Chapitre 11
Polynômes

Table des matières

Vidal AGNIEL

Un polynôme s'écrit de la forme :

$$P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0,$$

où les a_i s'appellent les coefficients de P et X où est l'indéterminée.
Le premier problème est de définir correctement ce que l'on veut dire par "l'indéterminée X", de choisir à quel ensemble appartiennent les coefficients a_i, et d'avoir les outils nécessaires pour manipuler les polynômes efficacement.
On retrouvera les polynômes tant en analyse (par ex. les développements limités) qu'en algèbre (par ex. polynôme caractéristique d'une application linéaire). Une bonne maîtrise des produits, divisions et factorisations de polynômes ainsi que de la caractérisation des racines est indispensable.

1 Polynômes, opérations sur les polynômes

1.1 Polynômes à une indéterminée

Dans tout ce chapitre, l'ensemble $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{Q}$. Ces ensembles sont des corps.

Définition 1
Soit $\mathbb{K}$ un corps. On appelle **indéterminée** un objet X que l'on peut :

- additionner avec lui-même : $X + X = 2X$
- multiplier par un élément de $\mathbb{K}$: $\lambda \times X$
- multiplier avec lui-même : $X^2 = X \times X$

Attention : L'indéterminée X n'est pas un nombre.

En fait, l'indéterminée X est une suite, et tous les polynômes sont des suites. La construction d'un polynôme n'est pas au programme.

Définition 2
Soit $\mathbb{K}$ un corps. On appelle **polynôme à une indéterminée** à coefficients dans $\mathbb{K}$ toute expression de la forme $a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$.
Ce sont des sommes finies, de multiples, des puissances de X.
L'ensemble des polynômes est noté $\mathbb{K}[X]$.
Un élément de $\mathbb{K}[X]$ se notera $P(X)$ (pour indiquer qu'il dépend de l'indéterminée X).
On écrira au choix $P(X) = a_0 + a_1X + \ldots + a_nX^n$ ou $P(X) = \sum_{k=0}^{n} a_kX^k$.
Les nombres $a_0, \ldots, a_n$ sont dans $\mathbb{K}$. Ce sont les **coefficients** de P.
Le nombre a_k est appelé **coefficient de degré** k de P.

Par convention, pour $P(X) = a_0 + a_1X + \ldots + a_nX^n$, on pose $a_k = 0$ pour tout $k > n$.

Remarque 3 (Définition formelle (HP)) —
Un polynôme $P \in \mathbb{K}[X]$ est une suite $(a_k)_k$ qui possède un nombre fini de termes non-nuls.
Autrement dit, on a $P = (a_k)_{k\geq 0} = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$.
Pour $k \in \mathbb{N}$, on définit X^k comme la suite qui vaut 1 au rang k et 0 ailleurs : $X^k = (0, \ldots, 0, 1, 0, \ldots)$.
On sait déjà additionner deux suites et multiplier une suite par une constante. On a par exemple $(2, 1, 3, 0, 0, \ldots) = 2.X^0 + 1.X^1 + 3.X^2 = 3X^2 + 2X + 1$.
Pour P, cela donne : $P = (a_0, \ldots, a_n, 0, \ldots) = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, \ldots, 0, a_n, 0, \ldots) = a_0(1, 0, \ldots) + a_1(0, 1, 0, \ldots) + \ldots + a_n(0, \ldots, 0, 1, 0, \ldots) = a_0X^0 + a_1X^1 + a_2X^2 + \ldots + a_nX^n = \displaystyle\sum_{k=0}^{n} a_kX^k$.

Remarque 4 — *L'indéterminée X est un élément très important pour travailler dans $\mathbb{K}[X]$.*
On écrit souvent $P(X)$ à la place de P. Cette écriture est parfois très utile (par exemple pour différencier un polynôme $P(X)$ de sa fonction polynômiale associée $x \mapsto P(x)$).

1.2 Opérations sur les polynômes

Définition 5 (**Opérations** $+, ., \times$ **sur les polynômes**)
Soit $\mathbb{K}$ un corps. On définit sur $\mathbb{K}[X]$ deux lois internes $(+, \times)$ et une loi externe $(.)$. Soient

$P(X) = a_0 + \ldots + a_n X^n, Q(X) = b_0 + \ldots + b_n X^n + \ldots + b_m X^m$ deux polynômes de $\mathbb{K}[X]$ (avec $n \leq m$).

1. L'addition, $+$, est définie par :

$$(a_0 + \ldots + a_n X^n) + (b_0 + \ldots + b_n X^n + \ldots + b_m X^m)$$
$$(a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \ldots + b_m X^m.$$

   Un tel objet est bien un polynôme.
   Le polynôme **nul**, noté $0_{\mathbb{K}[X]}$ ou 0, est l'élément neutre pour l'addition $+$.
2. La multiplication par un scalaire de $\mathbb{K}$, ., définie par :

$$\lambda.(a_0 + \ldots + a_n X^n) = (\lambda a_0) + (\lambda a_1)X + \ldots + (\lambda a_n)X^n.$$

3. La multiplication, $\times$, est définie par :

$$(a_0 + \ldots + a_n X^n) \times (b_0 + \ldots + b_n X^n + \ldots + b_m X^m) = c_0 + c_1 X + \ldots + c_{n+m} X^{n+m}, \text{ avec } c_r = \sum_{k=0}^{n} a_k b_{r-k}.$$

   Un tel objet est bien un polynôme car $c_k = 0$ pour $k > m + n$.
   Le polynôme **constant égal à** 1, noté $1_{\mathbb{K}[X]}$ ou 1, est l'élément neutre pour la multiplication $\times$.

Proposition 6
Soit $\mathbb{K}$ un corps. Soient $P, Q, R \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$. On a :

1. $P + (Q + R) = (P + Q) + R$ ($+$ est associative) ;
2. $P + Q = Q + P$ ($+$ est commutative) ;
3. $P + 0 = 0 + P = P$ (0 est le neutre de $+$) ;
4. $\lambda.(P + Q) = \lambda.P + \lambda.Q$ (. est distributive sur $+$) ;
5. $P \times (Q \times R) = (P \times Q) \times R$ ($\times$ est associatve) ;
6. $(P \times Q) = (Q \times P)$ ($\times$ est commutative) ;
7. $(P \times 1) = (1 \times P) = P$ (1 est le neutre de $\times$) ;
8. $P \times (Q + R) = P \times Q + P \times R = (Q + R) \times P$ ($\times$ est distributive sur $+$) ;
9. $P \times (\lambda.Q) = \lambda.P \times Q$ ($\times$ et . commutent).

L'ensemble $(\mathbb{K}[X], +, .)$ est un $\mathbb{K}$-espace vectoriel (comme $\mathbb{R}^2$ ou $\mathbb{R}^3$).
L'ensemble $(\mathbb{K}[X], +, \times)$ est un anneau (comme $\mathbb{R}$ ou $\mathbb{C}$).

Proposition 7 (**Egalité entre polynômes**) *Soit $\mathbb{K}[X]$ un corps. Soit $P(X) = a_0 + \ldots + a_n X^n \in \mathbb{K}[X]$. Deux polynômes P et Q sont égaux ssi tous leurs coefficients sont égaux. En particulier, P est le polynôme nul si et seulement si tous ses coefficients sont nuls (ssi $a_0 = a_1 = \ldots = a_n = 0$).*

Dans la définition d'un polynôme $P(X)$, les coefficients $a_0, \ldots, a_n$ sont pris dans $\mathbb{K}$ sans aucune condition. C'est-à-dire que l'on peut écrire : $X^2 = X^2 + 0.X^3 = X^2 + 0.X^{100}$.
Il existe une façon d'écrire un polynôme P qui est sans ambiguité. Cette écriture utilise ce que l'on appelle le coefficient dominant de P.

Proposition 8 (**Equations produit-nul**) *Un produit de deux polynômes est nul si et seulement si l'un des deux polynômes est nul.*

Écriture d'un polynôme

Proposition 9
Tout polynôme $P \in \mathbb{K}[X]$ non nul s'écrit de manière unique de la forme :

$$P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0,$$

avec $a_0, \ldots, a_n \in \mathbb{K}$ et $a_n \neq 0$.
Le coefficient a_n non-nul est alors appelé le **coefficient dominant** de P.

Preuve — Soit $P(X) = a_0 + \ldots + a_m X^m$ un polynôme.
Comme P est non-nul, il existe au moins un coefficient a_k de P tel que $a_k \neq 0$.
On pose n le plus grand indice tel que $a_m n \neq 0$ (il existe bien). Cela veut dire que pour tout $j > m$, on a $a_j = 0$.
Ainsi, on obtient que $P(X) = a_0 + \ldots + a_n X^n$. Comme l'entier n est unique (c'est LE plus grand indice), cette écriture est unique. □

REMARQUE 10 — *Pour écrire un produit de polynômes en utilisant le symbole $\sum$, cela donne :*

$$\left(\sum_{k=0}^{n} a_k X^k\right) \times \left(\sum_{k=0}^{m} b_k X^k\right) = \sum_{k=0}^{m+n} c_k X^k, \text{ avec } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

EXEMPLE 11 — *Pour multiplier rapidement deux polynômes, on utilise la distributivité du produit sur la somme et on regroupe les termes de même degré :*

$$\begin{aligned}(X+1)(X^3+X+2) &= X^4(1.1) + X^3(1.1) + X^2(1.1) + X(1.1+1.2) + (1.2) = X^4 + X^3 + X^2 + 3X + 2,\\ (X^2+X+1)(X^2-4X+3) &= X^4(1.1) + X^3(1.(-4)+1.1) + X^2(1.1+1.(-4)+1.3) + X(1.3+1.(-4)) + (1.3)\\ &= X^4 - 3X^3 - X + 3.\end{aligned}$$

REMARQUE 12 — *De la même façon, on peut aussi définir $\mathbb{Z}[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{Z}$. Cet ensemble n'est pas nouveau, car $\mathbb{Z}[X]$ est aussi le sous-ensemble de $\mathbb{Q}[X]$ des polynômes dont tous les coefficients sont entiers.*

Les polynômes à coefficients dans $\mathbb{Z}$ apparaissent beaucoup, mais il faut d'abord étudier les polynômes à coefficients dans un corps pour les comprendre. Ce chapitre étudie $\mathbb{K}[X]$.

1.3 Degré d'un polynôme

DÉFINITION 13
Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul.
On appelle **degré** de P, noté $\deg(P)$, le plus grand entier k tel que $a_k \neq 0$.
Pour $d = \deg P$, le nombre a_d est le **coefficient dominant** de P.
Le nombre a_0 est appelé le **coefficient constant** de P.
On dit que P est un polynôme **unitaire** si son coefficient dominant vaut 1.
Par convention, le degré du polynôme nul est $\deg(0) = -\infty$.

EXEMPLES 14
Le polynôme $2X^2 + X + 1$ n'est pas unitaire, mais $X^7 + X^3 + 2$ l'est. On a $\deg(X^7 + X^3 + 2) = 7$.
Pour $\lambda \in \mathbb{K}^*$ on a $\deg(\lambda) = 0$, tandis que $\deg(0) = -\infty$.
Pour tout $n \geq 0$, on a $\deg(X^n) = n$.

PROPOSITION 15
Soient $P,Q \in \mathbb{K}[X]$. On a alors :

1. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$;
   Si $\deg P \neq \deg Q$, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$.
2. $\deg(P \times Q) = \deg(P) + \deg(Q)$;
3. $\forall \lambda \in \mathbb{K}^*$, $\deg(\lambda.P) = \deg(P)$.

Preuve —

1. Si $P = 0$ alors $P + Q = Q$ et le résultat est évident. Il en est de même si $Q = 0$.
   Si $P \neq 0$ et $Q \neq 0$, alors, en posant $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ avec $n = \deg(P)$ et $m = \deg(Q)$, on a :
   $$P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k.$$
   Ainsi, cela donne :
   $$\deg(P+Q) \leqslant \max(\deg(P), \deg(Q)).$$

2. Si $P = 0$ ou $Q = 0$, alors $P \times Q = 0$ et :
$$\deg(P\,Q) = \deg(0) = -\infty = \deg(P) + \deg(Q)\,.$$
Sinon, on a $P = \sum_{k=0}^{n} a_k\, X^k$ avec $a_n \neq 0$ et $Q = \sum_{k=0}^{m} b_k\, X^k$ avec $b_m \neq 0$. Cela donne :
$$PQ = \sum_{k\in\mathbb{N}} \Big(\sum_{i+j=k} a_i b_j \Big) X^k.$$
Le coefficient de degré $n+m$ est $a_n b_m \neq 0$, et tous les coefficients de degré strictement supérieur à $n+m$ sont nuls. Donc, on a :
$$\deg(P\,Q) = \deg(P) + \deg(Q)\,.$$

□

Exemples 16

1. $\deg((X^3 + X + 3) + (X^2 + 2)) = 3$;
2. $\deg((X^3 + X + 3) + (-X^3 + 3X + 7)) = 1$;
3. $\deg((X^3 + X + 2)(X^5 + 3X^4 + 2)) = 8$.

Proposition 17
Soit $\mathbb{K}[X]$ un corps. Soient $P, Q \in \mathbb{K}[X]$.
On a $P \times Q = 0$ si et seulement si $P = 0$ ou $Q = 0$.

Démonstration — On regarde le degré de $P \times Q$.

Remarque 18 — *Attention ! L'écriture* $P(X) = \sum_{k=0}^{n} a_k X^k$ *avec* $a_0, \ldots, a_n \in \mathbb{K}$ *nous dit seulement que* $\deg(P) \leq n$. *Il faut rajouter la condition* $a_n \neq 0$ *pour avoir* $\deg(P) = n$.

Exemple 19 — *Quel est de degré du polynôme* $(X+1)^n - (X-1)^n$ *?*

Proposition 20
Soit $\mathbb{K}$ un corps.
Les polynômes $P \in \mathbb{K}[X]$ qui possèdent un inverse pour la multiplication $\times$ sont les polynômes constants et non-nuls.

Démonstration — On utilise l'équation $P \times Q = 1$, et les propriétés du degré des polynômes.

Ensemble $\mathbb{K}_n[X]$

Définition 21
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}$. On définit $\mathbb{K}_n[X]$ l'ensemble des polynômes sur $\mathbb{K}$ de degré inférieur ou égal à n :
$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X],\ \deg(P) \leq n\}.$$

On verra que l'ensemble $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $(\mathbb{K}[X], +, .)$, de dimension $n+1$.

1.4 Fonctions polynomiales, évaluation d'un polynôme

Définition 22
Soit $P(X) \in \mathbb{K}[X]$, avec $P(X) = \sum_{k=0}^{n} a_k X^k$.
On appelle **fonction polynomiale associée au polynôme** $P(X)$, notée f_P, la fonction définie par :
$$f_P : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & f_P(x) := \sum_{k=0}^{n} a_k x^k \end{array}.$$

Définition 23
Soit $P(X) \in \mathbb{K}[X]$, avec $P(X) = \sum_{k=0}^{n} a_k X^k$. Soit $a \in \mathbb{K}$.
On appelle **évaluation de** P **en** a le nombre $f_P(a)$.
On note alors $P(a) := f_P(a) = \sum_{k=0}^{n} a_k a^k$.

Exemple 24 — *La fonction $x \in \mathbb{R} \mapsto ax^2 + bx + c$ est la fonction polynômiale associée à $P(X) = aX^2 + bX + c \in \mathbb{R}[X]$.*
On a alors $P(1) = f_P(1) = a + b + c$, $P(0) = f_P(0) = 0 + 0 + c = c$.

L'intérêt de cette définition est de bien distinguer les trois objets que l'on peut manipuler : le polynôme $P(X)$, la fonction polynômiale f_P, le nombre $P(a)$ ou $f_P(a)$.
On utilise f_P et $P(a)$ pour étudier le polynôme $P(X)$.

Proposition 25
Soient $P, Q \in \mathbb{K}[X]$, et $\lambda \in \mathbb{K}$. On a :

- $f_{P+Q} = f_P + f_Q$
- $f_{\lambda P} = \lambda f_P$
- $f_{P \times Q} = f_P . f_Q$.

Démonstration — On écrit P et Q avec leurs coefficients, puis $P + Q$, λP, $P \times Q$, et on vérifie que les fonctions polynômiales associées coïncident.

Composition de polynômes

Définition 26
Soient $P, Q \in \mathbb{K}[X]$, avec $P(X) = \sum_{k=0}^{n} a_k \, X^k$.
On définit la composée des polynômes P et Q, notée $P \circ Q$, par le polynôme :

$$P \circ Q(X) = P(Q(X)) := \sum_{k=0}^{\infty} a_k \, Q(X)^k.$$

Remarque 27 —

1. *Dans le cas particulier où $Q(X) = X$, on a $P(Q(X)) = P(X)$. C'est pourquoi on utilise aussi bien les notations P que $P(X)$ pour désigner ce polynôme.*
2. *On fera attention au fait que l'opération de composition des polynômes n'est pas distributive à gauche avec $+, ., \times$. En effet, en général on a :*

   $$P \circ (Q+R)(X) \neq P \circ Q(X) + P \circ R(X) \ , \ \ P \circ (\lambda X) \neq \lambda P(X) \ \ \text{et} \ \ P \circ (Q \times R)(X) \neq P \circ Q(X) \times P \circ R(X).$$

3. *Pour $f_P : \mathbb{K} \to \mathbb{K}$ et $f_Q : \mathbb{K} \to \mathbb{K}$ les fonctions polynomiales associées aux polynômes P et Q, alors on a $f_{P \circ Q} = f_P \circ f_Q$.*
   La composée de polynômes est construite pour s'assimiler à une composée de fonctions.
   C'est pourquoi elle ne se comporte pas très bien avec l'addition et les multiplications.

Exemple 28 — *Pour $P(X) = X^2 + 2X + 3$, $\lambda = 2$, et $Q(X) = X + 1$, on a :*

$P \circ Q(X) = P(X + 1)(X + 1)^2 + 2(X + 1) + 3 = X^2 + 4X + 6$ et $P(\lambda . X) = 4X^2 + 4X + 3$,
tandis que $Q \circ P(X) = P(X) + P(1) = X^2 + 2X + 4$ et $\lambda . P(X) = 2X^2 + 4X + 6$.

Exercice 1 — *Soient $P, Q \in \mathbb{K}[X]$. Déterminer $\deg(P \circ Q)$ en fonction de $\deg(P)$ et $\deg(Q)$.*
On commencera par étudier le cas où $P(X) = X^k$, $Q(X) = X^l$.

Grâce à la notion de degré, on peut effectuer une action supplémentaire entre deux polynômes : la division euclidienne.
Cet élément est fondamental pour toute l'étude de la factorisation des polynômes.

2 Division euclidienne de polynômes

2.1 Notion de divisibilité

Définition 29
Soient A, $B \in \mathbb{K}[X]$ deux polynômes.
On dit que A **divise** B, noté $A|B$, s'il existe un polynôme $C \in \mathbb{K}[X]$ tel que $B = AC$.
On dit que B **est un multiple de** A, s'il existe un polynôme $C \in \mathbb{K}[X]$ tel que $B = AC$.

Remarque 30 — *On peut toujours diviser un polynôme P par son coefficient dominant pour le rendre unitaire.*
C'est pourquoi on travaille parfois seulement avec des polynômes unitaires.

Cette relation de divisibilité sur $\mathbb{K}[X]$ est similaire à celle sur $\mathbb{Z}$. Travailler "au coefficient dominant près" dans $\mathbb{K}[X]$ est égal à travailler "au signe près" dans $\mathbb{Z}$.

Remarque 31 — *Si P est non-nul, pour Q un diviseur de P on a $\deg(Q) \leq \deg(P)$. En effet la relation $P = R.Q$ donne $\deg(P) = \deg(RQ) = \deg(R) + \deg(Q)$.*
Et comme P est non-nul, on a $R \neq 0$, donc $\deg(R) \geq 0$, ce qui donne $\deg(Q) = \deg(P) - \deg(R) \leq \deg(P)$.
Les polynômes qui divisent P ont un degré compris entre 0 et $\deg(P)$.

Exemple 32 — *Soit $P \in \mathbb{K}[X]$ non-nul. Pour tout $\lambda \in \mathbb{K}$ non-nul, on a $P = \lambda.(\frac{1}{\lambda}P)$.*
Autrement dit, tous les polynômes constants non-nuls (ceux de degré 0) sont des diviseurs de P, et tous les polynômes de la forme γP (les multiples de P par un scalaire non-nul) sont des diviseurs de P.

Maintenant, soit Q de même degré que P tel que $Q \mid P$. On a donc $R \in \mathbb{K}[X]$ tel que $P = R.Q$.
En regardant les degrés, on obtient $\deg(P) = \deg(RQ) = \deg(R)+\deg(Q)$. Comme $\deg(Q) = \deg(P)$, cela donne $\deg(R) = 0$.
Ainsi, on a $R(X) = \lambda$ pour une certaine constante $\lambda \in \mathbb{K}^*$. Cela implique donc que $Q(X) = \frac{1}{\lambda}P(X)$.
En conclusion, les diviseurs de P qui sont de même degré sont uniquement les multiples de P par une constante.

L'arithmétique sur l'ensemble des polynômes $\mathbb{K}[X]$ est très similaire à l'arithmétique sur l'ensemble des entiers $\mathbb{Z}$. Cela est dû au théorème suivant.

2.2 Division euclidienne de polynômes

Théorème 33 (Division euclidienne de polynômes)
Soient A et $B \in \mathbb{K}[X]$ avec $B \neq 0$.
Alors, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$A = QB + R \qquad \text{avec} \qquad \deg R < \deg B.$$

Preuve — L'unicité se montre comme pour la division euclidienne d'entiers : on suppose qu'il existe deux couples possibles, et on montre qu'ils sont égaux.
Existence : Le cas $B = \lambda \in \mathbb{K}^*$ ($\deg B = 0$) est immédiat avec $(Q, R) = (\lambda^{-1}A, 0)$. Supposons B non constant.
On procède par récurrence sur $\deg(A)$. On remarque d'une part que si $\deg(A) < \deg(B)$, alors $(Q, R) = (0, A)$.
D'autre part, si $\deg A \geq \deg B$, en écrivant :

$$A = a_n X^n + \ldots + a_0,\ B = b_m X^m + \ldots + b_0,\ \text{avec } a_n b_m \neq 0,$$

on remarque que le polynôme $A - \dfrac{a_n}{b_m} X^{n-m} B$ est de degré strictement inférieur à $\deg(A)$, ce qui permet d'appliquer l'hypothèse de récurrence à ce dernier. □

Remarque 34 — *Soient $A, B \in \mathbb{K}[X]$ avec B non-nul. On a $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.*

Exemple 35 (Algorithme de la division euclidienne) —
On effectue une division euclidienne de polynômes en faisant descendre le degré du polynôme à diviser. Voici en exemple la division euclidienne de $A = X^5 + 4X^4 + 2X^3 + X^2 - X - 1$ par $B = X^3 - 2X + 3$:

$$\begin{array}{rrrrrr|l} X^5 & +4X^4 & +2X^3 & +X^2 & -X & -1 & X^3-2X+3 \\ \cline{7-7} & 4X^4 & +4X^3 & -2X^2 & -X & -1 & X^2+4X+4 \\ & & 4X^3 & +6X^2 & -13X & -1 & \\ & & & 6X^2 & -5X & -13 & \end{array}$$

On trouve finalement $X^5+4X^4+2X^3+X^2-X-1=(X^3-2X+3)(X^2+4X+4)+(6X^2-5X-13)$.

3 Polynômes irréductibles, décomposition en facteurs irréductibles

Définition 36
Soit $P \in \mathbb{K}[X]$. On dit que P est un **polynôme irréductible sur** $\mathbb{K}$ si $deg(P) \geq 1$ et P n'est divible que par lui-même (à un multiple dans $\mathbb{K}$ près) ou par les polynômes constants.

Un polynôme irréductible sur $\mathbb{K}$ est donc un polynôme dont les diviseurs sont, au multiple dans $\mathbb{K}$ près, 1 et lui-même. Tout comme un nombre premier est un entier dont les diviseurs sont, au signe près, 1 et lui-même.

Exemple 37 —

1. X^2+1 *irréductible sur* $\mathbb{R}$ *(écrire la division de* X^2+1 *par* $X+a$ *et aboutir à une contradiction), mais n'est pas irréductible sur* $\mathbb{C}$: $X^2+1=(X+i)(X-i)$.
2. *Les polynômes de degré* 1, $P(X)=aX+b$, *sont toujours irréductibles (quelque soit le corps* $\mathbb{K}$*).*
3. X^2-2 *est un polynôme irréductible sur* $\mathbb{Q}$, *mais n'est pas irréductible sur* $\mathbb{R}$ *car* $X^2-2=(X+\sqrt{2})(X-\sqrt{2})$.

Exemple 38 — *Dans* $\mathbb{R}[X]$ *et* $\mathbb{Q}[X]$, *le polynôme* X^3-1 *se factorise en* $X^3-1=(X-1)(X^2+X+1)$. *Mais dans* $\mathbb{C}[X]$, *il se factorise en* $X^3-1=(X-1)(X-j)(X-j^2)$.

Exemple 39 — *Les diviseurs unitaires de* $X^3-5X+6=(X-2)(X-3)$ *sont les suivants :* 1, $X-2$, $X-3$, $(X-2)(X-3)$.

4 Racines d'un polynôme

Définition 40 (**Racine d'un polynôme**)
Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.
On dit que α est une **racine** du polynôme P si l'on a $P(\alpha)=f_P(\alpha)=0$.

Proposition 41 (**Lien entre racines et factorisation**)
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
Alors, a est une racine de P si et seulement si $(X-a)|P(X)$.

Preuve — On écrit la division euclidienne de $P(X)$ par $(X-a)$: $P(X)=(X-a)Q(X)+R(X)$ avec $\deg(R)<\deg(X-A)=1$. $R(X)$ est donc un polynôme constant : $R(X)=\lambda$. L'évaluation en a donne $P(a)=0.Q(a)+R(a)=\lambda$. Ainsi, a est une racine de P si et seulement si $R(X)=0$, si et seulement si $(X-a)$ divise $P(X)$. $\square$

4.1 Multiplicité d'une racine, polynômes scindés

Définition 42
Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, et $k \geq 1$.
On dit que a est une **racine de multiplicité** k de P si l'on a $(X-a)^k|P$ et $(X-a)^{k+1} \nmid P$.
Une racine de multiplicité 1 est appelée **racine simple** de P.

Proposition 43
Soient $P \in \mathbb{K}[X]$ et $a_1,\ldots,a_r \in \mathbb{K}$, tels que $a_1,\ldots,a_r$ sont des racines de P de multiplicités

respectives α_1, ...,α_r. Alors il existe $Q \in \mathbb{K}[X]$ tel que :

$$P(X) = (X - a_1)^{\alpha_1} \dots (X - a_r)^{\alpha_r} Q(X) \quad \text{avec} \quad , \forall 1 \leq i \leq r,\, Q(a_i) \neq 0.$$

Démonstration —Admis.

Définition 44
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est **de multiplicité** 0 pour P si l'on a $(X-\alpha)^0|P$ et $(X-a)^1 \not| P$.
Les nombres de multiplicité 0 sont tous les nombres qui ne sont pas des racines de P.

Corollaire 45
Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ de degré $n \geq 0$.
• Alors P possède au plus n racines, comptées avec leur multiplicité.
• Soit $Q \in \mathbb{K}[X]$ avec $\deg(Q) \leq n$, et tel que Q possède $n+1$ racines ou plus.
Alors, Q est le polynôme nul.

Preuve — Dans la proposition précédente, on a $\deg(P) = n = a_1 + \ldots + a_r + \deg(Q)$. D'où $a_1 + \ldots + a_r \leq n$. □

Définition 46 (**Polynôme scindé**)
Soit $P \in \mathbb{K}[X]$ non-nul.
On dit que P est **scindé** s'il admet autant de racines (comptées avec multiplicité) que son degré.
Il est équivalent de dire que $P(X) = a_n \prod_{i=1}^{r} (X - z_i)^{\alpha_i}$, pour des $z_1, \ldots, z_r \in \mathbb{K}$.
On dit que P est **scindé à racines simples** si le polynôme P est scindé et si toutes ses racines sont distinctes.
Il est équivalent de dire que $P(X) = a_n \prod_{i=1}^{n} (X - z_i)$, pour des $z_1, \ldots, z_n \in \mathbb{K}$ distincts.

Exemple 47 — *Le polynôme $X^n - 1$ admet n racines dans $\mathbb{C}$, qui sont les racines n-ièmes de l'unité. Donc, ce polynôme est scindé à racines simples.*

Remarque 48 — *Nous verrons que les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1, et que les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux 1 et ceux de degré 2 de discriminant strictement négatif (c'est-à-dire sans racines réelles). Cela est lié aux propriétés de $\mathbb{R}$ et de $\mathbb{C}$ en analyse.*

5 Dérivation dans $\mathbb{K}[X]$

5.1 Dérivée d'un polynôme

Définition 49
Soit $P \in \mathbb{K}[X]$ avec $P = a_n X^n + \ldots + a_0$.
On définit le **polynôme dérivé** de P, noté P', le polynôme :

$$P'(X) = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + a_1.$$

Remarque 50 — *Pour $n \geq 1$ et $a_n \neq 0$, le coefficient na_n est non-nul.*

Proposition 51
Soit $P \in \mathbb{K}[X]$. On a $\deg(P') = \deg(P) - 1$ si $\deg(P) \geq 1$, et $P'(X) = 0$ sinon.

Proposition 52 (**Application linéaire de dérivation**)
La fonction $D : P \in \mathbb{K}[X] \mapsto P' \in \mathbb{K}[X]$ est une application linéaire.
De plus, $\mathrm{Ker}(D) = \{\lambda,\, \lambda \in \mathbb{K}\}$ est l'ensemble des polynômes constants. ($P'(X) = 0 \Leftrightarrow P(X) = a_0$)

Démonstration —A faire après le chapitre Applications linéaires.

Proposition 53 (Formules de dérivation)
Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$, $m \geq 1$. On a :

1. $(\lambda P)'(X) = \lambda P'(X)$;
2. $(P+Q)'(X) = P'(X) + Q'(X)$ (dérivée d'une somme) ;

3. $(PQ)'(X) = P'(X)Q(X) + P(X)Q'(X)$ (dérivée d'un produit) ;
4. $(P^m)'(X) = mP'(X)P(X)^{m-1}$ (dérivée d'une puissance) ;
5. $(P \circ Q)'(X) = Q'(X).(P' \circ Q)(X)$ (dérivée d'une composée).

Proposition 54 (**Polynôme dérivé et fonction polynômiale, sur** $\mathbb{R}$)
Soient $\mathbb{K} = \mathbb{R}$ et $P \in \mathbb{R}[X]$. Soient $f_P : x \mapsto P(x)$ et $f_{P'} : x \mapsto P'(x)$ les fonctions polynômiales associées à P et P'.
Alors on a $f_{P'} = (f_P)'$.

Remarque 55 — *Dans le cadre des fonctions, la notion de dérivée a un sens sur $\mathbb{R}$. Ainsi, on peut identifier la dérivée d'un polynôme réel à la dérivée de sa fonction polynômiale associée. Pour tout corps $\mathbb{K}$, l'opération de dérivation des polynômes de $\mathbb{K}[X]$ est bien définie.*
Mais pour un corps comme $\mathbb{C}$, dériver une fonction $f : \mathbb{C} \to \mathbb{C}$ n'a pas de sens pour le moment. Il ne faudra donc pas confondre en général polynôme dérivé (qui existe) et dérivée de la fonction polynômiale (qui n'existe pas forcément).

5.2 Formule de Taylor

Proposition 56 (**Dérivées de** $(X-a)^n$)
Soient $\alpha \in \mathbb{K}$, $n \geq 1$, $k \geq 0$. On pose $P(X) = (X-\alpha)^n$.
En notant $P^{(k)}$ le polynôme dérivé k-ième de P, on a :

$$P^{(k)}(X) = \frac{n!}{(n-k)!}(X-\alpha)^{n-k} \text{ si } 0 \leq k \leq n$$
$$P^{(k)}(X) = 0 \text{ si } k > n.$$

On en déduit que $P^{(n)}(X) = n!$, et que $P^{(k)}(\alpha) = 0$ si $k \neq n$.

Preuve — On démontre le résultat par récurrence sur k. □

Théorème 57 (**Formule de Taylor pour les polynômes**)
Soient $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$ de degré n. On a l'égalité suivante :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = P(a) + \frac{P'(a)}{1!}(X-a) + \ldots + \frac{P^{(n)}(a)}{n!}(X-a)^n.$$

Démonstration —Admis.

Remarque 58 — *Si l'on choisit $a = 0$, on obtient la relation $P(X) = P(0) + P'(0)X + \ldots + \frac{P^{(n)}(0)}{n!}X^n$. Ainsi, dans l'écriture $P(X) = a_0 + a_1X + \ldots + a_nX^n$, les coefficients a_k de P sont associés aux dérivées successives de P, par la relation $a_k = \frac{P^{(k)}(0)}{k!}$.*

Exemple 59 — *On a $X^2 - 10X + 1 = 1 + \frac{10}{1}(X-10) + \frac{2}{2}(X-10)^2 = 1 + 10(X-10) + (X-10)^2$. Appliquer la formule de Taylor à :*

1. *$X^3 + X^2 + X + 1$ et $\alpha = 1$;*
2. *$2X^4 + 2X + 1$ et $\alpha = -1$.*

La formule de Taylor correspond à un changement de variables pour les polynômes. Au lieu d'écrire P comme une combinaison linéaire de $1, X, X^2, \ldots, X^n$, on l'écrit comme une combinaison linéaire de $1, (X-a), (X-a)^2, \ldots, (X-a)^n$. Par rapport à ces nouvelles variables, les coefficients de P changent, et la formule de Taylor fournit une expression très pratique de ces coefficients.

5.3 Caractérisation des racines multiples

Proposition 60 (**Caractérisation des racines simples**)
Soient $\mathbb{K}$ un corps, $a \in \mathbb{K}$, et $P \in \mathbb{K}[X]$.
L'élément a est une racine simple du polynôme P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.

Preuve — Si P admet une racine b de multiplicité $k \geq 1$, on a alors $P(X) = (X-b)^k.Q(X)$, avec $Q(b) \neq 0$. En dérivant, on obtient : $P'(X) = (X-b)^k Q'(X) + k(X-b)^{k-1}Q(X)$.

Supposons que a est une racine simple de P. On a donc $P(a) = 0$ et $P'(X) = (X-a)Q'(X) + 1.Q(X)$. Cela donne $P'(a) = 0 + Q(a) \neq 0$.

Réciproquement, supposons que $P(a) = 0$ et $P'(a) \neq 0$. Alors a est une racine de P. Soit k la multiplicité de a. Si $k > 1$, alors le polynôme $(X-a)^{k-1}$ s'annule en a, et on obtient : $P'(a) = (a-a)Q'(a) + k(a-a)^{k-1}Q(a) = 0$. Comme on a $P'(a) \neq 0$, a est donc de multiplicité 1. □

Proposition 61 (**Caractérisation des racines multiples**)
Soient $a \in \mathbb{K}$, $k \geq 1$, et $P \in \mathbb{K}[X]$.
Alors a est une racine de P de multiplicité k si et seulement si $P(a)$, $P'(a)$,...,$P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Preuve — C'est une conséquence immédiate de la formule de Taylor. En écrivant

$$P = P(a) + \frac{P'(a)}{1!}(X-a) + \ldots + \frac{P^{(i)}}{n!}(X-a)^i + \ldots + \frac{P^{(n)}}{n!}(X-a)^n,$$

on peut remarquer que $P(X)$ est un multiple de $(X-a)^k$ mais pas de $(X-a)^{k+1}$ si et seulement si $P(a)$,$P'(a), \ldots, P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$. □

Exemple 62 — *Dans $\mathbb{C}[X]$, pour $\omega \neq 0$, le polynôme $P(X) = X^n - \omega$ n'admet que des racines simples. En effet, son polynôme dérivé est $P'(X) = nX^{n-1}$. Le polynôme P' a 0 comme sele racine (de multiplicité $n-1$), alors que $P(0) = -\omega \neq 0$. Comme P et P' n'ont pas de racines communes, cela veut dire quand $P(a) = 0$ on a $P'(a) \neq 0$.*

5.4 Théorème de Rolle pour les polynômes réels

On rappelle les deux résultats d'analyse suivants, qui sont utiles pour étudier les polynômes à coefficients réels.

Proposition 63 (**Théorème des valeurs intermédiaires**)
Soit $I = [a,b]$ un intervalle de $\mathbb{R}$. Soit $f : [a,b] \to \mathbb{R}$ une fonction continue sur $[a,b]$.
• Si $f(a) \neq f(b)$, pour tout $d \in]f(a), f(b)[$, il existe $c \in]a,b[$ tel que $f(c) = d$.
• Si $f(a) < 0$ et $f(b) > 0$ (ou $f(a) > 0$ et $f(b) < 0$), alors il existe $c \in]a,b[$ tel que $f(c) = 0$.

Proposition 64 (**Théorème de Rolle**)
Soit $I = [a,b]$ un intervalle de $\mathbb{R}$. Soit $f : [a,b] \to \mathbb{R}$ une fonction continue sur $[a,b]$ et dérivable sur $]a,b[$.
Si $f(a) = f(b)$, alors il existe $c \in]a,b[$ tel que $f'(c) = 0$.

Corollaire 65
Soit $P \in \mathbb{R}[X]$.
• Soient a, b deux racines de P distinctes.
Alors il existe $c \in]a,b[$ tel que $P'(c) = 0$ (c est une racine de P).
• Si P possède r racines distinctes $a_1 < a_2 < \ldots < a_r$, alors le polynôme P' possède au moins $r-1$ racines $b_1, \ldots, b_{r-1}$ telles que $b_i \in]a_i, a_{i+1}[$.
P' possède donc au moins $r-1$ racines distinctes qui ne sont pas des racines de P.

Preuve — On utilise le théorème de Rolle à P sur chaque intervalle $[a_i, a_{i+1}]$. □

Remarque 66 — *Pour $P \in \mathbb{R}[X]$, le théorème de Rolle permet de trouver des racines de P'.
Il ne dit pas comment calculer la valeur des racines $b_1, \ldots, b_{r-1}$, mais on a des informations sur le nombre de racines distinctes de P' et sur leur position.
Cela est très important dans l'étude des polynômes réels/complexes comme fonctions, pour savoir sur quels intervalles le polynôme prend des valeurs positives/négatives/nulles.*

Corollaire 67 (**Polynômes réels scindés et dérivée**)
Soit $P \in \mathbb{R}[X]$ un polynôme scindé.
Alors P' est scindé.
De plus, si P est scindé à racines simples alors P' est scindé à racines simples.

5.5 Racines complexes conjuguées de polynômes réels

Lemme 68
Soit $P \in \mathbb{R}[X]$. Soit $\alpha \in \mathbb{C}$.
On a alors $P(\overline{\alpha}) = \overline{P(\alpha)}$.

Preuve — On écrit $P = a_n X^n + \ldots + a_0$ avec $a_i \in \mathbb{R}$. Alors, on a :

$$P(\bar{\alpha}) = a_n \bar{\alpha}^n + \ldots + a_1 \bar{\alpha} + a_0 = \overline{a_n \alpha^n + \ldots + a_1 \alpha + a_0} = \overline{P(\alpha)}.$$

□

Proposition 69
Soit $P \in \mathbb{R}[X]$. Soit $w \in \mathbb{C}$. Soit $k \in \mathbb{N}^*$.
Alors w est une racine complexe de P de multiplicité k ssi $\overline{w}$ est une racine de P de multiplicité k.

Preuve — Soit $k \in \mathbb{N}^*$. Avec le lemme précédent, on a $P(w) = 0, P'(w) = 0, \ldots, P^{(k-1)}(w) = 0, P^{(k)}(w) \neq 0$ ssi $\overline{P(w)} = 0, \overline{P'(w)} = 0, \ldots, \overline{P^{(k-1)}(w)} = 0, \overline{P^{(k)}(w)} \neq 0$ ssi $P(\overline{w}) = 0, P'(\overline{w}) = 0, \ldots, P^{(k-1)}(\overline{w}) = 0, P^{(k)}(\overline{w}) \neq 0$, car chaque polynôme $P, P', \ldots, P^{(k)}$ est à coefficients réels. □

5.6 Racines d'un polynôme et de son polynôme dérivé

Proposition 70
Soit $P \in \mathbb{R}[X]$. Si a est une racine de P de multiplicité k ($k \geq 1$), alors a est aussi une racine de P' de multiplicité $k-1$.

Preuve — On a $P(X) = (X-a)^k.Q(X)$ avec $Q(a) \neq 0$. Alors, $P'(X) = k(X-a)^{k-1}Q(X) + (X-a)^k Q'(X) = (X-a)^{k-1}(kQ(X) + (X-a)Q'(X))$.
On obtient ainsi $(X-a)^{k-1} \mid P'(X)$ et $kQ(a) + (a-a)Q'(a) = kQ(a) + 0 = kQ(a) \neq 0$, donc a est une racine de P' de multiplicité $k-1$. □

Remarque 71 — *Si a est une racine de P de multiplicité 1, alors a est de multiplicité 0 pour P' (c'est-à-dire que $(X-a)^1 \not| P'$, que a n'est pas une racine de P').*
Par exemple, pour $P(X) = (X-1)(X-2)$, on a $P'(X) = 2X - 3 = 2(X - \frac{3}{2})$.
Ainsi, toutes les racines multiples de P sont des racines de P', et toutes les racines simples de P ne sont pas des racines de P'.
Si l'on connaît beaucoup de racines de P, on connaît ainsi beaucoup de racines de P' (mais pas toutes).
On ne peut par contre rien dire sur P' si a n'est pas une racine de P.
Par exemple, pour $P(X) = (X-2)^{30} + 1$, 2 n'est pas une racine de P mais 2 est une racine de P' de multiplicité 29.

6 Décomposition en produit de polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

6.1 Factorisation dans $\mathbb{C}[X]$

Théorème 72 (**Théorème de D'alembert-Gauss**)
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Démonstration —Ce théorème, bien que très fondamental, est admis.

Corollaire 73 (**Racines complexes d'un polynôme**)
Soit $P \in \mathbb{C}[X]$ un polynôme de degré n, avec $n \in \mathbb{N}^*$. Alors P possède exactement n racines, comptées avec multiplicité.

Corollaire 74 (**Polynômes irréductibles dans $\mathbb{C}$**)
Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Corollaire 75 (**Factorisation en produit de facteurs irréductibles dans $\mathbb{C}$**)
Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. Alors P se décompose en :

$$P = a_n \prod_{i=1}^{r} (X - z_i)^{\alpha_i},$$

où $\alpha_1, \dots, \alpha_r$ sont des entiers non nuls et $z_1, \dots, z_r$ sont des nombres complexes deux à deux distincts.
Cette décomposition est unique à l'ordre des z_i près.

Remarque 76 — *On peut aussi formuler le corollaire en disant que tout polynôme $P \in \mathbb{C}[X]$ se décompose en un produit de polynômes de degré 1.*

6.2 Factorisation dans $\mathbb{R}[X]$

La situation dans $\mathbb{R}$ est relativement différente.

Proposition 77 (**Polynômes irréductibles dans $\mathbb{R}$**)
Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

1. Les polynômes de degré 1, $\lambda(X - \beta)$, avec $\lambda \neq 0$;
2. Les polynômes de degré 2, $aX^2 + bX + c$, avec $b^2 - 4ac < 0$.

Exemple 78 —

1. *Le polynôme $X^3 + 1$ n'est pas irréductible dans $\mathbb{R}[X]$ car -1 est une racine. Il se décompose en $X^3 + 1 = (X + 1)(X^2 - X + 1)$.*
2. *$X^4 + 1$ n'a pas de racines sur $\mathbb{R}$ mais n'est pas irréductible. Sa décomposition est :*

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

3. *Tout polynôme réel P de degré impair admet au moins une racine réelle. (Pourquoi ?)*

Corollaire 79 (**Factorisation en produit de facteurs irréductibles dans $\mathbb{R}$**)
Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$. Alors P se décompose en :

$$P = a_n \prod_{i=1}^{r} (X - c_i)^{\alpha_i} \times \prod_{j=1}^{m} (X^2 + c_j X + d_j)^{\beta_j},$$

où $\alpha_1, \dots, \alpha_r, \beta_i, \dots, \beta_m$ sont des entiers non nuls, les b_i sont distincts, les (c_j, d_j) sont distincts, avec $c_j^2 - 4d_j < 0$.
Cette décomposition est unique à l'ordre l'ordre des b_i et des (c_j, d_j) près.

Autrement dit, tout polynôme de $\mathbb{R}[X]$ s'écrit comme un produit de polynômes de degré 1 et de polynômes de degré 2 à discriminant strictement négatif.

Remarque 80 (**Factorisation dans $\mathbb{Q}$?**) — *La situation est infiniment plus délicate dans $\mathbb{Q}[X]$.
Par exemple, pour $P(X) = X^4 + 1$, les racines complexes de P sont $\exp(\frac{i\pi}{4})$,$\exp(\frac{3i\pi}{4})$,$\exp(\frac{5i\pi}{4})$, et $\exp(\frac{7i\pi}{4})$.
Ce polynôme est réductible dans $\mathbb{R}[X]$ car*

$$X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

*Les polynômes de droite sont de discriminant -1, et sont donc irréductibles.
Si P était réductible dans $\mathbb{Q}[X]$, on aurait $P = QR$, avec $Q, R \in \mathbb{Q}[X]$ non-constants. On aurait donc $P = QR$ dans $\mathbb{R}[X]$, donc $Q(X) = X^2 \pm \sqrt{2}X + 1$. Mais $\sqrt{2}$ est irrationnel, donc un tel polynôme n'est pas à coefficients rationnels. Ainsi, P est irréductible dans $\mathbb{Q}[X]$.*

En fait, l'ensemble $\mathbb{Q}[X]$ possède des polynômes irréductible de n'importe quel degré n.

7 Relations entre coefficients et racines

Avec la factorisation, on a deux façons d'écrire un polynôme P. Soit $P(X) = a_nX^n + \ldots + a_0$, soit $P(X) = \Pi_i P_i(X)$.
Il existe un lien fort entre ces deux écritures.

Proposition 81
Soit $P \in \mathbb{K}[X]$ un polynôme de degré n qui est scindé. Soient $\alpha_1, \ldots, \alpha_n$ les racines de P, comptées avec multiplicité. Pour $P(X) = a_nX^n + \ldots + a_0$ et $P(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$, on a :

$$\alpha_1 + \ldots + \alpha_n = -\frac{a_{n-1}}{a_n}.$$

$$\alpha_1 \times \ldots \times \alpha_n = (-1)^n \frac{a_0}{a_n}.$$

Preuve — Il faut développer le produit $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$ et identifier les coefficients devant X^{n-1} et devant X^0 pour obtenir ces relations. □

Exemple 82 — *Dans le cas de polynômes unitaires ($a_n = 1$), pour le degré 2 et 3, on obtient les relations suivantes.*

1. *Soit $P = X^2 + aX + b = (X - \alpha_1)(X - \alpha_2)$. Alors on a :* $\begin{cases} \alpha_1 + \alpha_2 = -a \\ \alpha_1\alpha_2 = b \end{cases}$
2. *Soit $P = X^3 + a_2X^2 + a_1X + a_0 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$. Alors on a :*
   (a) $\alpha_1 + \alpha_2 + \alpha_3 = -a_2$;
   (b) $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = a_1$;
   (c) $\alpha_1\alpha_2\alpha_3 = -a_0$.

Remarque 83 (Détermination des racines d'un polynôme) — *Soit $P \in \mathbb{K}[X]$.*

• ***Degré 1*** *: On a $P(X) = \lambda(X - \alpha)$ et il n'y a rien à étudier.*

• ***Degré 2*** *: On a $P(X) = aX^2 + bX + c$. Le discriminant $\Delta = b^2 - 4ac$ permet de dire si P possède ou non des racines dans le corps $\mathbb{K}$, et de donner l'expression de ces racines en fonction de a, b, c. Ces expressions utilisent $+, \times, -, \frac{1}{\cdot}$ et $\sqrt{\cdot}$.*

• ***Degré 3*** *: Il existe des formules appelées formules de Cardan qui permettent de dire si P possède ou non des racines dans le corps $\mathbb{K}$, et de donner l'expression de ces racines en fonction des coefficients $a_0, \ldots, a_3$. Ces expressions utilisent $+, \times, -, \frac{1}{\cdot}$, $\sqrt{\cdot}$ et $\sqrt[3]{\cdot}$, et sont un peu lourdes.*

• ***Degré 4*** *: Il existe des formules appelées formules de Cardan qui permettent de dire si P possède ou non des racines dans le corps $\mathbb{K}$, et de donner l'expression de ces racines en fonction des coefficients $a_0, \ldots, a_4$. Ces expressions utilisent $+, \times, -, \frac{1}{\cdot}$, $\sqrt{\cdot}$, $\sqrt[3]{\cdot}$ et $\sqrt[4]{\cdot}$, et sont très lourdes.*

• ***Degré 5*** *: Il n'existe aucune formule générale utilisant $+, \times, -, \frac{1}{\cdot}$, et $\sqrt[n]{\cdot}$ $\forall n \geq 2$, qui permet de dire si P possède des racines dans le corps $\mathbb{K}$, ni d'exprimer les racines de P en fonction des coefficients $a_0, \ldots, a_5$.*
Autrement dit, il existe des polynômes P de degré 5 dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ tels que leurs racines ne sont égales à aucune expression algébrique utilisant les opérations $+, \times, -, \frac{1}{\cdot}$, et $\sqrt[n]{\cdot}$ $\forall n \geq 2$ et les coefficients $a_0, \ldots, a_5$. Cela est par exemple le cas pour $P(X) = X^5 - 6X + 3$.
On peut estimer les racines de ce polynôme dans $\mathbb{R}$ ou $\mathbb{C}$ à l'aide d'algorithmes (trouver les lieux où $P(x)$ est aussi proche de 0 que l'on veut), mais cela est moins efficace que de calculer des valeurs approchées de sommes/produits/quotients de racines n-èmes de nombres rationnels.

- Ainsi, si l'on vous demande de déterminer les racines d'un polynôme P de degré 3 ou plus, vous aurez forcément des racines évidentes, des relations algébriques, ou des propriétés supplémentaires pour déterminer des racines de P et vous ramener à un polynôme de degré 2 ou 1.

7.1 Résolution de systèmes à deux inconnues

Proposition 84
Soient $a, b \in \mathbb{K}$. Les solutions du système $\begin{cases} x+y &= a \\ xy &= b \end{cases}$ sont exactement les couples (α_1, α_2) tels que α_1 et α_2 sont les deux racines, si elles existent (éventuellement racines doubles), du polynôme $X^2 - aX + b = 0$.

Preuve — En effet (α_1, α_2) est solution du système ssi

$$(X-\alpha_1)(X-\alpha_2) = X^2 - (\alpha_1+\alpha_2)X + \alpha_1\alpha_2 = X^2 - aX + b = 0.$$

□

Exemple 85 — *On veut résoudre le système* $\begin{cases} x+y &= -3 \\ xy &= 2 \end{cases}$

Un couple $(x, y) = (\alpha_1, \alpha_2)$ est solution du système si et seulement si α_1 et α_2 sont racines du polynôme $X^2 + 3X + 1$. Or, les racines de ce polynômes sont -1 et -2, donc l'ensemble des couples solutions est $\{(-1, -2), (-2, -1)\}$.

8 Décomposition en éléments simples

Les polynômes étant analogues du point de vue algébrique aux nombres entiers relatifs, l'analogue des nombres rationnels sont les fractions rationnelles (des quotients de polynômes). Plutôt que de construire formellement un quotient de polynômes, nous allons considérer le point de vue des fonctions.

Définition 86 (**Fonction rationnelle**)
Soit $f : D_f \to \mathbb{R}$ une fonction d'une variable réelle. On dit que f est une **fonction rationelle** s'il existe deux polynômes P et Q dans $\mathbb{R}[X]$ tel que pour tout $x \in D_f$ on a $f(x) = \frac{P(x)}{Q(x)}$.

Les fonctions rationnelles sont exactement les quotients de fonctions polynômiales. Elles peuvent être définies sur $\mathbb{R}$ tout entier, privé des racines de Q.

Exemple 87 — $x \mapsto \frac{1}{x}$, $x \mapsto \frac{1}{x(x+1)}$, $x \mapsto \frac{1-x^2}{1+x^2}$ *sont des fonctions rationnelles.*

Proposition 88
Soient f, g deux fonctions rationnelles, et $\lambda \in \mathbb{R}$. Alors $f+g$, $f.g$, λf sont des fonctions rationnelles.

Exemple 89 — *On a* $(x \mapsto \frac{1}{x-1}) + (x \mapsto \frac{1}{x+1}) = x \mapsto \frac{x+1+(x-1)}{(x-1)(x+1)} = x \mapsto \frac{2x}{x^2-1}$.
Pour $x \in \mathbb{R}$ différent de 0 et de -1 on a $\frac{1}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1}$, *donc* $(x \mapsto \frac{1}{x}) - (x \mapsto \frac{1}{x+1}) = x \mapsto \frac{1}{x(x+1)}$.

Théorème 90 (**Décomposition en éléments simples**)
Soient $(P, Q) \in \mathbb{R}[X]^2$ avec $Q \neq 0$, et $f : x \mapsto \frac{P(x)}{Q(x)}$.
On pose $Q(X) = \lambda \prod_{i=1}^{r} (X - a_i)^{\alpha_i} \prod_{j=1}^{s} (X^2 + b_j X + c_j)^{\beta_j}$ la décomposition de Q en produit de polynômes irréductibles dans $\mathbb{R}[X]$.
Alors, il existe $R \in \mathbb{R}[X]$, $e_{i,k} \in \mathbb{R}$ pour $(i, k) \in \mathbb{N}^2$ avec $1 \leq i \leq r$ et $1 \leq k \leq \alpha_i$, $(f_{j,k}, g_{j,k}) \in \mathbb{R}^2$ pour $(j, k) \in \mathbb{N}^2$ avec $1 \leq j \leq s$ et $1 \leq k \leq \beta_j$, tels que :

$$\forall x \in D_f,\ f(x) = R(x) + \sum_{i=1}^{r} \sum_{k=1}^{\alpha_i} \frac{e_{i,k}}{(x - a_i)^k} + \sum_{j=1}^{s} \sum_{k=1}^{\beta_j} \frac{f_{j,k} x + g_{j,k}}{(x^2 + b_j x + c_j)^k}.$$

De plus, cette décomposition est unique.

Corollaire 91 (**Cas Q à racines simples**)
Soient $(P, Q) \in \mathbb{R}[X]^2$ avec $Q \neq 0$, à racines simples, et $f : x \mapsto \frac{P(x)}{Q(x)}$.
On pose $Q(X) = \lambda \prod_{i=1}^{r} (X - a_i) \prod_{j=1}^{s} (X^2 + b_j X + c_j)$ la décomposition de Q en produit de polynômes

irréductibles dans $\mathbb{R}[X]$.
Alors, il existe $R \in \mathbb{R}[X]$, $e_i \in \mathbb{R}$ pour $1 \leq i \leq r$, et $(f_j, g_j) \in \mathbb{R}^2$ pour $1 \leq j \leq s$, tels que :

$$\forall x \in D_f,\ f(x) = R(x) + \sum_{i=1}^{r} \frac{e_i}{x - a_i} + \sum_{j=1}^{s} \frac{f_j x + g_j}{x^2 + b_j x + c_j}.$$

De plus, cette décomposition est unique.

EXEMPLE 92 — *L'égalité* $\frac{1}{x(x+1)} = \frac{1}{x} + \frac{-1}{x+1}$ *correspond à la décomposition en éléments simples de* $x \mapsto \frac{1}{x(x+1)}$.
De même, l'égalité $\frac{x+3}{x-1} = \frac{x-1+1+3}{x-1} = 1 + \frac{4}{x-1}$ *correspond à la décomposition en éléments simples de* $x \mapsto \frac{x+3}{x-1}$.

REMARQUE 93 — *La forme générale de la décomposition en éléments simples est "lourde", mais dès que le polynôme Q possède peu de racines ou que ses racines sont simples, le nombre de termes n'est pas très élevé.*
Le nombre de coefficients $e_{i,k}, f_{j,k}, g_{j,k}$ *est égal à* $\alpha_1 + \alpha_2 + \ldots + \alpha_r + 2\beta_1 + \ldots + 2\beta_s = \deg(Q)$.
En général Q est de degré petit $(2, 3, 4)$, il n'y a donc que peu de coefficients à déterminer.
Et, le polynôme R est le quotient dans la division euclidienne de P par Q.
On peut donc le déterminer séparément en effectuant une division euclidienne.
Si $\deg(P) < \deg(Q)$, *alors on a automatiquement* $R = 0$.

REMARQUE 94 — *Pour* $f(x) = R(x) + \sum_{i=1}^{r} \sum_{k=1}^{\alpha_i} \frac{e_{i,k}}{(x-a_i)^k} + \sum_{j=1}^{s} \sum_{k=1}^{\beta_j} \frac{f_{j,k}x+g_{j,k}}{(x^2+b_jx+c_j)^k}$, *on peut déterminer certains coefficients par un calcul de limite.*
En effet, $(x - a_i)^{\alpha_i} f(x)$ *s'écrit comme une somme de fractions polynômiales dont tous les termes sont multiples de* $(x - a_i)$ *au numérateur, excepté un terme qui est constant et vaut* e_{i,α_i}.
Ainsi, on a $\lim_{x\to a_i}((x - a_i)^{\alpha_i} f(x)) = e_{i,\alpha_i}$.
De la même façon, en notant z_j et $\overline{z_j}$ les racines complexes conjuguées de $X^2 + b_j X + c_j$, on a dans $\mathbb{C}$: $\lim_{z\to z_j}((z^2+zb_j+c_j)^{\beta_j} f(z)) = z_j.f_{j,\beta_j}+g_{j,\beta_j}$ *et* $\lim_{z\to \overline{z_j}}((z^2+zb_j+c_j)^{\beta_j} f(z)) = \overline{z_j}.f_{j,\beta_j}+g_{j,\beta_j}$.
Cela permet de déterminer la paire $(f_{j,\beta_j}, g_{j,\beta_j})$.

REMARQUE 95 — *Considérons le cas où* $R(x) = 0$, *c'est-à-dire où* $f(x) = \sum_{i=1}^{r} \sum_{k=1}^{\alpha_i} \frac{e_{i,k}}{(x-a_i)^k} + \sum_{j=1}^{s} \sum_{k=1}^{\beta_j} \frac{f_{j,k}x+g_{j,k}}{(x^2+b_jx+c_j)^k}$.
On peut alors obtenir une somme de coefficients avec un calcul de limite.
En effet, $xf(x)$ s'écrit comme une somme de fractions polynômiales dont tous les numérateurs sont de degré inférieur ou égal à celui des dénominateurs. Donc, chacune de ces fractions polynômiales a une limite quand x tend vers $+\infty$, qui vaut soit $e_{i,1}$, soit $f_{j,1}$, soit 0. *Ainsi, on a* $\lim_{x\to+\infty}(xf(x)) = \sum_{i=1}^{r} e_{i,1} + \sum_{j=1}^{s} f_{j,1}$.

Si les remarques précédentes ne sont pas assez efficaces pour déterminer la décomposition en éléments simples de $x \mapsto \frac{P(x)}{Q(x)}$, ce qui arrive en général lorsque Q possède des racines multiples, des racines complexes conjuguées, ou est de trop grand degré, il existe une méthode générale basée sur la résolution d'un système linéaire.

MÉTHODE 96 — *Déterminer la décomposition en éléments simples de la fonction rationnelle* $x \mapsto \frac{P(x)}{Q(x)}$:

- *On effectue la division euclidienne de P par Q :* $P = AQ + B$ *avec* $\deg(B) < \deg(Q)$.
  On a alors $R = A$.
  Si $\deg(P) < \deg(Q)$, *alors on a automatiquement* $R = 0$.
- *On a* $\frac{P(x)}{Q(x)} - R(x) = \frac{A(x)Q(x)+B(x)}{Q(x)} - \frac{R(x)Q(x)}{Q(x)} = \frac{B(x)}{Q(x)}$.
  Pour déterminer les coefficients $e_{i,k}, f_{j,k}, g_{j,k}$, *il suffit de le faire pour* $\frac{B(x)}{Q(x)}$, *qui est une fonction rationnelle plus simple car* $\deg(B) < \deg(Q)$.
- *On peut toujours déterminer ces coefficients en écrivant la forme de la décomposition en éléments simples, et en développant celle-ci par une mise au dénominateur commun. On obtient une équation de la forme* $\frac{B(x)}{Q(x)} = \frac{S(x)}{Q(x)}$ *où $S(x)$ est un polynôme dont les coefficients dépendent des* $e_{i,k}, f_{j,k}, gj, k$.
  Cette équation est vraie ssi on a $B(x) = S(x)$. *Et, deux fonctions polynômiales sont identiques si et seulement si elles ont les mêmes coefficients.*

Cela fournit un système linéaire de $\deg(Q)$ *équations, comportant* $\deg(Q)$ *inconnues.*
On peut alors résoudre ce système avec la méthode du Pivot pour obtenir son unique solution.

EXEMPLE 97 — *Soit* $f : x \mapsto \frac{x^4+3x^2-1}{(x+2)}$. *On pose* $D_f = \mathbb{R} \setminus \{-2\}$. *Il existe alors* $a \in \mathbb{R}$ *et* $R \in \mathbb{R}[X]$ *tels que pour tout* $x \in D_f$ *on a* $f(x) = R(x) + \frac{a}{x+2}$.
On effectue la division euclidienne de $X^4 + 3X^2 - 1$ *par* $X + 2$: $X^4 + 3X^2 - 1 = (X + 2)(X^3 - 2X^2 + 7X - 14) + 27$.
Ainsi, pour $x \in D_f$, *on a* $f(x) = x^3 - 2x^2 + 7x - 14 + \frac{27}{x+2}$.

EXEMPLE 98 — *Soit* $f : x \mapsto \frac{1}{x^2-5x+1}$. *Les racines de* $Q(X) = X^2 - 5X + 1$ *sont* $x_1 = \frac{5+\sqrt{21}}{2}$ *et* $x_2 = \frac{5-\sqrt{21}}{2}$. *On pose* $D_f = \mathbb{R} \setminus \{x_1, x_2\}$. *Il existe alors* $(a, b) \in \mathbb{R}^2$ *tel que pour tout* $x \in D_f$ *on a* $f(x) = \frac{a}{x-x_1} + \frac{b}{x-x_2}$.
On a : $a + b = \lim_{x\to+\infty}(xf(x)) = \lim_{x\to+\infty}(\frac{x}{x^2-5x+1}) = 0$, *donc* $b = -a$.
Et, on a $a = \lim_{x\to x_1}((x - x_1)f(x)) = \lim_{x\to x_1} \frac{(x-x_1)}{(x-x_1)(x-x_2)} = \lim_{x\to x_1} \frac{1)}{(x-x_2)} = \frac{1}{x_1-x_2} = \frac{1}{\sqrt{21}}$.
Ainsi, pour $x \in D_f$, *on a* $f(x) = \frac{1}{\sqrt{21}}(\frac{1}{x-x_1} + \frac{-1}{x-x_2})$.

EXEMPLE 99 — *Soit* $f : x \mapsto \frac{3x^2-2x+5}{(x+2)(x-1)(x-3)}$. *On pose* $D_f = \mathbb{R} \setminus \{1, -2, 3\}$. *Il existe alors* $(a, b, c) \in \mathbb{R}^3$ *tel que pour tout* $x \in D_f$ *on a* $f(x) = \frac{a}{x+2} + \frac{b}{x-1} + \frac{c}{x-3}$.
Et on a : $a = \lim_{x\to-2}((x + 2)f(x)) = \lim_{x\to-2}(\frac{3x^2-2x+5}{(x-1)(x-3)}) = \frac{3(-2)^2-2(-2)+5}{(-2-1)(-2-3)} = \frac{21}{15} = \frac{7}{5}$,
$b = \lim_{x\to1}((x - 1)f(x)) = \frac{3(1)^2-2(1)+5}{(1+2)(1-3)} = \frac{6}{-6} = -1$.
De plus on a $a+b+c = \lim_{x\to+\infty} xf(x) = \lim_{x\to+\infty} \frac{3x^2-2x+5}{(x+2)(x-1)(x-3)} = 3$. *On a donc* $c = 3-a-b = \frac{15-7+5}{5} = \frac{13}{5}$.
Ainsi, pour $x \in D_f$ *on a* $\frac{3x^2-2x+5}{(x+2)(x-1)(x-3)} = \frac{1}{5}(\frac{7}{x+2} + \frac{-5}{x-1} + \frac{13}{x-3})$.

EXEMPLE 100 (**Dérivée logarithmique**) — *Soit* $f : x \mapsto \frac{P'(x)}{P(x)}$, *avec* $P(x) = \prod_{i=1}^{r}(x - a_i)^{\alpha_i}$.
On pose $D_f = \mathbb{R} \setminus \{a_1, \ldots, a_r\}$.
D'après les formules de dérivation, on reconnaît que f *est la dérivée de* $\ln(|P|)$ *sur* D_f.
Or, pour $x \in D_f$, *on a* $\ln(|P(x)|) = \ln(\prod_{i=1}^{r} |(x - a_i)^{\alpha_i}|) = \sum_{i=1}^{r} \ln(|x - a_i|^{\alpha_i}) = \sum_{i=1}^{r} \alpha_i \ln(|x - a_i|)$.
On obtient alors que la dérivée de $\ln(|P|)$ *en* x *vaut :* $f(x) = (\ln(|P|))'(x) = \sum_{i=1}^{r} \frac{\alpha_i}{x-a_i}$.
Par unicité de la décomposition en éléments simples, on a ainsi obtenu la décomposition en éléments simples de f.

Bilan du contenu nécessaire à maîtriser :

- Définition d'un polynôme (suite avec un nombre fini de termes non-nuls). Sens de l'inconnue X. Coefficients d'un polynôme. Ecriture $P(X) = \sum_{k=0}^{n} a_k X^k$. Ensemble de polynômes $\mathbb{K}[X]$.
- Somme de polynômes $P+Q$, multiplication par un scalaire $\lambda.P$, produit de polynômes $P \times Q$. Savoir calculer une somme et un produit de polynômes proprement (réarranger les coefficients selon les puissances de X).
- Degré d'un polynôme, coefficient dominant. Cas particulier du polynôme nul. Degré d'une somme et d'un produit de polynômes. Ensemble $\mathbb{K}_n[X]$ de polynômes de degré majoré par n. Savoir identifier le degré d'un polynôme.
- Evaluation d'un polynôme P en un nombre x, notée $P(x)$. Fonction polynômiale associée à P : $f_P : x \in \mathbb{K} \mapsto P(x) \in \mathbb{K}$.
- Composée de polynômes $P \circ Q$. Lien entre opérations entre polynômes et opérations entre fonctions polynômiales associées.
- Un polynôme unitaire est un polynôme dont le coefficient dominant vaut 1.
- Division euclidienne de polynômes : Il existe un unique couple (Q, R) de polynômes tel que $P = AQ + R$, $\deg(R) < \deg(Q)$.
  Savoir calculer une division euclidienne de polynômes. Liens avec la division euclidienne d'entiers.
- Définition de A divise P. A divise P ssi le reste dans la div. eucl. de A par P est nul.
- Un polynôme P est irréductible si ses seuls diviseurs sont constants ou multiples de P (égaux à 1 ou P à un facteur près).
- a est une racine du polynôme P si $P(a) = 0$. a est une racine ssi $(X - a)$ divise P.
  Multiplicité d'une racine a. Polynômes scindés, scindés à racines simples.
- Polynôme dérivé P'. Savoir dériver un polynôme P. Degré de P'. Relation entre dérivée de P et dérivée de f_P (cas réel).
  Caractérisation des racines multiples : a est une racine de P de multiplicité k ssi $P(a) = 0, P'(a) = 0, \ldots, P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.
- Formule de Taylor pour les polynômes : Pour P de degré au plus n, on a $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.
  Savoir utiliser la formule de Taylor pour retrouver un polynôme P à partir de ses nombres dérivés en un point a.
- Théorème de Rolle pour les polynômes réels : Entre deux racines de P se trouve une racine de P'.
- Pour P un polynôme à coefficients réels et a une racine complexe de P de multiplicité k, $\overline{a}$ est aussi une racine de P de multiplicité k. (racines complexes conjuguées)
- P est irréductible dans $\mathbb{R}[X]$ ssi P est de degré 1 ou de degré 2 à discriminant strictement négatif. P est irréductible dans $\mathbb{C}[X]$ ssi P est de degré 1.
- Théorème de décomposition en produit de facteurs irréductibles : Tout polynôme P non-constant de $\mathbb{C}[X]$ (resp. $\mathbb{R}[X]$) s'écrit comme un produit de polynômes irréductibles.
  Ce produit est unique à l'ordre près des termes.
- Relations entre coefficients et racines pour les polynômes scindés.
  Pour P de degré n et de racines $\alpha_1, \ldots, \alpha_n$, on a $a_0 = (-1)^n \alpha_1 \ldots \alpha_n$ et $a_{n-1} = -(\alpha_1 + \ldots + \alpha_n)$.
- (x, y) est solution du système "$x + y = a$ et $xy = b$" ssi x et y sont les racines de $P(X) = X^2 - aX + b$. Savoir résoudre un tel système d'équations.