# Chapitre VII
# Polynômes à une indéterminée

Dans ce cours, $\mathbb{K}$ désigne $\mathbb{R}$, $\mathbb{C}$ ou un corps commutatif quelconque.

## I – Rappels, opérations générales

### 1. Définitions

**Définition :** On appelle polynôme à coefficients dans $\mathbb{K}$ et à une indéterminée $X$ une expression de la forme $P(X) = a_0 + a_1X + \cdots + a_nX^n$ avec $a_0, a_1, \dots, a_n \in \mathbb{K}$.

On note $\mathbb{K}[X]$ l'espace des polynômes à coefficients dans $\mathbb{K}$.

**Idée :** On voit un polynôme comme une expression algébrique, une suite de coefficients en fait, plutôt qu'une fonction.

**Convention :** On pose $X^0 = 1 \quad \rightarrow \quad P(X) = \sum_{i=0}^{n} a_iX^i$

**Définition :** Si $P \neq 0$, alors on appelle le *degré* de $P$ le plus grand $n$ tel que $a_n \neq 0$.
On pose par convention $\deg 0 = -1$ ou $-\infty$.

On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg P \leq n\}$ le sous-espace des polynômes de degré $\leq n$.

**Attention :** Les expressions $\sqrt{X^2 + 2X + 1}$, $\frac{1}{X+1}$, $\sum_{n=0}^{\infty} \frac{X^n}{n!} \notin \mathbb{R}[X]$.

### 2. Opérations algébriques

#### i) Structure d'espace vectoriel (rappels)

Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. $P + Q$ et $\lambda P$ ont déjà été définis.

**Propriétés :**
**1)** $\mathbb{K}[X]$ et $\mathbb{K}_n[X]$ sont des $\mathbb{K}$-ev.
**2)** L'application $\varphi$: $\begin{matrix}\mathbb{K}_n[X] \to \mathbb{K}^{n+1} \\ P \mapsto (a_0, a_1, \dots, a_n)\end{matrix}$ est un isomorphisme.
**3)** La famille $B = (1, X, \dots, X^n)$ est la base canonique de $\mathbb{K}_n[X]$.
**4)** $\dim \mathbb{K}_n[X] = n + 1$.

#### ii) Produit dans $\mathbb{K}[X]$

On définit un produit interne dans $\mathbb{K}[X]$ en posant $X^p \times X^q = X^{p+q}$, et on étend par linéarité et par distributivité de $+$ par rapport à $\times$.

$$\text{Si } P = \sum_{k=0}^{\deg P} a_kX^k \text{ et } Q = \sum_{q=0}^{\deg Q} b_qX^q \text{ alors } P \times Q = \sum_{n=0}^{\deg P + \deg Q} c_nX^n$$

avec $c_n = \sum_{k=0}^{n} a_kb_{n-k}$ somme finie.

**Exemple :** $(1+X)(1-X) = 1+X-X-X^2 = 1-X^2$.

**Propriétés du produit :**
∗ Si $P$ et $Q$ sont non nuls, alors $PQ$ est non nul et $\deg(PQ) = \deg P + \deg Q$. On dit alors que $\mathbb{K}[X]$ est intègre : $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$.

∗ Commutatif : $PQ = QP$

∗ Associatif : $P(QR) = (PQ)R$

∗ Distributif par rapport à $+$ : $(P+Q)R = PR + QR$.

∗ $P = 1$ est l'élément neutre pour le produit.

**Structure d'algèbre commutative** : $(\mathbb{K}[X], +, \times)$ est une *algèbre commutative*. (Il n'y a pas d'inverse pour $\times$, ce n'est donc pas un corps). Il est donc différent du corps des fractions rationnelles, noté lui $(\mathbb{K}(X), +, \times)$. (Voir cours d'analyse.)

**iii) Composition des polynômes**

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

Alors on note $P \circ Q = \sum_{k=0}^{d} a_k Q(X)^k$ : c'est-à-dire que l'on remplace l'indéterminée $X$ par $Q(X)$.

**Exemple :** $P(X^2)$ , $P(X+a)$, $a \in \mathbb{K}$.

**Propriété** : Si $P$ et $Q$ sont non nuls, alors $\deg(P \circ Q) = \deg P \times \deg Q$.

**iv) Dérivation**

On pose $(X^n)' = nX^{n-1}$, pour tout entier $n$ strictement positif, et on étend par linéarité en posant :
$\left(\sum_{k=0}^{d} a_k X^k\right)' = \sum_{k=1}^{d} k a_k X^{k-1}$.

On vérifie la règle de Leibnitz : $(PQ)' = P'Q + PQ'$. (Exercice : par linéarité suivant $P$ et $Q$.)

**v) Substitution, fonctions polynomiales associées**

A tout polynôme algébrique $P \in \mathbb{K}[X]$, on peut associer plusieurs fonctions polynomiales.

Soit $A$ une partie de $\mathbb{K}$. Par exemple : $A = \mathbb{R}, \mathbb{C}, [a,b], \mathbb{N}\ldots$

On considère l'application

$$S_A : \begin{matrix}\mathbb{K}[X] \to P_A \\ P(X) \mapsto \overline{P}\end{matrix} \quad \text{avec} \quad \overline{P} : \begin{matrix}A \to \mathbb{K} \\ x \mapsto a_0 + a_1 x + \cdots + a_n x^n\end{matrix} \text{ fonction sur } A.$$

On substitue la *variable* $x \in A$ à l'*indéterminée* $X$ pour obtenir la fonction $\overline{P}$ sur $A$.

$P_A$ est l'espace des fonctions polynomiales sur $A$.

**Théorème :** $S_A$ est un isomorphisme si et seulement si $A$ a une *infinité* de points,
i.e. le polynôme $\overline{P}$ sur $A$ détermine uniquement $P$ lorsque $card\ A = +\infty$.

**Démonstration :** Si $P$ est de degré $n$, alors il est déterminé par ses valeurs prises en $n+1$ points (interpolation de Lagrange), ce qui est possible pour tout $n$ si $A$ n'est pas fini.

→ Ok pour $A = \mathbb{N}, \mathbb{R}, \mathbb{C}, [a,b]$ si $a < b$…

**Propriétés :** $\overline{PQ} = \overline{P} \times \overline{Q}$ et $\overline{P+Q} = \overline{P} + \overline{Q}$.

**Conséquence importante** : On peut *identifier* algébriquement la notion abstraite de polynôme à une indéterminée à celle de fonction polynomiale, si on regarde cette fonction sur suffisamment de points.

### vi) Formule de Taylor

**Théorème :** Soient $x_0 \in \mathbb{K}$, et $P \in \mathbb{K}[X]$ de degré $n$. On a :

$$P(X+x_0) = P(x_0) + P'(x_0)X + P''(x_0)\frac{X^2}{2!} + \cdots + P^{(n)}(x_0)\frac{X^n}{n!}$$

**Démonstration :** C'est une formule linéaire par rapport à $P$. Il suffit de vérifier pour $P = X^n$.

$P(X+x_0) = (X+x_0)^n = x_0^n + nx_0^{n-1}X + \cdots + nx_0X^{n-1} + X^n$

$P(X+x_0) = \sum_{k=0}^{n}\binom{n}{k}x_0^{n-k}X^k$ (binôme de Newton, algébrique par récurrence)

avec $\binom{n}{k} = C_n^k = \frac{n(n-1)\ldots(n-k-1)}{k!}$.

D'autre part, $(x_0^n)^{(k)} = n(n-1)\ldots(n-k-1){x_0}^{n-k} = \binom{n}{k}k!\,x_0^{n-k}$

→ Les formules coïncident. Formule du binôme = Formule de Taylor pour $P = X^n$.

**Remarques** :
**1)** Cette formule marche aussi pour $P \in \mathbb{C}[X]$ → Il existe une formule de Taylor pour $P(z+z_0)$ avec $z \in \mathbb{C}$.
**2)** Il n'y a pas de reste dans la formule de Taylor lorsque l'on travaille avec des polynômes.

# II – Division et factorisation

## 1. Division euclidienne

On a sur $\mathbb{K}[X]$ une opération algébrique de division avec reste, similaire à la division euclidienne des entiers.

**Définition :** Soient $P, Q \in \mathbb{K}[X]$. On dit que $Q$ divise $P$ s'il existe un polynôme $R$ tel que $P = Q \times R$.

**Attention :** On évite d'écrire $R = \frac{P}{Q}$, car il ne s'agit en général pas d'un polynôme.

**Théorème de la division euclidienne :** Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$.
Alors il existe deux polynômes $Q$ et $R$ tels que :
**i)** $A = BQ + R$
**ii)** et $\deg R < \deg B$.

Les polynômes $Q$ et $R$ ainsi définis sont uniques : $Q$ s'appelle le *quotient* de la division de $A$ par $B$ et $R$ s'appelle le *reste* de la division.

**Démonstration de l'unicité de $Q$ et $R$ :** On suppose que $A = BQ + R = BQ' + R'$

$\Rightarrow B(Q - Q') = R' - R$.

Si $Q \neq Q'$ alors $B(Q - Q') \geq \deg B$ alors que $\deg(R' - R) < \deg B$.

$\rightarrow B(Q - Q') = R' - R \Rightarrow Q = Q'$ et $R = R'$.

**Démonstration de l'existence de $Q$ et $R$ :** On procède par algorithme, en suivant l'exemple :

$$\begin{array}{r|l} A = 2X^3 + 2X^2 + X - 1 & B = X^2 - X + 1 \\ \hline -\,2XB = 2X^3 - 2X^2 + 2X & 2X + 4 = Q \\ \hline A' = 4X^2 - X - 1 & \\ -\,4B = 4X^2 - 4X + 4 & \\ \hline 3X - 5 = R & \end{array}$$

On a donc bien $A = BQ + R \rightarrow 2X^3 + 2X^2 + X - 1 = (X^2 - X + 1)(2X + 4) + (3X - 5)$

On vérifie le coefficient dominant et la constante.

**En particulier** : On dit que $B$ divise $A$ si et seulement si $R = 0$.

**Exemple :** $A = X^3 + 2X^2 + 3X + 2$ et $B = X + 1$.

$$\begin{array}{r|l} X^3 + 2X^2 + 3X + 2 & X + 1 \\ \hline -\,(X^3 + X^2) & X^2 + X + 2 = Q \\ \hline X^2 + 3X + 2 & \\ -(X^2 + X) & \\ \hline 2X + 2 & \\ -\,(2X + 2) & \\ \hline 0 = R & \end{array}$$

On a donc $X + 1$ qui divise $X^3 + 2X^2 + 3X + 2$, le reste de la division étant nul, et aussi

$$X^3 + 2X^2 + 3X + 2 = (X + 1)(X^2 + X + 2)$$

En particulier, on a pour $X = -1$ que $A = 0 \rightarrow -1$ est racine de $A$.

## 2. Racines et factorisation de polynômes

### i) Cas d'une racine unique

**Proposition :** Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors $X - a$ divise $P$ si et seulement si $P(a) = 0$ i.e. $a$ est une racine de $P$.

**Démonstration :** On divise $P$ par $X-a$ avec reste : $P=(X-a)Q+R$ avec $\deg R<1 \to R$ est donc une constante.

Pour $X=a$, on obtient $P(a)=R \Leftrightarrow P=(X-a)Q+P(a)$.

Donc $X-a$ divise $P$ si et seulement si $P(a)=0$.

**Définition :** Si $a$ est une racine de $P$, on appelle *multiplicité* de $a$ le plus grand entier $n$ supérieur à 1 tel que $(X-a)^n$ divise $P$. On dit aussi que $a$ est une *racine d'ordre* $n$.

**Théorème de caractérisation des racines multiples par les dérivées.**
**1)** $a$ est une racine d'ordre $n$ de $P$ si et seulement si

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

**2)** $a$ est une racine d'ordre supérieur ou égal à $n$ de $P$ ssi

$$P(a)=P'(a)=\cdots=P^{(n-1)}(a)=0.$$

**Exemples :**
$*$ $a$ racine d'ordre 1 $\Leftrightarrow$ $a$ est une racine simple $\Leftrightarrow P(a)=0$ et $P'(a)\neq 0$.
$*$ $a$ racine d'ordre 2 $\Leftrightarrow$ $a$ est une racine double $\Leftrightarrow P(a)=P'(a)=0$ et $P''(a)\neq 0$.

**Démonstration :**
Preuve par récurrence possible, ou avec Taylor. On a

$$P(X)=P(a)+P'(a)(X-a)+\cdots+P^{(n)}(a)\frac{(X-a)^n}{n!}+\cdots+P^{(d)}(a)\frac{(X-a)^d}{d!} \text{ avec } \deg P=d.$$

$$P(X)=\underbrace{(X-a)^n}_{B}\underbrace{\left(\frac{P^{(n)}(a)}{n!}+\cdots+\frac{P^{(d)}(a)}{d!}(X-a)^{d-n}\right)}_{Q}+\underbrace{P(a)+\cdots+\frac{P^{(n-1)}(a)}{(n-1)!}(X-a)^{n-1}}_{R}$$

avec $\deg R\leq n-1<n=\deg(X-a)^n$.

On a $a$ racine d'ordre supérieur à $n \Leftrightarrow (X-a)^n$ divise $P$
$\Leftrightarrow R=0$
$\Leftrightarrow P(a)=\cdots=P^{(n-1)}(a)=0$
De plus, $a$ est une racine d'ordre $n$ si $P^{(n)}(a)\neq 0$.

**ii) Généralisation pour plusieurs racines**

On peut factoriser un polynôme dont on connait plusieurs racines.

**Théorème :** Soit $P\in\mathbb{K}[X]$.
Alors $a_1,a_2,\ldots,a_k\in\mathbb{K}$ sont les racines de $P$ d'ordres respectifs supérieurs à $n_1,n_2,\ldots,n_k$ si et seulement si

$$(X-a_1)^{n_1}\times(X-a_2)^{n_2}\times\ldots\times(X-a_k)^{n_k} \text{ divise } P.$$

**Corollaire :** Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors $P$ a au plus $n$ racines dans $\mathbb{K}$ (si comptées avec leur multiplicité). Plus précisément, on a toujours :

$$card(\text{racines simples}) + 2card(\text{racines doubles}) + \cdots \leq n = \deg P$$

**Démonstration :** Récurrence sur $k$.

$*$ Le cas $k = 1$ est vérifié par définition.

$*$ On suppose que $a_1$ est une racine de $P$ d'ordre supérieur à $n_1 \Leftrightarrow P = (X - a_1)^{n_1} Q$.

- Si $a$ est une racine de $Q$, alors $P(a) = 0$ et $a$ est aussi racine de $P$.

**Inversement**, les racines de $P$ différentes de $a_1$ sont aussi des racines de $Q$, car pour $X = a$, on a $0 = (a - a_1)^{n_1} Q(a)$. Sachant que $a \neq a_1$, on a forcément $Q(a) = 0$.

Si $a$ est racine d'ordre $n$ de $Q$, alors $Q = (X - a)^n D$ avec $D(a) \neq 0$.

$\Rightarrow P(X) = (X - a)^n (X - a_1)^{n_1} D(X)$ avec $(a - a_1)^{n_1} D(a) \neq 0$ si $a \neq a_1$.

$\Rightarrow a$ est racine d'ordre $n$ de $P$.

**Conclusion :** Les racines de $P$ et $Q$ différentes de $a_1$ sont les mêmes avec même multiplicité. On peut appliquer la récurrence à $D$.

**Illustration :** Soit $P$ un polynôme quelconque. A quelles conditions sur $P$ a-t-on $X^2 + X$ divise $P$ ?

**2 méthodes :** $*$ On divise $P$ par $X^2 + X$ et on regarde le reste. Cette méthode peut être « fastidieuse » si $P = X^n + X + a$ avec $n = 10^{39484}$.

$*$ Ou bien on factorise et on utilise le théorème : $X^2 + X = X(X + 1) \rightarrow X^2 + X$ divise $P$ si et seulement si $P(0) = P(-1) = 0 \Leftrightarrow a = 0$ et $n$ est pair.

## 3. Notion de PGCD et algorithme d'Euclide

Il est difficile de connaitre les facteurs d'un polynôme donné. Par contre, il est facile de savoir si deux polynômes ont des diviseurs communs grâce à l'algorithme d'Euclide.

**Proposition :** Soient $P_1, P_2 \in \mathbb{K}[X]$ données avec $P_2 \neq 0$.
On divise $P_1$ par $P_2 \rightarrow P_1 = P_2 Q + R$ avec $\deg R < \deg P_2$.
Alors $D$ est un diviseur commun de $P_1$ et $P_2$ si et seulement si $D$ est un diviseur commun de $P_2$ et $R$.

**Démonstration :**
- Si $D$ divise $P_1$ et $P_2$ alors $P_1 = DQ_1$ et $P_2 = DQ_2$

$$\Longrightarrow R = P_2 - P_1 Q = D(Q_1 - Q_2)$$

$\Rightarrow D$ divise $R$.

**Inversement**, si $D$ divise R et $P_2$, alors $R = DQ_2$ et $P_2 = DQ_3$
$\Rightarrow P_1 = P_2Q + R = D(Q_3Q + Q_2)$ et $D$ divise $P_1$.

**Intérêt :** $\deg R < \deg P_2$, on peut recommencer en divisant $P_2$ par $R$ si $R$ est non nul.

**Algorithme d'Euclide :** Soient $P_1, P_2 \in \mathbb{K}[X]$ avec $P_2 \neq 0$.
On divise successivement :

$* P_1 = P_2Q_1 + R_1$

$* P_2 = P_1Q_2 + R_2$

$* R_1 = R_2Q_3 + R_3$

…

$* R_{n-2} = R_{n-1}Q_n + R_n$,

avec $\deg P_2 > \deg R_1 > \deg R_2 > \cdots > \deg R_n$.

On poursuit les divisions jusqu'à obtenir $R_n = 0$.

**Définitions :**
**1)** Le dernier reste *non nul* $R_{n-1}$ est le *plus grand diviseur commun, ou pgcd,* de $P_1$ et $P_2$. C'est-à-dire que tout autre diviseur commun de $P_1$ et $P_2$ est un diviseur de ce pgcd**.**

**2)** Si le pgcd est une constante non nulle, alors $P_1$ et $P_2$ n'ont pas de facteur commun autres que les constantes. On dit alors que $P_1$ et $P_2$ sont *premiers entre eux.*

**Remarque :** « le » pgcd n'est bien défini qu'à une constante multiplicative non nulle près.

**Exemple :** $*$ Soient $P_1 = X^3 + 2X^2 + 4X + 8$ et $P_2 = X^3 + 2X^2 + 2X + 4$.

Quel est le PGCD entre $P_1$ et $P_2$ ?

$$\begin{array}{r|l} X^3 + 2X^2 + 4X + 8 & X^3 + 2X^2 + 2X + 4 \\ \hline -(X^3 + 2X^2 + 2X + 4) & 1 \\ \hline 2X + 4 = R_1 & \end{array}$$

$$\begin{array}{r|l} X^3 + 2X^2 + 2X + 4 & 2X + 4 \\ \hline -(X^3 + 2X^2 + 2X + 4) & X^2/2 + 1 \\ \hline 2X + 4 & \\ \hline -(2X + 4) & \\ \hline 0 & \end{array}$$

Le Pgcd entre $P_1$ et $P_2$ étant le dernier reste non nul, on a donc $\text{Pgcd}(P_1, P_2) = X + 2$.

En divisant $P_1$ et $P_2$ par $X + 2$, on trouve :
$P_1 = (X + 2)(X^2 + 4)$
$P_2 = (X + 2)(X^2 + 2)$
$\rightarrow -2$ est racine commune de $P_1$ et $P_2$.

**Exemple d'application : les discriminants**

Si $P \in \mathbb{K}[X]$ possède une racine (au moins) double, $a$, alors $a$ est racine de $P$ et de $P'$.
$\Leftrightarrow (X-a)$ divise à la fois $P$ et $P'$.

$\Rightarrow (X-a)$ divise $\mathrm{Pgcd}(P, P')$.

Cela conduit à la notion de *discriminant* pour les polynômes.

**Exemples :**
$* P = aX^2 + bX + c$
$\rightarrow P' = 2aX + b$

$$\begin{array}{r|l} aX^2+bX+c & 2aX+b \\ \hline -(aX^2+bX/2) & X/2+b/4a \\ \hline bX/2+c & \\ -(bX/2+b^2/4a) & \\ \hline c-b^2/4a=R & \end{array}$$

Si $b^2 - 4ac \neq 0$ alors $P$ n'a pas de racine double
Si $b^2 - 4ac = 0$ alors $\frac{X}{2} + \frac{b}{4a} = \frac{1}{2}\left(X + \frac{b}{2a}\right)$ est le Pgcd de $P$ et $P'$.

$\rightarrow -\frac{b}{2a}$ est une racine double de $P$ (bien connu) !

$*$ Cas moins connu : si $P = X^3 + pX + q$ ,
on a $P' = 3X^2 + p$

$$\begin{array}{r|l} X^3+pX+q & 3X^2+p \\ \hline -(X^3+pX/3) & X/3 \\ \hline 2pX/3+q=R_1 & \end{array}$$

$$\begin{array}{r|l} 3X^2+p & 2pX/3+q \\ \hline -(3X^2+9qX/2p) & 9X/2p-27q/4p^2 \\ \hline -9qX/2p+p & \\ -(-9qX/2p-27q^2/4p^2) & \\ \hline p-27q^2/4p^2 & \end{array}$$

$\rightarrow$ Discriminant $\Delta = 4p^3 + 27q^2$

Si $\Delta \neq 0$, pas de racine double.
Si $\Delta = 0$, une racine double : $X = \frac{3q}{p}$.

# III – Le théorème d'Alembert-Gauss et ses conséquences

## 1. Factorisation ou décomposition dans $\mathbb{C}[X]$

### i) Les énoncés

**Théorème de d'Alembert-Gauss :**
Tout polynôme $P$ non constant dans $\mathbb{C}[X]$ admet au moins une racine complexe.
i.e. $\forall\, P \in \mathbb{C}[X], P$ non constant, $\exists\, z_0 \in \mathbb{C}$ tel que $P(z_0) = 0$.

**Conséquence : théorème de décomposition dans $\mathbb{C}[X]$**
Tout polynôme $P$ non constant dans $\mathbb{C}[X]$ se factorise sous la forme

$$P = c\prod_{i=1}^{k}(X - z_i)^{n_i} \text{ avec } c \in \mathbb{C}.$$

$\Leftrightarrow$ Si $P$ est de degré $n \geq 1$, alors il possède *exactement* $n$ racines complexes comptées avec leur multiplicité. On dit que $P$ est *scindé* dans $\mathbb{C}[X]$.

**Remarque :** $c$ est le coefficient de degré $n$ dans $P$ (coefficient dominant).

**Démonstration de la conséquence :** Tant que $\deg P \geq 1$, on lui trouve des racines, que l'on peut mettre en facteur. Cela s'arrête au bout d'un moment car il y a au plus $n$ racines.

### ii) Démonstration du théorème d'Alembert-Gauss

Hors programme ! Donnée ici « Pour la Patrie, la Science et la Gloire », et peut-être aussi pour donner envie à certains d'entre vous de continuer à faire des maths.

Soit $P \in \mathbb{C}[X]$ de degré supérieur à 1. On se demande s'il existe un $z_0 \in \mathbb{C}$ tel que $P(z_0) = 0$.

**La difficulté :** il n'y a pas de formule explicite pour les racines des polynômes de degré supérieur ou égal à 5. (Évariste Galois, vers 1831.)

**On doit donc utiliser une méthode théorique :**

On considère $\alpha = \inf(|P(z)|) \geq 0, z \in \mathbb{C}$.
**Deux étapes :**
**1)** Montrer que l'inf est atteint en un point $z_0$.
**2)** Montrer que cet inf est nul i.e. $\alpha = |P(z_0)| = 0$.

**1ère étape :** par définition de la borne inférieure, il existe une suite $(z_n)_{n\geq 1}$ de $\mathbb{C}$ telle que $|P(z_n)| \to \inf(|P(z)|) = \alpha$.

On montre que la suite $(z_n)$ est bornée : On a $P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0$

$\to |P(z)| \geq |a_n||z|^n + |a_{n-1}||z|^{n-1} + \cdots + |a_0| \xrightarrow[|z|\to+\infty]{} +\infty$

$\Rightarrow$ Il existe $R$ tel que si $|z| \geq R$ alors $|P(z)| \geq \alpha + 1$.

Comme $|P(z_n)| \to \alpha < \alpha + 1$, alors il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|P(z_n)| \leq R$.

Si $z_n = x_n + iy_n$, alors $|x_n| \leq |z_n| \leq R^n$ et $|y_n| \leq |z_n| \leq R^n$

⇒ Les suites $(x_n)$ et $(y_n)$ sont des suites réelles bornées.

D'après le théorème de Bolzano-Weierstrass, il existe une sous-suite $\left(x_{\varphi_1(n)}\right)$ de $x_n$ qui converge vers un réel $x_0$, *puis* une sous-suite $\left(y_{\varphi_2(\varphi_1(n))}\right)$ de $y_n$ qui converge vers un réel $y_0$.

Si on pose $\psi = \varphi_1 \, o \, \varphi_2$, alors on a $x_{\psi(n)} \to x_0$ et $y_{\psi(n)} \to y_0$

⇒ $z_{\psi(n)} \to z_0 = x_0 + iy_0$.

Par continuité de $|P(z)|$, on a $|P(z_0)| = \lim_{n\to+\infty}\left|P\left(z_{\psi(n)}\right)\right| = \alpha$

**2ème étape :** Montrer que $\alpha = 0$ en raisonnant par l'absurde. On suppose $\alpha > 0$ et on écrit la formule de Taylor pour $P$ en $z_0$ :

$P(z_0 + h) = P(z_0) + \frac{h^k}{k!}P^{(k)}(z_0) + o(h^k)$ avec $P^{(k)}(z_0) \neq 0$ (sinon $P$ serait constant, ce qui est contraire aux hypothèses)

On développe le module au carré :

$$|P(z_0 + h)|^2 = P(z_0 + h) \times \overline{P(z_0 + h)}$$
$$= |P(z_0)|^2 + \frac{h^k}{k!}P^{(k)}(z_0)\overline{P(z_0)} + \frac{\overline{h^k}}{k!}\overline{P^{(k)}(z_0)}P(z_0) + o(h^k)$$
$$= |P(z_0)|^2 + Re(h^k C) + o(h^k) \text{ avec } C = \frac{1}{k!}P^{(k)}(z_0)\overline{P(z_0)} \neq 0$$

On doit avoir $|P(z_0 + h)|^2 \geq |P(z_0)|^2$ pour tout $h \in \mathbb{C}$.

On écrit $h$ sous la forme polaire :$h = |h|e^{i\theta}$ et $C = |C|e^{i\alpha}$

$$\to Re(h^k C) = Re\left(|h|^k e^{ik\theta}|C|e^{i\alpha}\right)$$
$$= |h|^k|C|\cos(k\theta + \alpha) \quad \text{avec } k \text{ et } \alpha \text{ donnés.}$$

On prend $\theta$ tel que $k\theta + \alpha = \pi \to Re(h^k C) = -|h|^k|C|$

⇒ $|P(z_0 + h)|^2 - |P(z_0)|^2 = -|h|^k|C| + o(h^k) < 0$ pour $|h|$ assez petit.

**Contradiction** ⇒ $\alpha = 0 = |P(z_0)|$

⇒ $|P(z_0)| = 0$. CQFD.

**iii) Un exemple classique**

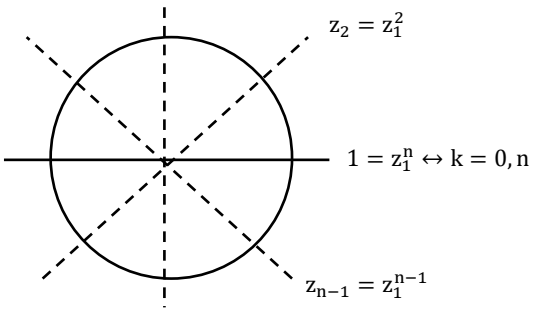
Soit P ∈ $\mathbb{K}[X]$ défini par $P(X) = X^n - 1$, $n \in \mathbb{N}$.

**Problème :** *Décomposer* P dans $\mathbb{C}[X]$ → le mettre sous la forme d'un produit de facteurs de degré 1.

Pour cela, on cherche les racines de P dans $\mathbb{C}$ :

$P(z) = 0 \Leftrightarrow z^n = 1 \Leftrightarrow z = e^{\frac{2ik\pi}{n}},\ k \in \mathbb{Z}$

$z = z_1^k = z_k$ avec $z_1 = e^{\frac{2i\pi}{n}}$ et $0 \leq k \leq n-1$.




Le polynôme P de degré n possède n racines. Cela rend les racines obligatoirement simples.

On a donc finalement :

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

## 2. Factorisation ou décomposition dans $\mathbb{R}[X]$

**Un exemple :** On voudrait factoriser au maximum $P(X) = X^4 - 1$ dans $\mathbb{R}[X]$.

Problème : Peut-on avoir $P(X) = Q_1(X)Q_2(X)$ avec $\deg Q_1 = 1$ ?

Non, car cela ferait que $Q_1(X) = aX + b$, et donc que $Q_1\left(-\frac{b}{a}\right) = 0$ , ce qui impliquerait que P admet une seule racine réelle : $-\frac{b}{a}$. C'est impossible, car $P(X) \geq 1$ sur $\mathbb{R}$.

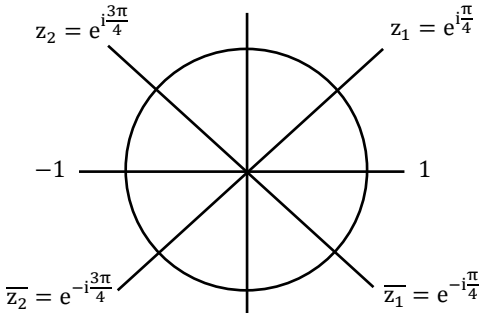
Il reste donc la possibilité $P(X) = P_1(X)P_2(X)$ avec $\deg P_1 = \deg P_2 = 2$.

**Méthode :** On cherche d'abord à factoriser dans $\mathbb{C}[X]$, c'est-à-dire à trouver les racines complexes de P.

$P(z) = 0 \Leftrightarrow z^4 = -1 \Leftrightarrow z = e^{\frac{ik\pi}{4}}, k \in \mathbb{Z}$.

Les quatre racines de P sont : $z_1,\ z_2,\ \overline{z_1},\ \overline{z_2}$

$\rightarrow P(X) = (X - z_1)(X - z_2)(X - \overline{z_1})(X - \overline{z_2})$




Si l'on développe les expressions conjuguées entre elles, on trouve l'expression :

$$P(X) = (X^2 - 2\mathrm{Re}(z_1)X + |z_1|^2)(X^2 - 2\mathrm{Re}(z_2)X + |z_2|^2)$$

Soit $P(X) = \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right)$. (Cela ne sautait pas aux yeux !)

On ne peut pas factoriser d'avantage P car il n'a pas de facteur de degré un.

On a pu regrouper les racines non réelles conjuguées deux par deux.

**Définition :** Si $P(X) = a_0 + a_1X + \cdots + a_nX^n$ à coefficients complexes, on note

$\overline{P}(X) = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n$ le *polynôme conjugué* de $P$.

**Propriétés :**

**a)** $P = \overline{P} \Leftrightarrow P \in \mathbb{R}[X]$,

**b)** $\overline{P}(\overline{z}) = \overline{P(z)} = \overline{a_0 + a_1 z + \cdots + a_n z^n}$ pour $z \in \mathbb{C}$,

**c)** $\overline{PQ} = \overline{P}.\overline{Q}$,

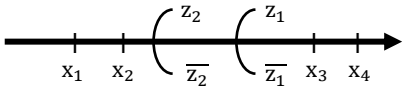
**c)** $z$ racine d'ordre $k$ de $P \Leftrightarrow \overline{z}$ racine d'ordre $k$ de $\overline{P}$.

**Démonstration a), b) c) :** clair en passant aux fonctions polynomiales sur $\mathbb{C}$.

**d)** $z$ racine d'ordre $k$ de $P \overset{def}{\Leftrightarrow} P(X) = (X - z)^k Q(X)$ avec $Q(z) \neq 0$.

$\Leftrightarrow$ d'après c), $\overline{P}(X) = (X - \overline{z})^k \overline{Q}(X)$ avec $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$.

**Illustration :** On se donne un polynôme $P \in \mathbb{R}[X]$.




**Théorème de factorisation dans $\mathbb{R}[X]$**

Soit $P \in \mathbb{R}[X]$ un polynôme de degré supérieur à 1.

- Soient $x_1, x_2, \ldots, x_k$ les racines réelles de $P$ d'ordres respectifs $n_1, n_2, \ldots, n_k$
- Soient $z_1, z_2, \ldots, z_q, \overline{z_1}, \overline{z_2}, \ldots, \overline{z_q}$ les racines non réelles de $P$ d'ordres respectifs $m_1, m_2, \ldots, m_q$.

Alors $P$ se factorise dans $\mathbb{R}[X]$ sous la forme :

$$P(X) = C(X - x_1)^{n_1} .. (X - x_k)^{n_k} (X^2 - 2\mathrm{Re}(z_1)X + |z_1|^2)^{m_1} .. \left(X^2 - 2\mathrm{Re}(z_q) + |z_q|^2\right)^{m_q}$$

**Démonstration :** On factorise $P$ dans $\mathbb{C}[X]$ :

$$P(X) = \prod_{i=1}^{k} (X - x_i)^{n_i} \prod_{j=1}^{q} \left[(X - z_j)(X - \overline{z_j})\right]^{m_q}$$

$$P(X) = \prod_{i=1}^{k} (X - x_i)^{n_i} \prod_{j=1}^{q} \left(X^2 - 2Re(z_j)X + |z_j|\right)^{m_q} \quad \rightarrow \text{ factorisation dans } \mathbb{R}[X].$$

**Exemple :** Décomposer $P(X) = X^n - 1$ dans $\mathbb{R}[X]$.

On a vu que les racines complexes de P sont de la forme $z_k = e^{\frac{2ik\pi}{n}}$ ; $0 \leq k \leq n - 1$.

$*$ **Si $n$ est pair**, on peut poser $n = 2p, p \in \mathbb{N}$

$z_0 = 1$, $z_p = -1$ sont les racines réelles de P.

$z_1, z_2, \ldots, z_{p-1}, \overline{z_1}, \overline{z_2}, \ldots, \overline{z_{p-1}}$ sont les racines non réelles de P, et on a :

$$P(X) = (X - 1)(X + 1) \prod_{k=1}^{p-1} \left(X^2 - 2\cos\left(\frac{k\pi}{p}\right)X + 1\right).$$

$*$ **Si $n$ est impair**, on peut poser $n = 2p + 1, p \in \mathbb{N}$

Il n'y a alors qu'une racine réelle : $z_0 = 1$, et on a :

$$P(X) = (X - 1) \prod_{k=1}^{p} \left(X^2 - 2\cos\left(\frac{2k\pi}{2p+1}\right)X + 1\right).$$

## 3. Notion de polynôme irréductible

**Définition :** Soient $P \in \mathbb{K}[X]$ avec $P$ non constant. On dit que $P$ est *irréductible* si $P = QR$ avec $Q$et $R \in \mathbb{K}[X]$, implique que $Q$ ou $R$ est constant.

$\Leftrightarrow$ Les seuls diviseurs de $P$ dans $\mathbb{K}[X]$ sont les constantes et les multiples de $P$.

**Attention** : la notion de polynôme irréductible *dépend* du corps $\mathbb{K}$.

Les polynômes irréductibles jouent le rôle des nombres premiers pour la factorisation des polynômes.

**Proposition :** Tout $P \in \mathbb{K}[X]$ non constant se factorise comme produit de polynômes irréductibles.

**Démonstration :** Si $P$ n'est pas irréductible, on le factorise jusqu'à obtenir des facteurs irréductibles.

**Théorème :**
**1)** Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.
$P(X) = aX + b$ avec $a \neq 0$.
**2)** Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 avec le discriminant négatif.
$P(X) = aX^2 + bX + c$ avec $a \neq 0$ et $\Delta = b^2 - 4ac < 0$.

**Démonstration : 1)** A faire en exercice.

**2)** Soit $P \in \mathbb{R}[X]$ un polynôme irréductible.
$*$ Si $P$ possède une racine réelle $x_0 \in \mathbb{R}$ alors $P$ s'écrit $P(X) = (X - x_0)Q(X)$ avec $Q$ constante car $P$ est irréductible. On a donc $P(X) = C(X - x_0)$ de degré 1.
$*$ Si $P$ n'a pas de racine réelle, d'après Alembert Gauss, $P$ possède au moins une racine complexe $z_0 \in \mathbb{C}$.
$\rightarrow P(\overline{z_0}) = \overline{P(z_0)} = 0 \rightarrow \overline{z_0}$ est une racine de $P$.

$\rightarrow P(X) = (X - z_0)(X - \overline{z_0})Q(X) = (X^2 - 2\mathrm{Re}(z_0)X + |z_0|^2)Q(X)$
Avec $\Delta = 4(\mathrm{Re}(z_0)^2 - |z_0|^2) = -4\,\mathrm{Im}(z_0) < 0$.

Comme $P$ est irréductible, $Q(X) = C$.

$\rightarrow P$ est de degré 2 sans racine réelle.

**Remarques :**
**1)** Les deux énoncés de la décomposition dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$ vus sont des cas particuliers du principe général énoncé ici.
**2)** Le problème est beaucoup plus difficile dans $\mathbb{Q}[X]$. Il y a des polynômes irréductibles de degré arbitrairement grand. Par exemple :
$P(X) = X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, mais il est réductible dans $\mathbb{R}[X]$. (Voir TD)