Chapitre 11
Polynômes

Table des matières

Vidal AGNIEL

Polynômes à une indéterminée

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 fonction. Mais sa construction 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 — *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 $x \mapsto P(x)$).*

Définition 4
Soit $\mathbb{K}$ un corps. On définit sur $\mathbb{K}[X]$ deux lois internes $(+, \times)$ et une loi externe $(.)$. Soient $P(X) = a_0 + \ldots + a_nX^n, Q(X) = b_0 + \ldots + b_nX^n + \ldots + b_mX^m$ deux polynômés de $\mathbb{K}[X]$ (avec $n \leq m$).

1. L'addition, $+$, est définie par :

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

   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, $\times$, est définie par :

$$(a_0+\ldots+a_nX^n)+(b_0+\ldots+b_nX^n+\ldots+b_mX^m) = c_0+c_1X+\ldots+c_{n+m}X^{n+m}, \text{ avec } c_r = \sum_{k=0}^{n} a_k b_{r-k}.$$

   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 $\times$.
3. La multiplication par un scalaire de $\mathbb{K}$, ., définie par :

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

Proposition 5
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 $\mathbb{C}$).

Démonstration —Sur feuille.

Remarque 6 — *Soit $\mathbb{K}[X]$ un corps. Soit $P(X) = a_0+\ldots+a_nX^n \in \mathbb{K}[X]$.*
Alors, 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.

Écriture d'un polynôme

Proposition 7
Tout polynôme $P \in \mathbb{K}[X]$ non nul s'écrit de manière unique de la forme :

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

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 $P(X) = a_0+\ldots+a_mX^m$ 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 $a_mn \neq 0$ (il existe bien).
Cela veut dire que pour tout $j > m$, on a $a_j = 0$.
Ainsi, on obtient que $P(X) = a_0+\ldots+a_nX^n$.
Comme l'entier n est unique (c'est LE plus grand indice), cette écriture est unique. □

Remarque 8 — *Pour écrire un produit de polynômes en utilisant le symbole $\sum$, cela donne :*

$$\left(\sum_{k=0}^{n} a_kX^k\right) \times \left(\sum_{k=0}^{m} b_kX^k\right) = \sum_{k=0}^{m+n} c_kX^k, \text{ avec } c_k = \sum_{i=0}^{k} a_ib_{k-i}.$$

Exemple 9 — *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 10 — *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 $\mathbb{K}[X]$.

1.2 Degré d'un polynôme

Définition 11
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 12
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 13
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 14

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 15
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 16 — *Attention ! L'écriture* $P(X)=\sum_{k=0}^{n}a_kX^k$ *avec* $a_0,\dots,a_n\in\mathbb{K}$ *nous dit seulement que* $\deg(P)\leq n$. *Il faut rajouter la condition* $a_n\neq 0$ *pour avoir* $\deg(P)=n$.

Exemple 17 — *Quel est de degré du polynôme* $(X+1)^n-(X-1)^n$ *?*

Proposition 18
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 19
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 $n+1$.

1.3 Fonctions polynomiales

Définition 20
Soit $P(X)\in\mathbb{K}[X]$, avec $P(X)=\sum_{k=0}^{n}a_kX^k$.
On appelle **fonction polynomiale associée au polynôme** $P(X)$, notée P ou f_P ou $(x\mapsto P(x))$, la fonction définie par :

$$P:\begin{array}{ccc}\mathbb{K} & \to & \mathbb{K}\\ x & \mapsto & P(x):=\sum_{k=0}^{n}a_kx^k\end{array}.$$

Exemple 21 — *La fonction* $x\in\mathbb{R}\mapsto ax^2+bx+c$ *est entre autres la fonction polynômiale associée à* $aX^2+bX+c\in\mathbb{R}[X]$.

Composition de polynômes

Définition 22
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 23 —

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 :*

   $$P\circ(Q+R)(X) \neq P\circ Q(X)+P\circ R(X) \quad , \quad P\circ(\lambda X) \neq \lambda P(X) \quad \text{et} \quad P\circ(Q\times R)(X) \neq P\circ Q(X)\times P\circ R(X).$$
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 24 — *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 $Q \circ P(X) = P(X) + P(1) = X^2 + 2X + 9$ 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 25
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 26 — *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 $\mathbb{Z}$.

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 27 (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 28 — *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 29 (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 $B = X^3 - 2X + 3$:

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

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 30
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 31 —

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 32 — *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 33 — *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 34 (**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 $P(\alpha) = 0$, où $P(\alpha)$ désigne l'image de α par la fonction polynômiale associée à P.

Proposition 35 (**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 $P(X)$. □

4.1 Multiplicité d'une racine, polynômes scindés

Définition 36
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 $(X-\alpha)^k | P$ et $(X-a)^{k+1} \not| P$.
Une racine de multiplicité 1 est appelée **racine simple** de P.

Proposition 37
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 :

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

Démonstration —Admis.

Corollaire 38
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 39 (**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 40 — *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 41 — *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 42
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 43 — *Pour $n \geq 1$ et $a_n \neq 0$, le coefficient $n a_n$ est non-nul.*

Proposition 44
Soit $P \in \mathbb{K}[X]$. On a $\deg(P') = \deg(P) - 1$ si $\deg(P) \geq 1$, et $P'(X) = 0$ sinon.

Proposition 45 (**Application linéaire de dérivation**)
La fonction $D : P \in \mathbb{K}[X] \mapsto P' \in \mathbb{K}[X]$ est une application linéaire.
De plus, $\operatorname{Ker}(D) = \{\lambda, \lambda \in \mathbb{K}\}$ est l'ensemble des polynômes constants. ($P'(X) = 0 \Leftrightarrow P(X) = a_0$)

Démonstration —A faire après le chapitre Applications linéaires.

Proposition 46 (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 47 (**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 48 — *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 49 (**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 50 (**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.

EXEMPLE 51 — *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 fomule de Taylor à :
1. $X^3 + X^2 + X + 1$ *et* $\alpha = 1$ *;*
2. $2X^4 + 2X + 1$ *et* $\alpha = -1$.

5.3 Caractérisation des racines multiples

PROPOSITION 52 (**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 53 (**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 54 — *Dans $\mathbb{C}[X]$, pour $\omega \neq 0$, l polynôme $P(X) = X^n - \omega$ n'admet que des racines simples, puisque $P'(X) = nX^{n-1}$ n'admet pas de racine commune avec P.*

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 55 (**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 56 (**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 57
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 58 — *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 59 (**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.

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

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

Théorème 60 (**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 61 (**Polynômes irréductibles dans $\mathbb{C}$**)
Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Corollaire 62 (**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 $\alpha_1, \ldots, \alpha_r$ sont des entiers non nuls et $z_1, \ldots, z_r$ sont des nombres complexes deux à deux distincts.
Cette décomposition est unique à l'ordre des z_i près.

Remarque 63 — *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, comme nous allons le prouver.

Lemme 64
Soit $P \in \mathbb{R}[X]$. Soit $\alpha \in \mathbb{C} \setminus \mathbb{R}$ une racine complexe de P. Alors, $\bar{\alpha}$ est aussi une racine de P.

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

$$P(\bar{\alpha}) = a_n \bar{\alpha}^n + \ldots + a_1 \bar{\alpha} + a_0 = \overline{a_n \alpha^n + \ldots + a_1 \alpha + a_0} = \overline{P(\alpha)} = 0.$$

Donc $\bar{\alpha}$ est bien une racine de P. □

Proposition 65 (**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 66 —

1. *Le polynôme $X^3 + 1$ n'est pas irréductile 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 67 (**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 $\alpha_1, \ldots, \alpha_r, \beta_i, \ldots, \beta_m$ 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 68 (**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 69
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 70 — *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 71 (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 72
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 73 — *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 $\{(-1, -2), (-2, -1)\}$.

Bilan du contenu <u>nécessaire</u> à maîtriser :

- Définition d'un polynôme. Coefficients. Ensemble $\mathbb{K}[X]$.
- Connaître et savoir réaliser les opérations sur les polynômes : Somme, multiplication par λ, produit.
  Savoir calculer un produit de polynômes proprement (réarranger les coefficients selon leur degré).
- Degré. Degré d'une somme, d'un produit. Savoir identifier le degré d'un polynôme. Ensemble $\mathbb{K}_n[X]$.
- Fonction polynômiale associée f_P.
- Composée $P \circ Q$. Lien avec les fonctions polynômiales.
- Polynômes unitaires.
- Division euclidienne de polynômes $P = AQ + R$, $\deg(R) < \deg(Q)$. Divisibilité de polynômes. Polynômes irréductibles.
- Racines d'un polynôme. a est une racine ssi $(X - a)$ divise P.
  Multiplicité d'une racine, polynômes scindés/scindés à racines simples.
- Dérivée d'un polynôme. Savoir dériver un polynôme P. Lien avec la fonction polynômiale f_P. Degré de P'. Caractériser les racines multiples à l'aide des dérivées.
- Formule de Taylor pour les polynômes $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.
  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'.
- Polynômes irréductibles dans $\mathbb{R}[X]$ (degré 1 et degré 2 à discriminant < 0) et dans $\mathbb{C}[X]$ (degré 1).
- Relations entre coefficients et racines pour les polynômes scindés. Les relations entre a_0, a_{n-1} et les racines $\alpha_1, \ldots, \alpha_n$ sont à connaître.
- Savoir résoudre un système "$x + y = a$ et $xy = b$" avec les racines d'un polynôme de degré 2.