

## I. Ensemble des entiers naturels

### I.1. Existence de $\mathbb{N}$

Il existe un ensemble  $\mathbb{N}$  vérifiant les propriétés:

$\mathbb{N}$  est muni de deux opérations internes :  $+$  et  $\times$  vérifiant:  $+$  et  $\times$  sont

**associatives** :  $\forall (a, b, c) \in \mathbb{N}^3 \quad a + (b + c) = (a + b) + c \quad a(bc) = (ab)c$ ,

**commutatifs** :  $\forall (a, b) \in \mathbb{N}^2 \quad a + b = b + a \quad ab = ba$ ,

admettent un **élément neutre** (0 pour  $+$  et 1 pour  $\times$ ) :  $\forall a \in \mathbb{N} \quad a + 0 = 0 + a = a \quad a \times 1 = 1 \times a = a$ ,

$\times$  est **distributive** par rapport à  $+$  :  $\forall (a, b, c) \in \mathbb{N}^3 \quad a \times (b + c) = a \times b + a \times c$

$$(b + c) \times a = b \times a + c \times a,$$

tout élément est **régulier** pour  $+$  :  $\forall (a, b, c) \in \mathbb{N}^3 \quad a + b = a + c \implies b = c$ ,

tout élément non nul est régulier pour  $\times$  :  $\forall (a, b, c) \in \mathbb{N}^3 \quad a \neq 0 \quad ab = ac \implies b = c$ .

$\mathbb{N}$  est muni d'une **relation d'ordre total**  $\leq$ , compatible avec  $+$  :

$$\forall (a, b, c, d) \in \mathbb{N}^4 \quad (a \leq b \text{ et } c \leq d) \implies a + c \leq b + d$$

Tout sous-ensemble non vide de  $\mathbb{N}$  admet un plus petit élément.

Tout sous-ensemble non vide et majoré de  $\mathbb{N}$  admet un plus grand élément.

### I.2. Principe de récurrence

On veut montrer que  $\forall n \in \mathbb{N}$  la propriété  $P(n)$  est vraie

**récurrence simple** : on montre  $P(0)$  et pour un  $n \in \mathbb{N} \quad P(n) \implies P(n + 1)$

**récurrence forte** : on montre  $P(0)$  et pour un  $n \in \mathbb{N} \quad (\forall k \in \{0..n\} \quad P(k)) \implies P(n + 1)$

**récurrence double** : on montre  $P(0), P(1)$  et pour un  $n \in \mathbb{N} \quad P(n)$  et  $P(n + 1) \implies P(n + 2)$

### I.3. Nombres premiers

Un entier  $p$  est **premier** si  $p \geq 2$  et  $n$  a pour seuls diviseurs 1 et lui-même.

L'ensemble des nombres premiers est infini.

Tout entier  $n$  se décompose de manière unique à l'ordre près en produits de facteurs premiers:  $n = \prod_{k=1}^r p_i^{\alpha_i}$

avec  $p_i$  premier,  $\alpha_i \in \mathbb{N}^*$

### I.4. Division euclidienne

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}^* \quad \exists! (q, r) \in \mathbb{N}^2 \quad a = bq + r \text{ avec } 0 \leq r < b$$

$q$  est le quotient et  $r$  le reste de la division euclidienne de  $a$  par  $b$ .

### I.5. PGCD-PPCM

$(a, b) \in (\mathbb{N}^*)^2$ ,  $\text{pgcd}(a, b)$  est le plus grand diviseur commun à  $a$  et  $b$  noté  $a \wedge b$ ,

$\text{ppcm}(a, b)$  est le plus petit multiple commun à  $a$  et  $b$  noté  $a \vee b$ .

$$\text{On a } \forall (a, b, q) \in (\mathbb{N}^*)^3 \quad a \wedge b = (a - bq) \wedge b$$

On en déduit **l'algorithme d'Euclide** :  $(a, b) \in (\mathbb{N}^*)^2$  on pose  $r_0 = \max(a, b) \quad r_1 = \min(a, b)$

Pour  $i \in \mathbb{N}^*$ , si  $r_i \neq 0$ , on note  $r_{i+1}$  le reste de la division euclidienne de  $r_{i-1}$  par  $r_i$

L'algorithme s'arrête à un rang  $n + 1$  tel que  $r_{n+1} = 0$ . Le  $\text{pgcd}$  de  $(a, b)$  est le dernier reste  $r_n$  non nul

Les entiers naturels non nuls  $a$  et  $b$  sont **premiers entre eux** si  $a \wedge b = 1$

*EUCLIDE d'Alexandrie, grec, vers -330/-260 : œuvre monumentale en treize livres "Les éléments" : les livres I à IV sont consacrés la géométrie plane, les livres VII, VIII, IX, X à l'arithmétique (étude des entiers*



naturels, divisibilité, nombres premiers, nombres irrationnels nombres incommensurables ), les derniers livres sont consacrés aux aires et aux volumes des configurations usuelles du plan et de l'espace.

**Relation entre pgcd et ppcm :**  $(a, b) \in (\mathbb{N}^*)^2 \quad (a \wedge b)(a \vee b) = ab$

## II. Ensemble des entiers relatifs

### II.1. Existence de $\mathbb{Z}$

Il existe  $\mathbb{Z}$  ensemble des entiers relatifs contenant les éléments de  $\mathbb{N}$  et leurs opposés.

$(\mathbb{Z}, +)$  est un groupe commutatif :  $+$  est associative , commutative, admet 0 pour élément neutre et tout élément de  $\mathbb{Z}$  admet un opposé.

$(\mathbb{Z}, +, \times)$  est un anneau : de plus  $\times$  est associative , commutative, admet 1 pour élément neutre  $\times$  est **distributive** par rapport à  $+$  .

Tout sous-ensemble non vide minoré de  $\mathbb{Z}$  admet un plus petit élément.

Tout sous-ensemble non vide et majoré de  $\mathbb{Z}$  admet un plus grand élément.

$\mathbb{Z}$  est muni d'une relation d'ordre total  $\leq$  qui prolonge celle de  $\mathbb{N}$ .

### II.2. Division euclidienne

$\forall (a, b) \in \mathbb{Z} \times \mathbb{N}^* \quad \exists! (q, r) \in \mathbb{Z} \times \mathbb{N} \quad a = bq + r \text{ avec } 0 \leq r < b$   
 $q$  est le quotient et  $r$  le reste de la division euclidienne de  $a$  par  $b$ .

## III. Ensemble des décimaux, des relatifs

Il existe  $\mathbb{D}$  ensemble des décimaux, tout élément de  $\mathbb{D}$  s'écrit sous forme de fraction décimale,

ie  $\frac{a}{10^p} \quad a \in \mathbb{Z}, p \in \mathbb{N}$ .

Il existe  $\mathbb{Q}$  ensemble des relatifs, tout élément de  $\mathbb{Q}$  s'écrit sous la forme  $\frac{p}{q}$  ,  $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ .

$(\mathbb{Q}, +, \times)$  est un anneau commutatif tel que tout élément non nul admet un inverse rationnel, ie  $(\mathbb{Q}, +, \times)$  est un corps.

$\mathbb{Q}$  est muni d'une relation d'ordre total  $\leq$  qui prolonge celle de  $\mathbb{Z}$ .

## IV. Ensemble des réels

### IV.1. Existence de $\mathbb{R}$

Il existe  $\mathbb{R}$  ensemble des réels vérifiant:

$\mathbb{R}$  contient  $\mathbb{Q}$

$\mathbb{R}$  est muni d'une relation d'ordre total  $\leq$  prolongeant celle de  $\mathbb{Q}$  et compatible avec  $+$ .

$\mathbb{R}$  vérifie le **théorème de la borne supérieure**: tout sous-ensemble non vide de  $\mathbb{R}$  et majoré admet une borne supérieure.

(et  $\mathbb{R}$  vérifie le **théorème de la borne inférieure**: tout sous-ensemble de  $\mathbb{R}$  non vide et minoré admet une borne inférieure)

Un élément réel non rationnel s'appelle **irrationnel**.

Rappel sur la borne supérieure (et inférieure):

$$M = \sup \mathcal{A} \iff \begin{cases} \forall a \in \mathcal{A} & a \leq M \\ \forall \epsilon > 0 & \exists a \in \mathcal{A} \quad M - \epsilon < a \leq M \end{cases}$$

$$m = \inf \mathcal{A} \iff \begin{cases} \forall a \in \mathcal{A} & m \leq a \\ \forall \epsilon > 0 & \exists a \in \mathcal{A} \quad m \leq a < m + \epsilon \end{cases}$$



## IV.2. Valeur absolue

$$x \in \mathbb{R} \quad |x| = \sup(x, -x)$$

**Propriétés :**  $\forall (x, y) \in \mathbb{R}^2 \quad |xy| = |x||y|$

$$\forall (x, y) \in \mathbb{R}^2 \quad ||x| - |y|| \leq |x + y| \leq |x| + |y|$$

## IV.3. Partie entière

La **partie entière** du réel  $x$  est le plus grand entier (dans  $\mathbb{Z}$ ) inférieur ou égal à  $x$ , noté  $E(x)$  ou  $\lfloor x \rfloor$

$$\text{On a } \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

## IV.4. Intervalles de $\mathbb{R}$

$\mathcal{I}$  est un **intervalle** de  $\mathbb{R}$  si  $\forall (x, y) \in \mathcal{I}^2 \quad x < y \implies [x, y] \subset \mathcal{I}$

Tout intervalle non vide de  $\mathbb{R}$  contient au moins un rationnel et un irrationnel.

# V. Complexes

## V.1. Existence de $\mathbb{C}$

Il existe un corps  $(\mathbb{C}, +, \times)$  contenant  $\mathbb{R}$  dans lequel  $-1$  est un carré,  $-1 = i^2$  et  $\mathbb{C} = \{a + ib ; (a, b) \in \mathbb{R}^2\}$

$\mathbb{C}$  n'est pas totalement ordonné

## V.2. Partie réelle, partie imaginaire

Si  $z \in \mathbb{C} \quad z = a + ib \quad (a, b) \in \mathbb{R}^2 \quad \mathcal{R}e(z) = a$  est la **partie réelle** de  $z$  et  $\mathcal{I}m(z) = b$  est sa **partie imaginaire**

Si  $\mathcal{R}e(z) = 0$ , on dit que  $z$  est un **imaginaire pur** et on note  $z \in i\mathbb{R}$ .

Le **conjugué** de  $z$  est  $\bar{z} = a - ib$

**Propriétés :**  $z + \bar{z} = 2 \mathcal{R}e(z) \quad z - \bar{z} = 2i \mathcal{I}m(z)$

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$$

$$\bar{\bar{z}} = z \text{ (la conjugaison est involutive)} \quad \text{et si } z \neq 0 \quad \overline{\left(\frac{1}{z}\right)} = \frac{1}{\bar{z}}$$

$$z = \bar{z} \iff z \in \mathbb{R} \quad ; \quad z = -\bar{z} \iff z \in i\mathbb{R}$$

## V.3. Module

Si  $z \in \mathbb{C} \quad z = a + ib \quad (a, b) \in \mathbb{R}^2 \quad$  le **module** de  $z$  est  $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$

**Propriétés :**  $|z| = 0 \iff z = 0 \quad |z_1 z_2| = |z_1| |z_2| \quad \text{si } z \neq 0 \quad \left|\frac{1}{z}\right| = \frac{1}{|z|}$

**Inégalité triangulaire :**  $|z_1 + z_2| \leq |z_1| + |z_2|$

$$\text{et } |z_1 + z_2| = |z_1| + |z_2| \iff (z_1 = 0 \text{ ou } \frac{z_2}{z_1} \in \mathbb{R})$$

$$\text{On en déduit } ||z_1| - |z_2|| \leq |z_1 - z_2|$$

## V.4. Argument d'un complexe non nul

On note  $U$  l'ensemble des complexes de module 1.  $U$  est stable par produit et par passage à l'inverse.

Si  $z = a + ib \in U \quad$  l'**argument** de  $z$  est la mesure de l'angle  $(\vec{i}, \overrightarrow{OM})$  où  $M(a, b)$  est sur le cercle unité ( $M$  d'affixe  $z$ ) (argument défini à  $2\pi$  près)

Si  $z \in \mathbb{C}^*$  l'argument de  $z$  est l'argument de  $\frac{z}{|z|}$

d'où la **forme trigonométrique** de  $z \in \mathbb{C}^* \quad z = |z| e^{i\theta}$



**0 n'a pas d'argument**

**Propriétés :**  $(z_1, z_2) \in (\mathbb{C}^*)^2$   $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$  ;  $\arg\left(\frac{1}{z_2}\right) = -\arg(z_2)$

## V.5. Exponentielle complexe

Si  $t \in \mathbb{R}$  on note  $e^{it} = \cos(t) + i \sin(t)$

Si  $z \in \mathbb{C}$   $z = a + ib$   $(a, b) \in \mathbb{R}^2$  on note  $e^z = e^a e^{ib} = e^a (\cos(b) + i \sin(b))$

**Propriétés :**  $e^{z_1+z_2} = e^{z_1} e^{z_2}$   $(e^{z_1})^n = e^{nz_1}$

$|e^z| = e^{\operatorname{Re} z} = e^a$   $\arg(e^z) = \operatorname{Im}(z) = b$

$\forall (z, z') \in \mathbb{C}^2$   $e^z = e^{z'} \iff z - z' \in 2\pi\mathbb{Z}$

Les solutions de  $e^z = Z = re^{i\theta}$  ( $Z \neq 0$ ) sont  $z = \ln r + i(\theta + 2k\pi)$  ( $k \in \mathbb{Z}$ )

On peut définir les fonctions trigonométriques : si  $z \in \mathbb{C}$   $\cos(z) = \frac{e^{iz} + e^{-iz}}{2}$   $\sin(z) = \frac{e^{iz} - e^{-iz}}{2i}$   
 $\cosh(z) = \frac{e^z + e^{-z}}{2}$   $\sinh(z) = \frac{e^z - e^{-z}}{2}$

## V.6. Formules

**Formule de Moivre :**  $(\cos(\theta) + i \sin(\theta))^n = \cos(n\theta) + i \sin(n\theta)$

*DE MOIVRE Abraham 1667 Vitry-le-François 1754 Londres : Exilé à Londres en 1688 car protestant, précurseur du développement de la géométrie analytique et de la théorie des probabilités, il publie "The Doctrine of Chances" en 1718 et "Miscellanea Analytica" en 1730. De Moivre est connu pour avoir prédit le jour de sa mort : comptant qu'il dormait quinze minutes de plus chaque nuit et sommant cette progression arithmétique, il en déduit qu'il mourrait lorsque ses nuits feraient vingt-quatre heures.*

**Formules d'Euler :**  $\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}$   $\sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}$

**Transformation amplitude-phase :**  $(a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$   $a \cos \theta + b \sin \theta = \sqrt{a^2 + b^2} \cos(\theta - \alpha)$

où  $\cos(\alpha) = \frac{a}{\sqrt{a^2 + b^2}}$   $\sin(\alpha) = \frac{b}{\sqrt{a^2 + b^2}}$

**Formule :**  $e^{i\alpha} + e^{i\beta} = e^{i\frac{\alpha+\beta}{2}} 2 \cos\left(\frac{\alpha-\beta}{2}\right)$   $e^{i\alpha} - e^{i\beta} = e^{i\frac{\alpha+\beta}{2}} 2i \sin\left(\frac{\alpha-\beta}{2}\right)$

**Cas particulier :**  $1 + e^{i\beta} = e^{i\frac{\beta}{2}} 2 \cos\left(\frac{\beta}{2}\right)$   $1 - e^{i\beta} = e^{i\frac{\beta}{2}} 2i \sin\left(\frac{-\beta}{2}\right)$

**Théorème de relèvement :** Soit  $z \in \mathbb{C} \setminus \{-1\}$   $z = x + iy$  alors

$r = |z| = \sqrt{x^2 + y^2}$  et  $\theta = \arg(z) = 2 \arctan\left(\frac{y}{x+1}\right)$

## VI. Résolution d'équations

### VI.1. Racine $n^{\text{ième}}$

$Z \in \mathbb{C}^*$ , une racine  $n^{\text{ième}}$  de  $Z$  est un complexe  $z$  tel que  $z^n = Z$



$Z$  a  $n$  racines  $n^{ième}$

### Résolution :

Les racines  $n^{ième}$  de l'unité sont  $\exp\left(\frac{2ik\pi}{n}\right)$ ,  $k$  parcourant un intervalle de longueur  $n$

(par exemple  $0 \dots n-1$  ou  $1 \dots n$  ou un intervalle centré en 0)

On note  $U_n$  leur ensemble.

Pour  $Z \neq 1$ , ou on a une solution particulière  $z_0$ , les solutions sont alors  $z_0 \exp\left(\frac{2ik\pi}{n}\right)$ ,  $k$  parcourant un intervalle de longueur  $n$

sinon on écrit  $Z = r e^{i\theta}$  les solutions sont alors  $\sqrt[n]{r} \exp\left(i\frac{\theta}{n} + \frac{2ik\pi}{n}\right)$   $k$  parcourant un intervalle de longueur  $n$

## VI.2. Équation du deuxième degré

Soient  $(a, b, c)$  trois complexes ( $a \neq 0$ ), on considère l'équation  $az^2 + bz + c = 0$  de discriminant  $\Delta = b^2 - 4ac$

On écrit  $\Delta = \delta^2 = (u + iv)^2$  et on résout 
$$\begin{cases} u^2 - v^2 = \operatorname{Re}(\Delta) \\ 2uv = \operatorname{Im}(\Delta) \\ u^2 + v^2 = |\Delta| \end{cases}$$

Les racines sont alors  $\frac{-b + \delta}{2a}$  et  $\frac{-b - \delta}{2a}$

La somme des deux racines vaut  $-\frac{b}{a}$  et le produit des deux racines est  $\frac{c}{a}$

## VII. Applications géométriques des complexes

### VII.1. Affixe

On considère le plan affine euclidien  $\mathcal{P}$  muni d'un repère orthonormé  $(O, \vec{i}, \vec{j})$

L'application  $\mathcal{P} \rightarrow \mathbb{C}$

$M \begin{pmatrix} a \\ b \end{pmatrix} \mapsto z = a + ib$  est une bijection  $z$  est l'**affixe** du point  $M$  (ou du vecteur  $\vec{u} = a\vec{i} + b\vec{j}$ )

Soit  $r > 0$ ,  $\{z \in \mathbb{C}; |z - a| < r\}$  représente l'intérieur du disque de centre le point  $A$  d'affixe  $a$  de rayon  $r$  et  $|z - a| \leq r$  représente le disque de centre le point  $A$  d'affixe  $a$  de rayon  $r$

### Règles de calcul :

Le module de l'affixe correspond à la norme de  $\vec{u}$  ou la longueur du segment  $\|\overrightarrow{OM}\|$

L'argument de l'affixe correspond à l'angle  $(\vec{i}, \vec{u}) = (\vec{i}, \overrightarrow{OM})$

L'addition des complexes correspond à l'addition des vecteurs.

## VII.2. Propriétés géométriques

Les trois points  $A, B, C$  d'affixes respectives  $a, b, c$  sont alignés si et seulement si  $\frac{c-a}{b-a} \in \mathbb{R}$

$$\overrightarrow{AB} \perp \overrightarrow{AC} \iff \frac{c-a}{b-a} \in i\mathbb{R}$$

L'équation d'une droite en complexes est  $\bar{a}z + a\bar{z} + \gamma = 0$

L'équation d'un cercle en complexes est  $z\bar{z} - \bar{c}z - c\bar{z} + \gamma = 0$

L'ensemble des points  $M$  d'affixe  $z$  tels que  $\left| \frac{z-a}{z-b} \right| = k$  ( $a, b$  complexes fixés  $k > 0$ ) est un cercle si  $k \neq 1$  ( et la médiatrice de  $[A, B]$  si  $k = 1$ )

L'ensemble des points  $M$  d'affixe  $z$  tels que  $\arg\left(\frac{z-a}{z-b}\right) = k$  modulo  $\pi$  ( $a, b$  complexes fixés) est un cercle

### **VII.3. Transformations géométriques**

La transformation  $z \mapsto kz$  correspond à une homothétie de rapport  $k$  de centre  $O$ .

La transformation  $z \mapsto e^{i\theta}z$  correspond à une rotation de centre  $O$  et d'angle  $\theta$ .

La transformation  $z \mapsto \bar{z}$  correspond à la symétrie par rapport à  $(Ox)$ .

La transformation  $z \mapsto z + b$  ( $b \in \mathbb{C}$ ) correspond à une translation de vecteur d'affixe  $b$



## I. Définition . Premières propriétés

$\mathbb{K} = \mathbb{R}, \mathbb{C}$

Un polynôme  $P$  à coefficients dans  $\mathbb{K}$  est une suite presque nulle  $(a_n)_{n \in \mathbb{N}}$  d'éléments de  $\mathbb{K}$   
(ie  $\exists N \in \mathbb{N} \quad \forall n > N \quad a_n = 0$ )

Si  $P = (a_n)_n$  et  $Q = (b_n)_n$  on définit deux lois internes  $+$  et  $\times$  par  $P + Q = (a_n + b_n)_n$  et  $PQ = (c_n)_n$

$$\text{où } c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k=0}^n a_{n-k} b_k = \sum_{(i,j), i+j=n} a_i b_j$$

et une loi  $\cdot$  externe à domaine d'opérateurs  $\mathbb{K}$  par  $\alpha \in \mathbb{K} \quad \alpha P = (\alpha a_n)_n$

Muni de ces lois, l'ensemble des polynômes noté  $\mathbb{K}[X]$  est une algèbre commutative d'élément neutre  $(1, 0, 0, 0, \dots)$

$$\text{on note } X = (0, 1, 0, 0, \dots) \text{ alors } P = \sum_{k \geq 0} a_k X^k = \sum_{k=0}^N a_k X^k$$

$P \in \mathbb{K}[X] \quad P \neq 0 \quad (n = d^\circ P \text{ degré de } P \text{ si } n \text{ est le plus grand entier tel que } a_n \neq 0) \text{ alors } a_n \text{ est le coefficient dominant de } P \text{ (si } a_n = 1 \text{ on dit que } P \text{ est unitaire) et } a_n X^n \text{ est le terme dominant de } P$

Par convention  $d^\circ 0 = -\infty$

$$\begin{aligned} \text{On a } \forall (P, Q) \in \mathbb{K}[X]^2 \quad d^\circ(P + Q) &\leq \max(d^\circ P, d^\circ Q) \\ d^\circ(PQ) &\leq d^\circ P + d^\circ Q \\ d^\circ(\lambda P) &= \begin{cases} d^\circ P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases} \end{aligned}$$

$\mathbb{K}_n[X] = \{ P \in \mathbb{K}[X] ; d^\circ P \leq n \}$  est un sev de  $\mathbb{K}[X]$  de dimension  $n + 1$  dont une base est  $(X^k)_{0 \leq k \leq n}$

## II. Algorithme d'Hörner

$$\text{Si } P = \sum_{k=0}^n a_k X^k \text{ alors } P(\alpha) = a_0 + \alpha(a_1 + \alpha(a_2 + \alpha(\dots + \alpha(a_{n-1} + \alpha a_n))))$$

*HÖRNER William 1786 Bristol - 1837 Bath : Algèbriste, on lui doit divers algorithmes. Il s'investit aussi en optique avec son zootrope , petite machine d'animation montrant les différentes phases du mouvement, d'un animal par exemple*

## III. Division euclidienne

Soient  $(A, B) \in \mathbb{K}[X]^2 \quad A \neq 0$ ,  $A$  divise  $B$  (noté  $A/B$ ) si  $\exists P \in \mathbb{K}[X] \quad B = AP$ ,  $B$  est aussi appelé **multiple** de  $A$ .

Si  $A/B$  et  $B/A$  ( $A$  et  $B$  polynômes non nuls) alors  $A$  et  $B$  sont **associés** (et  $\exists \alpha \in \mathbb{K}^* \quad B = \alpha A$ )

**théorème de la division euclidienne :**  $\forall (P, A) \in \mathbb{K}[X]^2, \quad A \neq 0, \quad \exists ! (Q, R) \in \mathbb{K}[X]^2 \quad P = AQ + R$   
avec  $d^\circ R < d^\circ A$

$Q$  (respectivement  $R$ ) est le quotient (respectivement reste) de la division euclidienne de  $P$  par  $A$



## IV. Dérivation

Si  $P = \sum_{k=0}^n a_k X^k$  alors on définit le polynôme dérivé de  $P$  par  $P' = \sum_{k=1}^n k a_k X^{k-1}$

et par récurrence  $P^{(r)} = (P^{(r-1)})'$  si  $r \in \mathbb{N}^*$

**Propriétés :**  $P \mapsto P^{(r)}$  est une application linéaire

$$\forall (P, Q) \in \mathbb{K}[X]^2 \quad (PQ)' = P'Q + PQ'$$

$$\text{(formule de Leibniz)} \quad \forall (P, Q) \in \mathbb{K}[X]^2 \quad (PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$$

*LEIBNIZ Gottfried 1646 Leipzig - 1716 Hanovre : Juriste de formation, diplomate et non enseignant, Leibniz est principalement reconnu comme l'un des plus éminents philosophes et savants du 17ème siècle. Leibnizcrivait en latin: methodus differentialis, Analysis situs.. Il publie la majorité de ses travaux dans la revue Acta eruditorum (Actes des érudits) : inventeur du calcul différentiel et intégral : Nova methodus pro maximis et minimis, itemque Tangentibus.*

$$\text{composé: } \forall (P, Q) \in \mathbb{K}[X]^2 \quad (PoQ)' = Q'(P'oQ)$$

## V. Fonction polynôme

Si  $P = \sum_{k=0}^n a_k X^k$  alors la fonction polynôme associée à  $P$  est  $x \mapsto \sum_{k=0}^n a_k x^k$ , notée  $P(x)$

**théorème :** Le reste de la division euclidienne de  $P$  par  $X - a$  est  $P(a)$

et  $X - a \mid P$  si et seulement si  $P(a) = 0$

$P$  polynôme de degré  $n$ , alors  $P$  a au plus  $n$  zéros distincts.

Deux polynômes de  $\mathbb{K}_n[X]$  coïncidant en  $n + 1$  points distincts sont égaux .

## VI. Formule de Taylor-Lagrange

$$P \in \mathbb{K}[X], \quad d^n P = n! \quad a \in \mathbb{K}$$

$$P(X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X - a)^k \quad \text{ou} \quad P(X + a) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} X^k$$

*TAYLOR Brook 1685 Edmonton - 1731 Londres : Formé aux mathématiques par John Machin et admirateur de Newton, Taylor ajoute aux mathématiques une nouvelle branche appelée calcul de différences finies, il invente l'intégration par parties, et développe en série les fonctions dans Methodus incrementorum directa et inversa. Le calcul du reste n'est pas étudié rigoureusement par Taylor, c'est pourquoi, suite à des travaux ultérieurs, le développement de Taylor est rebaptisé : formule de Taylor-Lagrange, Taylor-Young, Taylor-Laplace.*

## VII. Ordre de multiplicité

$a \in \mathbb{K}$ ,  $a$  est zéro de  $P$  d'ordre de multiplicité  $m$  si  $(X - a)^m \mid P$  et  $(X - a)^{m+1}$  ne divise pas  $P$

**théorème :**  $a \in \mathbb{K}$   $a$  est zéro de  $P$  d'ordre de multiplicité  $m$  si et seulement si



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

**théorème :**  $a \in \mathbb{K}$       $a$  est zéro de  $P$  d'ordre de multiplicité  $\geq m$  si et seulement si  
 $P(a)=0$  ,  $P'(a)=0$  ,...,  $P^{(m-1)}(a)=0$

## VIII. Polynômes irréductibles

**définition :**  $P \in \mathbb{K}[X]$  est irréductible (ou premier) si  $P$  est non constant et les seuls diviseurs de  $P$  sont  $\alpha$  et  $\alpha P$  ,  $\alpha \in \mathbb{K}^*$

**théorème de d'Alembert-Gauss :** Tout polynôme non constant de  $\mathbb{C}[X]$  admet une racine complexe

*Jean le Rond d'ALEMBERT 1717 Paris - 1783 Paris : À la suite de la publication de divers mémoires sur le calcul intégral, sur la réfraction des corps solides, d'Alembert entre à l'Académie des sciences à 24 ans. Il s'intéresse à la dynamique, à la mécanique des fluides, la mécanique céleste, les cordes vibrantes, la théorie des vents et marées. Il introduit les équations aux dérivées partielles du second ordre. On lui doit le célèbre principe de la quantité de mouvement, dit principe de d'Alembert dans son "Traité de dynamique" pouvant s'exprimer ainsi : La quantité de mouvement d'un corps ou d'un système de points matériels isolé est constante. Dans l'Encyclopédie, d'Alembert propose le théorème de d'Alembert dont Gauss en donnera une preuve plus rigoureuse.*

*GAUSS Karl 1777 Brunschwic - 1855 Göttingen : mathématicien (arithmétique, géométrie différentielle), physicien (importants travaux et publications en électricité, optique et magnétisme, théorie du potentiel), Gauss est aussi un astronome réputé. Il tablit en 1801 l'orbite de Cérès, en utilisant la méthode des moindres carrés.*

Sur  $\mathbb{C}[X]$ , les polynômes irréductibles sont les polynômes de degré 1

Sur  $\mathbb{R}[X]$ , les polynômes irréductibles sont les polynômes de degré 1 et ceux de degré 2 à discriminant strictement négatif

Donc sur  $\mathbb{C}[X]$ , tout polynôme  $P$  non constant se décompose de manière unique sous la forme

$$P(X) = \lambda \prod_{k=1}^r (X - a_k)^{\alpha_k} \quad \text{avec } \lambda \in \mathbb{C}^*, a_k \in \mathbb{C}, \alpha_k \in \mathbb{N}^*$$

et sur  $\mathbb{R}[X]$ , tout polynôme  $P$  non constant se décompose de manière unique sous la forme

$$P(X) = \lambda \prod_{k=1}^r (X - a_k)^{\alpha_k} \prod_{k=1}^s (X^2 + p_k X + q_k)^{\beta_k}$$

avec  $\lambda \in \mathbb{R}^*$  ,  $a_k \in \mathbb{R}$ ,  $\alpha_k \in \mathbb{N}^*$  ,  $(p_k, q_k) \in \mathbb{R}^2$  avec  $p_k^2 - 4q_k < 0$  ,  $\beta_k \in \mathbb{N}^*$

Exemple à connaître :

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

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



## IX. Somme et produit des racines

**définition :**  $P$  est un polynôme **scindé** si  $P$  se décompose sous la forme  $P = \lambda (X - a_1)(X - a_2) \cdots (X - a_n)$

**Somme et produit des racines d'un polynôme scindé :**

$P$  scindé de degré  $n$   $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$

Soient  $\alpha_1, \alpha_2, \dots, \alpha_n$  les racines de  $P$  alors 
$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n} \\ \alpha_1 \alpha_2 \cdots \alpha_n = \frac{(-1)^n a_0}{a_n} \end{cases}$$

## X. Fractions rationnelles

**définition :** Une fraction rationnelle est  $\frac{P}{Q}, (P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$

On note  $\mathbb{K}(X)$  l'ensemble des fractions rationnelles.

Un zéro de  $Q$  s'appelle un **pôle** de la fraction rationnelle  $\frac{P}{Q}$ .

**décomposition en éléments simples dans le cas des pôles simples :** Soit  $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$ .

On suppose  $Q$  scindé à racines simples, ie  $Q(X) = a_n \prod_{k=1}^n (X - \lambda_k)$  avec  $\lambda_i \neq \lambda_j$  si  $i \neq j$

alors  $\exists ! E \in \mathbb{K}[X] \quad \exists ! (a_1, \dots, a_n) \in \mathbb{K}^n \quad \frac{P}{Q} = E + \sum_{k=1}^n \frac{a_k}{X - \lambda_k}$

$E$  s'appelle la partie entière de la fraction, c'est le quotient de la division euclidienne de  $P$  par  $Q$ .

**Propriété :**  $a_k = \lim_{x \rightarrow \lambda_k} (x - \lambda_k) \frac{P(x)}{Q(x)}$

**Utilisation :** 1. Recherche de primitives  
2. Calcul de dérivées successives

**décomposition en éléments simples dans le cas des pôles doubles :** Soit  $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$ .

On suppose , ie  $Q(X) = (X - \lambda)^2 Q_1(X)$  avec  $Q_1(\lambda) \neq 0$

alors  $\frac{P}{Q} = E + \frac{u}{X - \lambda} + \frac{v}{(X - \lambda)^2} + \frac{P_1}{Q_1} \quad (u, v) \in \mathbb{K}^2$

**Propriété :**  $v = \lim_{x \rightarrow \lambda} (x - \lambda)^2 \frac{P(x)}{Q(x)}$

et on détermine  $u$  avec une valeur particulière de  $x$  (non pôle de  $Q$ )

**décomposition en éléments simples , cas réel :** Soit  $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$ .

On suppose  $Q(X) = (X^2 + pX + q)Q_1(X)$  avec  $p^2 - 4q < 0$  et  $Q_1$  ne s'annule pas en les racines complexes de  $X^2 + pX + q$

alors  $\frac{P}{Q} = E + \frac{uX + v}{X^2 + pX + q} + \frac{P_1}{Q_1} \quad (u, v) \in \mathbb{R}^2$

**Propriété :** Soit  $z$  une racine complexe de  $X^2 + pX + q$

$uz + v = \lim_{x \rightarrow z} (x - z) \frac{P(x)}{Q(x)}$  et on identifie partie réelle et partie imaginaire.