0}{\lambda_i - \lambda_0} \cdots \frac{X - \lambda_{i-1}}{\lambda_i - \lambda_{i-1}} \frac{X - \lambda_{i+1}}{\lambda_i - \lambda_{i+1}} \cdots \frac{X - \lambda_n}{\lambda_i - \lambda_n}.$$

Notons tout de suite que les L_i sont tous des polynômes de degré n car produits de n termes de degré 1.

Proposition 17.64 : *Avec les notations précédentes,*

$$\forall (i, j) \in [\![0, n]\!]^2,\ L_i(\lambda_j) = \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

Démonstration. Si $j \neq i$, alors L_i est divisible par $X - \lambda_j$, et par conséquent possède λ_j comme racine. Donc $L_i(\lambda_j) = 0$.
Et pour $j = i$, on

$$L_i(\lambda_i) = \prod_{\substack{k=0 \\ k \neq i}}^{n} \frac{\lambda_i - \lambda_k}{\lambda_i - \lambda_k} = 1.$$

□

Notons que parmi les polynômes de $\mathbf{K}_n[X]$, il n'y a qu'un seul polynôme, à i fixé, vérifiant $P(\lambda_j) = \delta_{i,j}$.
En effet, un tel polynôme doit avoir les λ_k, $k \neq i$ comme racines, et donc est divisible par $\prod_{\substack{k=0\\k\neq i}}^{n}(X-\lambda_k)$.
Mais ce produit est précisément de degré n, et $\deg P \leqslant n$: il existe donc $\lambda \in \mathbf{K}$ tel que $P = \lambda \prod_{\substack{k=0\\k\neq i}}^{n}(X-\lambda_k)$.

Et alors $P(\lambda_i) = \lambda \prod_{\substack{k=0\\k\neq i}}^{n}(\lambda_i-\lambda_k)$.

Donc $P(\lambda_i) = 1 \Leftrightarrow \lambda \prod_{\substack{k=0\\k\neq i}}^{n}(\lambda_i-\lambda_k) = 1 \Leftrightarrow \lambda = \prod_{\substack{k=0\\k\neq i}}^{n}\frac{1}{\lambda_i-\lambda_k}$.

Proposition 17.65 : *Soit $P \in \mathbf{K}_n[X]$. Alors P s'écrit de manière unique comme combinaison linéaire des L_i, c'est-à-dire qu'il existe un unique $(n+1)$-uplet $\alpha_0, \dots, \alpha_n) \in \mathbf{K}^n$ tel que $P = \sum_{i=0}^{n}\alpha_i L_i$.*

Plus précisément, cette unique écriture est $P = \sum_{i=0}^{n} P(\lambda_i)L_i$.

Démonstration. Soit $P \in \mathbf{K}_n[X]$. Supposons que $P = \sum_{k=0}^{n}\alpha_k L_k$.

Alors pour tout $i \in [\![0,n]\!]$, $P(\lambda_i) = \sum_{k=0}^{n}\alpha_k L_k(\lambda_i) = \alpha_i L_i(\lambda_i) = \alpha_i$.
Donc si une telle écriture existe, elle est unique.

Inversement, considérons le polynôme $Q = P - \sum_{k=0}^{n} P(\lambda_k)L_k$.
Alors pour tout $i \in [\![0,n]\!]$, $Q(\lambda_i) = P(\lambda_i) - P(\lambda_i)L_i(\lambda_i) = 0$.
Donc Q possède au moins $n+1$ racines distinctes. Mais il est de degré au plus n, car P et les L_k le sont, donc il est nul.
Et par conséquent, $P = \sum_{k=0}^{n} P(\lambda_k)L_k$. □

Remarque
Plus généralement, deux polynômes de degré au plus n qui coïncident en $n+1$ points sont égaux.

Exemple 17.66

Il existe un unique polynôme $P \in \mathbf{R}_n[X]$ tel que pour $i \in [\![0,n]\!]$, $P(i) = \sqrt{i}$.
En effet, notons $\lambda_0 = 0, \dots, \lambda_n = n$ et $L_0, \dots, L_n$ les polynômes interpolateurs de Lagrange associés.
Si un polynôme $P \in \mathbf{R}_n[X]$ satisfaisant les conditions existe, alors nécessairement

$$P = \sum_{i=0}^{n} P(i)L_i = \sum_{i=0}^{n}\sqrt{i}L_i.$$

Donc un tel polynôme, s'il existe, est unique.
Et si on pose $P = \sum_{i=0}^{n}\sqrt{i}L_i$, alors pour tout $j \in [\![0,n]\!]$, $P(j) = \sum_{i=0}^{n}\sqrt{i}L_i(j) = \sqrt{j}L_j(j) = 1$, de sorte que P convient.

⚠ Si on est assurés que ce polynôme coïncide avec la fonction racine en 0, 1 et 2, on n'a aucune garantie sur son comportement ailleurs qu'en ces trois points, et il n'a pas de raison d'être proche de $\sqrt{x}$, même entre 0 et 2.

Le même principe que ci-dessus s'applique pour n'importe quelle fonction f que l'on souhaiterait «approcher» par un polynôme de degré au plus n, en ce sens qu'on peut trouver un polynôme de degré au plus n qui coïncide avec f en n points fixés en avance.

Un résultat que vous connaissez bien : par deux points d'abscisses différentes passe une et une seule fonction affine[18].
Pour $n = 2$, on prouve de même que par trois points d'abscisses deux à deux distinctes passe une unique parabole[19] (ou une droite si les trois points sont alignés).
Et plus généralement, pour $n + 1$ points d'abscisses distinctes, il existe un unique polynôme de degré au plus n dont la courbe représentative passe par ces points.

[18] Polynôme de degré au plus 1.
[19] Polynôme de degré 2.