Algèbre 1 Info (MAT1074L) L1 Maths-Info 2025-2026

Léon Matar Tine [1]

Automne 2025

1. Université Claude Bernard Lyon 1

1 Chapitre 1 : Calculs algébriques

- Rappel sur l'ensemble des nombres réels
  - Relation d'ordre sur $\mathbb{R}$
  - Intervalle de $\mathbb{R}$
  - Valeur absolue
  - Notion de Majorant, Minorant, Maximum, Minimum
- Les entiers naturels et les entiers relatifs
  - L'ensemble des entiers naturels $\mathbb{N}$
  - Opération d'addition et de multiplication sur $\mathbb{N}$ et $\mathbb{Z}$
- Rappel sur les fractions et les opérations sur les fractions
  - Opérations sur les fractions
- Règles sur les puissances
- Sommes et produits de familles finies de nombres réels
  - Définitions et propriétés élémentaires
- Techniques classiques de calculs algébriques
  - Sommes et produits télescopiques
  - Changement d'indice
  - Regroupement de termes
- Factorielle et coefficients binomiaux
  - Factorielle
  - Coefficients binomiaux

- Différents modes de démonstration
  - Raisonnement par hypothèse auxiliaire
  - Raisonnement par l'absurde
  - Raisonnement par contraposée
  - Raisonnement par contre exemple
  - Raisonnement par récurrence

4. Chapitre 4 : Applications
   - Image directe et image réciproque
   - Injection
   - Surjection
   - Bijection
   - La composition d'application
5. Chapitre 5 : Nombres complexes
   - Nombres complexes : forme algébrique
     - Lien entre $\mathbb{R}^2$ et $\mathbb{C}$
     - Partie réelle, partie imaginaire et conjugué
     - Calculs sur les complexes
   - Nombres complexes : forme géométrique
     - Image d'un complexe, affixe d'un vecteur et d'un point
     - Interprétation géométrique
     - Module

- Interprétation géométrique du module
- Racines carrées et équations du second degré
- Théorème fondamental de l'algèbre
- Argument et trigonométrie
- Formule de Moivre et notation exponentielle
- Formule de Moivre et notation exponentielle
- Racines nièmes d'un complexe
- Quelques applications trigonométriques
- Formules de duplication de l'argument

- Nombres complexes en géométrie
  - Homothétie, interprétation de $z \to az + b$, $a \neq 0$
  - Rotation, interprétation de $z \mapsto az + b$, avec $|a| = 1$

6 Chapitre 6 : Arithmétique

- Nombres premiers
- Division Euclidienne
- PGCD-PPCM
- Algorithme d'Euclide
- Identité et théorème de Bézout
- Théorème de Gauss et décomposition en facteurs premiers
- Congruence
- Bases

- Petit théorème de Fermat et Théorème des restes chinois

7. Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$
   - Définition de polynômes à coefficients réels ou complexes
   - Applications
   - Division Euclidienne
   - Pgcd, ppcm
     - Pgcd
     - Ppcm
   - Polynômes irréductibles
   - Racines des polynômes
   - Formule de Taylor pour les polynômes de $\mathbb{C}[X]$
     - Formule de Taylor

Chapitre 1 : Calculs algébriques

Rappel sur l'ensemble des nombres réels

Comme abordé au Collège puis au Lycée, l'ensemble des nombres réels est représenté en mathématique par le symbole $\mathbb{R}$.
Il existe dans $\mathbb{R}$ un ordre naturel que l'on note "$\leq$" entre les nombres et qui vérifie les trois propriétés fondamentales suivantes :

1. Pour tout $x \in \mathbb{R}$, $x \leq x$ (Réflexivité)
2. Pour tout $x, y, z \in \mathbb{R}$, si $x \leq y$ et $y \leq z$ alors $x \leq z$. (Transitivité).
3. Pour tout $x, y \in \mathbb{R}$, si $x \leq y$ et $y \leq x$ alors $x = y$. (Antisymétrie).

Avec cette relation d'ordre, il existe ce que l'on appelle l'ordre strict sur $\mathbb{R}$, noté "$<$" où $x < y$ si "$x \leq y$ et $x \neq y$". Cette ordre strict n'est ni réflexif ni antisymétrique.

Intervalle de $\mathbb{R}$

La relation d'ordre "$\leq$" dans $\mathbb{R}$ permet de définir les intervalles.

Definition

Soient a et b deux réels, tels que $a < b$. Un intervalle de $\mathbb{R}$ est un ensemble de la forme suivante :

- $[a, b] = \{x \in \mathbb{R}, a \leq x \leq b\}$
- $[a, b[= \{x \in \mathbb{R}, a \leq x < b\}$
- $]a, b] = \{x \in \mathbb{R}, a < x \leq b\}$
- $]a, b[= \{x \in \mathbb{R}, a < x < b\}$
- $]-\infty, a] = \{x \in \mathbb{R}, x \leq a\}$
- $]-\infty, a[= \{x \in \mathbb{R}, x < a\}$
- $]a, +\infty[= \{x \in \mathbb{R}, x > a\}$
- $[a, +\infty[= \{x \in \mathbb{R}, x \geq a\}$

Les intervalles suivants $[a, b]$; $[a, +\infty[$ et $]-\infty, b]$ sont dit fermés.
Les intervalles $]a, b[$; $]a, +\infty[$ et $]-\infty, b[$ sont dits ouverts.
Les intervalles $[a, b[$ et $]a, b]$ ne sont ni ouverts ni fermés.

Intervalle de $\mathbb{R}$

Proposition

Soient $x, y, z, t \in \mathbb{R}$.

1. *Si* $x \leq z$ *et* $y \leq t$ *alors* $x + y \leq z + t$.
2. *Si* $0 \leq x \leq y$ *et* $0 \leq z \leq t$ *alors* $0 \leq xz \leq yt$.
3. *On a* $x \leq y$ *si et seulement si* $-x \geq -y$.
4. *Si* $x \leq y$ *et* $z \leq 0$ *alors* $xz \geq yz$.

Valeur absolue

Definition

Soit $x \in \mathbb{R}$. On définit la valeur absolue de x, notée $|x|$, par :

$$|x| = \begin{cases} x \text{ si } & x \geq 0 \\ -x \text{ si } & x < 0 \end{cases}$$

Exemple

$|-1| = 1$; $|0| = 0$; $|x+1| = x+1$ *si* $x \geq -1$ *et* $|x+1| = -x-1$ *si* $x < -1$.

Propriété

- *Pour tout* $x \in \mathbb{R}$, *on a* $|x| \geq 0$.
- *Pour tout* $x \in \mathbb{R}$, *on a* $|x| = |-x|$
- $|x| = 0$ *si et seulement si* $x = 0$.
- *Pour tout* $x, y \in \mathbb{R}$, $|xy| = |x||y|$.
- *Pour tout* $x \in \mathbb{R}$ *et* $a \geq 0$, $|x| \leq a$ *équivaut à* $-a \leq x \leq a$.

Valeur absolue

Théorème (Inégalités triangulaires)

a) $|x + y| \leq |x| + |y|$

b) $\Big||x| - |y|\Big| \leq |x - y|$.

Notion de Majorant, Minorant, Maximum, Minimum

Definition (Majorant, Minorant)

Soit A une partie composée de nombres réels. On dit que A est :

- majorée s'il existe un réel M tel que $x \leq M$ pour tout $x \in A$. On dit que M est un majorant de A
- minorée s'il existe un réel m tel que $m \leq x$ pour tout $x \in A$. On dit que m est un minorant de A
- bornée si A est à la fois majorée et minorée

Exemple

L'intervalle $]16, 17]$ *est majoré par 17 et minoré par 10 par exemple.*

Notion de Majorant, Minorant, Maximum, Minimum

Remarque

- *Une partie majorée (resp. minorée) n'admet pas un unique majorant (resp. minorant). Elle en a une infinité.*
- *Les intervalles (sauf* $]-\infty,+\infty[=\mathbb{R}$*) sont des parties de* $\mathbb{R}$ *majorées ou minorées.*

Definition (Minimum, Maximum)

Soient A une parties de $\mathbb{R}$ et m et M deu nombres réels

- si $m \in A$ et m est un minorant de A, on dit que m est le minimun de A, noté $min(A)$
- si $M \in A$ et M est un majorant de A, on dit que M est le maximun de A, noté $max(A)$.

Notion de Majorant, Minorant, Maximum, Minimum

Exemple

- *l'intervalle* $]-1,2]$ *admet* 2 *comme maximum*
- *l'intervalle* $]-1,2[$ *est borné mais n'admet ni maximum ni minimum.*

Exercices d'application :

1. Est-ce que $[-\pi,\pi]$ admet un maximum ? un minimum ?
2. Donner l'ensemble des majorants des parties $A =]0,2[$ et $B =]-1,2]$.
3. Mettre sous forme d'intervalle les ensembles $\{x \in \mathbb{R},\ |x-1| \leq 2\}$ et $\{x \in \mathbb{R},\ |3x-4| \leq 1\}$.
4. Mettre l'intervalle $]-7,2[$ sous forme d'un ensemble utilisant une valeur absolue.

L'ensemble des entiers naturels $\mathbb{N}$

La construction de l'ensemble $\mathbb{N}$ des entiers naturels a été formalisée pour la première fois au 19ème siècle par le mathématicien italien Giuseppe Peano et le mathématiciens allemand Richard Dedekind. Cette construction dépasse le cadre de ce cours de L1 où nous nous contenterons d'admettre l'existence de $\mathbb{N}$ et supposons qu'il vérifie les règles suivantes :

1. $\mathbb{N}$ est non vide.
2. $\mathbb{N}$ est totalement ordonné : pour tout $i, j \in \mathbb{N}$, on a $i \leq j$ ou $j \leq i$.
3. Toute partie non vide de $\mathbb{N}$ possède un plus petit élément : si A est une partie de $\mathbb{N}$ non vide, alors il existe a appartenant à A tel que pour tout i appartenant à A, $a \leq i$.
4. Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.

L'ensemble des entiers naturels $\mathbb{N}$

Propriété

- *L'ensemble* $\mathbb{N}$ *possède un plus petit élément, noté* 0*.*
- $\mathbb{N}\backslash\{0\}$*, l'ensemble des entiers naturels privé de* 0*, possède un plus petit élément, noté* 1*.*

On peut ainsi nommer les entiers successifs :

1. pour tout $n \in \mathbb{N}$, la partie $\{p \in \mathbb{N}, p > n\}$ possède un plus petit élément, appelé successeur de n et noté $n+1$.
2. pour tout $n \in \mathbb{N}$, la partie $\{p \in \mathbb{N}, p < n\}$ possède un plus grand élément, appelé prédécesseur de n et noté $n-1$.

Ainsi $\mathbb{N} = \{0, 1, 2, \cdots\}$ est l'ensemble des nombres entiers naturels.
À partir de l'ensemble $\mathbb{N}$, on peut définir l'ensemble des entiers relatifs noté $\mathbb{Z}$, comme étant les entiers naturels et leurs opposés. Ainsi $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$.
En d'autres termes, un nombre est appelé entier relatif si c'est un entier naturel ou si son opposé est un entier naturel.

L'ensemble des entiers naturels $\mathbb{N}$

Remarque

Un entier naturel est donc un entier relatif. On dit que $\mathbb{N}$ est inclus dans $\mathbb{Z}$, ce que l'on note $\mathbb{N} \subset \mathbb{Z}$.

Opération d'addition et de multiplication sur $\mathbb{N}$ et $\mathbb{Z}$

Pour tout a, b et c dans $\mathbb{N}$ ou $\mathbb{Z}$ on a :

- $(a + b) + c = a + (b + c)$
- $(a * b) * c = a * (b * c)$

Il s'agit de l'associativité de l'addition et de la multiplication

- $a + 0 = 0 + a = a$
- $a * 1 = 1 * a = a$

0 est l'élément neutre de l'addition et 1 celui de la multiplication.

Opération d'addition et de multiplication sur $\mathbb{N}$ et $\mathbb{Z}$

- $a + b = b + a$
- $a * b = b * a$

Il s'agit de la commutativité de l'addition et de la multiplication

- $(a + b) * c = a * c + b * c$
- $a * (b + c) = a * b + a * c$

Il s'agit de la distributivité de l'addition par rapport à la multiplication et de la multiplication par rapport à l'addition.

- Pour tout $a \in \mathbb{Z}$, il existe un unique $a' \in \mathbb{Z}$ tel que $a + a' = a' + a = 0$. On note cet élément a' par $-a$ (symétrie ou opposé).

Rappel sur les fractions et les opérations sur les fractions

Definition

Une fraction est un nombre qui s'écrit sous la forme $\frac{a}{b}$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

On dit que deux fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ sont égaux si et seulement si $ab' = a'b$.

Propriété (Simplification)

Pour tout $a \in \mathbb{Z}$, b et m appartenant à $\mathbb{Z}^*$ alors $\frac{am}{bm} = \frac{a}{b}$.

Opérations sur les fractions

- Pour deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ on définit la somme par la formule $\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$
- Pour deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ on définit le produit par la formule $\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$.

Definition

L'ensemble des fractions, c'est-à-dire des nombres pouvant s'écrire sous la forme $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, constitue l'ensemble des nombres rationnels, noté $\mathbb{Q}$ en mathématique.

Règles sur les puissances

Definition

Soient a un nombre réel non nul et m un entier strictement positif. On définit $a^m = a \times a \times a \times \cdots \times a$ pris $m-$fois

Propriété

Pour deux entiers strictement positifs m et n on a :

- $a^m \times a^n = \underbrace{a \times a \times \cdots \times a}_{m-fois} \times \underbrace{a \times a \times \cdots \times a}_{n-fois} = a^{m+n}$.
- $(a^m)^n = \underbrace{\underbrace{a \times \cdots \times a}_{m-fois} \times \cdots \times \underbrace{a \times \cdots \times a}_{m-fois}}_{n-fois} = \underbrace{a \times \cdots \times a}_{mn-fois} = a^{mn}$
- $a^0 = 1$
- *Pour $m \in \mathbb{N}$, on peut définir a^{-m}, pour tout réel a non nul, par* $a^{-m} = \dfrac{1}{a^m}$.

Règles sur les puissances

Ainsi, on peut généraliser les formules précédentes dans le cas où m et n sont dans $\mathbb{Z}$.
Pour deux nombres réels a et b non nuls et $m \in \mathbb{Z}$, on a aussi $(a \times b)^m = a^m \times b^m$.
Généralisation :

- Soient $a \neq 0$ un nombre réel, m un entier relatif et n un entier strictement positif. Si $a > 0$ on définit $a^{\frac{m}{n}} = \sqrt[n]{a^m}$.
- Pour a et b deux réels strictement positifs et pour tous $x, y \in \mathbb{Q}$ on a : $a^x a^y = a^{x+y}$; $(a^x)^y = a^{xy}$; $(ab)^x = a^x b^x$.

Définitions et propriétés élémentaires

Definition (Symbole $\sum$ et $\prod$)

Soit I un ensemble fini non vide et $(a_i)_{i\in I}$ une famille de nombres réels. On note :

- $\sum_{i\in I} a_i$ la somme des éléments de la famille $(a_i)_{i\in I}$.
- $\prod_{i\in I} a_i$ le produit des éléments de la famille $(a_i)_{i\in I}$.

Remarque

Par convention, si $I = \emptyset$: $\sum_{i\in I} a_i = 0$ *et* $\prod_{i\in I} a_i = 1$.

Cas fondamental : Si $I = [\![m, n]\!]$ avec $m, n \in \mathbb{Z}$ et $m \leq n$:

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \cdots + a_n \quad \text{et} \quad \prod_{i=m}^{n} a_i = a_m \times a_{m+1} \times \cdots \times a_n.$$

Remarque

L'indice "i" ne sert qu'à compter c'est la raison pour laquelle

$$\sum_{i=1}^{n} 3i + 2 = \sum_{k=1}^{n} 3k + 2 = \sum_{s=1}^{n} 3s + 2.$$

Définitions et propriétés élémentaires

Exemple

1. *Soit* $n \in \mathbb{N}^*$; $\sum_{k=1}^{n} 28 = \underbrace{28 + 28 + \cdots + 28}_{n-fois} = 28n$
2. $\sum_{k=0}^{n} 28 = \underbrace{28 + 28 + \cdots + 28}_{(n+1)-fois} = 28(n+1)$
3. *somme des n premiers naturels :*
   $$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$
4. *somme des carrés des n premiers entiers :*
   $$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$
5. *somme géométrique : pour q réel et* $q \neq 1$ *on a*
   $$\sum_{k=0}^{n} q^k = 1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q}$$

Définitions et propriétés élémentaires

Plus généralement, si $m, n \in \mathbb{Z}$ avec $m \leq n$ on a

$$\sum_{k=m}^{n} q^k = q^m \frac{(1 - q^{n+1-m})}{1 - q}.$$

La preuve de ce résultat découle du raisonnement suivant : On note par $S_{m,n}$ cette somme. Ainsi on écrit d'une part

$$S_{m,n} = q^m + q^{m+1} + q^{m+2} + \cdots + q^n$$
$$q \times S_{m,n} = q^{m+1} + q^{m+2} + \cdots + q^n + q^{n+1}$$

En faisant la différence des deux lignes précédentes on trouve :

$$S_{m,n} - q \times S_{m,n} = q^m - q^{n+1} \Longrightarrow S_{m,n}(1 - q) = q^m - q^{n+1}$$

$$\Longrightarrow S_{m,n} = \frac{q^m - q^{n+1}}{1 - q}.$$

Définitions et propriétés élémentaires

Propriété (Linéarité de la somme)

Soit I, un ensemble fini, $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ deux familles de nombres. On a :

1. $\sum_{i\in I}(a_i + b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i$
2. *Pour tout réel λ,* $\sum_{i\in I} \lambda a_i = \lambda \sum_{i\in I} a_i$.

Exemple

Soit $n \geq 5$ un entier et x, y deux réels. Nommer et calculer la somme :

- $\sum_{k=0}^{n}(3k-2x) = \sum_{k=0}^{n} 3k - \sum_{k=0}^{n} 2x = 3\sum_{k=0}^{n} k - (n+1)2x =$
  $3\frac{n(n+1)}{2} - (n+1)2x = \frac{(n+1)(3n-4x)}{2}$
- $\sum_{s=0}^{n^2} x(s+y) = x\sum_{s=0}^{n^2}(s+y) = x\sum_{s=0}^{n^2} s + x\sum_{s=0}^{n^2} y =$
  $x\sum_{s=0}^{n^2} s + (n^2+1)xy = x\frac{(n^2+1)n^2}{2} + (n^2+1)xy = \frac{x}{2}(n^2+1)(n^2+2y).$
- $\sum_{i=4}^{n-1}(2^i+3) = \sum_{i=4}^{n-1} 2^i + \sum_{i=4}^{n-1} 3 = \sum_{i=4}^{n-1} 2^i + 3(n-4) =$
  $2^4\frac{1-2^{n-4}}{1-2} + 3(n-4) = \frac{2^4-2^n}{-1} + 3(n-4) = 2^n + 3n - 28$

Définitions et propriétés élémentaires

Propriété (Pour le produit)

1. *Pour tout λ réel, $\prod_{i \in I} \lambda = \lambda^n$ où n est le nombre d'élements de I.*
2. $\prod_{i \in I} a_i b_i = (\prod_{i \in I} a_i)(\prod_{i \in I} b_i)$
3. $\prod_{i \in I} \lambda a_i = \lambda^n (\prod_{i \in I} a_i)$ *avec n le nombre d'éléments de I.*

Propriété (Exponentielle d'une somme)

La propriété $e^{a+b} = e^a e^b$ se généralise à une famille de réels $a_1, a_2, a_3, \cdots, a_n$: $exp(\sum_{i=1}^n a_i) = \prod_{i=1}^n exp(a_i)$.

Propriété (Logarithme d'un produit)

Pour $b_1, b_2, b_3, \cdots, b_n \in \mathbb{R}_+^*$: $\ln(\prod_{i=1}^n b_i) = \sum_{i=1}^n \ln(b_i)$.

Sommes et produits télescopiques

Partons de la somme suivante $\sum_{k=1}^{n}(k+1)^3 - k^3$. Si on déroule cette somme on a pour différentes valeurs de k :

$k = 1$ on a $2^3 - 1^3$

$k = 2$ on a $3^3 - 2^3$

$k = 3$ on a $4^3 - 3^3$

$\ldots \quad \ldots$

$k = n - 1$ on a $n^3 - (n-1)^3$

$k = n$ on a $(n+1)^3 - n^3$.

En faisant la somme on remarque que beaucoup de termes se télescopent et on obtient $(n+1)^3 - 1^3$. Ainsi $\sum_{k=1}^{n}(k+1)^3 - k^3$ est une somme télescopique qui vaut après simplification $\sum_{k=1}^{n}(k+1)^3 - k^3 = (n+1)^3 - 1$.

Sommes et produits télescopiques

Definition

Si $(u_k)_{k\in[\![m,n]\!]}$ est une famille de nombres, la somme $\sum_{k=m}^{n}(u_{k+1}-u_k)$ est dite somme télescopique. Cette somme vaut $\sum_{k=m}^{n}(u_{k+1}-u_k)=u_{n+1}-u_m$.

Sommes et produits télescopiques

Exemple

$\sum_{k=1}^{n} \frac{e^{2(k+1)}}{(k+1)^2} - \frac{e^{2k}}{k^2} = ?$. *En posant* $u_k = \frac{e^{2k}}{k^2}$ *alors on reconnait la somme de termes télescopiques d'où*

$$\sum_{k=1}^{n} \frac{e^{2(k+1)}}{(k+1)^2} - \frac{e^{2k}}{k^2} = u_{n+1} - u_1 = \frac{e^{2(n+1)}}{(n+1)^2} - e^2.$$

De même, partons du produit $\prod_{k=1}^{n} \frac{e^{(k+1)^2}}{e^{k^2}} = ?$. *Pour ce produit, en posant* $u_k = e^{k^2}$, *le produit précédent s'écrit*

$\prod_{k=1}^{n} \frac{u_{k+1}}{u_k} = \frac{u_2}{u_1} \times \frac{u_3}{u_2} \times \cdots \times \frac{u_n}{u_{n-1}} \times \frac{u_{n+1}}{u_n}$ *et ainsi par simplification on a*

$$\prod_{k=1}^{n} \frac{u_{k+1}}{u_k} = \frac{u_{n+1}}{u_1} = \frac{e^{(n+1)^2}}{e}.$$

C'est ça qu'on appelle un produit télescopique.

Sommes et produits télescopiques

Definition (Produit télescopique)

On dit qu'un produit $\prod_{k=0}^{n} a_k$ est télescopique si pour tout $k \in \{0, 1, \cdots, n\}$, on peut écrire de façon simple a_k sous la forme $a_k = \dfrac{b_{k+1}}{b_k}$.

Soit $\prod_{k=0}^{n} \dfrac{b_{k+1}}{b_k}$ un produit télescopique. Alors $\prod_{k=0}^{n} \dfrac{b_{k+1}}{b_k} = \dfrac{b_{n+1}}{b_0}$.

Sommes et produits télescopiques

Exercice

Soit $n \geq 1$ un entier et soit $y \in \mathbb{R}$. Calculer

- $U_n := \sum_{j=3}^{n} \ln(j+1) - \ln(2j)$

  Indication : On commence par remarquer que $\ln(2j) = \ln(2) + \ln(j)$ puis on remarque une somme télescopique.

- $V_n(y) := \prod_{k=1}^{n} \frac{2y(k+1)^3}{k^3}$

  Indication : ici $2y$ ne dépend pas de k donc en le sortant du produit, le reste devient un produit télescopique.

Application des sommes télescopiques

factorisation de $a^n - b^n$ par $a - b$

Pour tout $a, b \in \mathbb{R}$ et pour tout $n \in \mathbb{N}^*$, $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$.

Preuve de la formule :

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1}(a-b)a^k b^{n-1-k} = \sum_{k=0}^{n-1} \underbrace{a^{k+1} b^{n-1-k}}_{a^{k+1}b^{n-(k+1)}} - a^k b^{n-k}$$

ainsi on remarque une somme télescopique. Ce qui donne

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = a^n b^0 - a^0 b^n = a^n - b^n.$$

Remarque

- *Pour* $n = 2$, $a^2 - b^2 = (a-b)(a+b)$
- *Pour* $b = 1$ *et* $a \neq 1$, $a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k$

Changement d'indice

Soit la somme $\sum_{k=m}^{n} a_k$, où $a_m, \cdots, a_n$ sont des nombres. L'intervalle des indices de la somme est
$[\![m, n]\!] = \{k, k \in [\![m, n]\!]\} := \{i + 3, i \in [\![m - 3, n - 3]\!]\}$.
Ainsi on a l'égalité : $\sum_{k=m}^{n} a_k = \sum_{i=m-3}^{n-3} a_{i+3}$.

Exemple

On veut faire les changements d'indices $i = k + 2$ et $j = k - n$ à la somme $S = \sum_{k=n}^{2n} \frac{e^{2k+1}}{k\sqrt{k+3}}$

- *Pour $i = k + 2$ alors $k = i - 2$ donc* $S = \sum_{i=n+2}^{2n+2} \frac{e^{2i-3}}{(i-2)\sqrt{i+1}}$
- *Pour $j = k - n$ alors $k = j + n$ donc* $S = \sum_{j=0}^{n} \frac{e^{2(j+n)+1}}{(j+n)\sqrt{j+n+3}}$

Regroupement de termes

Partons de l'exemple de la somme suivante : $S_n = \sum_{k=0}^{2n} \min(k, n), \quad n \geq 1.$

Ici on peut décomposer la somme en deux termes en écrivant

$$\begin{aligned} S_n &= \sum_{k=0}^{n} \min(k, n) + \sum_{k=n+1}^{2n} \min(k, n) \\ &= \sum_{k=0}^{n} k + \sum_{k=n+1}^{2n} n \\ &= \frac{n(n+1)}{2} + n(n) \\ &= \frac{n(3n+1)}{2}. \end{aligned}$$

Regroupement de termes

Regardons également l'exemple suivant : soit $n \geq 1$, calculer $S_n = \sum_{k=0}^{2n}(-1)^k k^2$? ici on remarque que :

$k = 0 \quad (-1)^0 = 1 \quad ; k = 1 \quad (-1)^1 = -1 \quad ; k = 2 \quad (-1)^2 = 1$

donc le terme $(-1)^k$ fait alterner le signe de S_n. Ainsi,

$S_n = -1 + 2^2 - 3^2 + 4^2 \cdots - (2n-1)^2 + (2n)^2$. En écrivant la somme

$S_n = \underbrace{2^2 + 4^2 + \cdots + (2n)^2}_{\text{termes pairs}} - \underbrace{(1 + 3^2 + \cdots + (2n-1)^2)}_{\text{termes impairs}}$. On a

$$S_n = \sum_{k=0}^{2n}(-1)^k k^2 = \underbrace{\sum_{p=0}^{n}(-1)^{2p}(2p)^2}_{k=2p} + \underbrace{\sum_{p=0}^{n-1}(-1)^{2p+1}(2p+1)^2}_{k=2p+1}$$

$$= \sum_{p=0}^{n} 4p^2 - \sum_{p=0}^{n-1} 4p^2 + 4p + 1 = \sum_{p=0}^{n} 4p^2 - \sum_{p=0}^{n-1} 4p^2 - \sum_{p=0}^{n-1} 4p - \sum_{p=0}^{n-1} 1$$

$$= 4n^2 - 4\frac{n(n-1)}{2} - n = 4n^2 - 2n^2 + 2n - n = 2n^2 + n$$

Factorielle

Definition

Soit $n \in \mathbb{N}$, on appelle factorielle n l'entier noté $n!$ défini par

$$n! = \prod_{k=1}^{n} k = 1 \times 2 \times 3 \cdots \times (n-1) \times n$$

Remarque

- $(n+1)! = n! \times (n+1)$
- $0!$ *est un produit vide, donc* $0! = 1$
- $1! = 1$; $2! = 2$; $3! = 6$

Factorielle

Exemple

- *Si on veut calculer le produit des n premiers entiers pairs :* $2 \times 4 \times 6 \times \cdots \times 2(n-1) \times 2n$ *?*
  Attention, ce produit ne vaut pas $(2n)!$*.*
  Écrivons le produit :

$$\begin{aligned} & 2 \times 4 \times \cdots \times 2(n-1) \times 2n \\ = \; & 2 \times 1 \times 2 \times 2 \times \cdots \times 2 \times (n-1) \times 2 \times n \\ = \; & 2^n \times (1 \times 2 \times 3 \cdots \times (n-1) \times n) \\ = \; & 2^n \times n! \end{aligned}$$

Factorielle

Exemple

- *Pour le produit des entiers impairs entre* 1 *et* $(2n+1)$ *:*
  $1 \times 3 \times 5 \cdots \times (2n-1) \times (2n+1)$.
  Attention, de même ici ce produit de vaut pas $(2n+1)!$.
  Écrivons le produit comme suit

$$\begin{aligned} & 1 \times 3 \times 5 \cdots \times (2n-1) \times (2n+1) \\ = & \frac{1 \times 2 \times 3 \cdots \times (2n-1) \times 2n \times (2n+1)}{2 \times 4 \times 6 \times \cdots \times 2(n-1) \times 2n} \\ = & \frac{(2n+1)!}{2^n \times n!} \end{aligned}$$

Coefficients binomiaux

Definition

Soit $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$. On définit le coefficient binomial $\binom{n}{p}$

c'est-à-dire "p parmi n" par $\binom{n}{p} = \dfrac{n!}{p!(n-p)!}$.

Remarque

- *pour* $p \in \mathbb{Z}$ *et* $p \notin [\![0, n]\!]$, $\binom{n}{p} = 0$.
- $\binom{n}{0} = 1\,;\ \binom{n}{1} = n\,;\ \binom{n}{2} = \dfrac{n(n-1)}{2}$

Coefficients binomiaux

Exemple

- $\binom{6}{2} = \frac{6!}{2!(6-2)!} = \frac{5 \times 6}{1 \times 2} = 15\,;\quad \binom{7}{3} = \frac{7 \times 6 \times 5}{1 \times 2 \times 3}$
- $\binom{12}{4} = \frac{12 \times 11 \times 10 \times 9}{1 \times 2 \times 3 \times 4}.$

Proposition

Pour tout $n \in \mathbb{N}$, pour tout $p \in \mathbb{Z}$ on a $\binom{n}{p} = \binom{n}{n-p}.$

Preuve

En effet si $p \in [\![0, n]\!]$ on a

$$\binom{n}{n-p} = \frac{n!}{(n-p)!(n-(n-p))!} = \frac{n!}{(n-p)!p!} = \binom{n}{p}.$$

Coefficients binomiaux

Remarque

$$\binom{n}{n} = \binom{n}{0} = 1\,; \binom{n}{n-1} = \binom{n}{1} = n\,; \binom{n}{n-2} = \binom{n}{2} = \frac{n(n-1)}{2}.$$

Tout ceci par symétrie.

Théorème

(Formule de Pascal) Pour tout $n \in \mathbb{N}^*$, pour tout $p \in \mathbb{Z}$

$$\binom{n-1}{p-1} + \binom{n-1}{p} = \binom{n}{p}.$$

La preuve est donnée ci-dessous.

Coefficients binomiaux

Preuve

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{Z}$ *avec* $p \in [\![0, n]\!]$

- *Si* $p = n$ *on a* $\binom{n-1}{n-1} + \binom{n-1}{n} = 1 + 0 \quad et \quad \binom{n}{n} = 1$
- *Si* $p \in [\![0, n-1]\!]$, *on écrit*

$$\begin{aligned}\binom{n-1}{p-1} + \binom{n-1}{p} &= \frac{(n-1)!}{(p-1)!(n-p)!} + \frac{(n-1)!}{p!(n-1-p)!} \\ &= (n-1)!\left(\frac{1}{(p-1)!(n-p)!} + \frac{1}{p!(n-p-1)!}\right).\end{aligned}$$

Or d'une part $\frac{1}{(p-1)!} = \frac{p}{p(p-1)!} = \frac{p}{p!}$ *ainsi* $\frac{1}{(p-1)!(n-p)!} = \frac{p}{p!(n-p)!}$.
D'autre part, $\frac{1}{(n-p-1)!} = \frac{n-p}{(n-p)!}$ *ainsi* $\frac{1}{p!(n-p-1)!} = \frac{n-p}{p!(n-p)!}$ *d'où*

$$\binom{n-1}{p-1} + \binom{n-1}{p} = \frac{(n-1)!}{p!(n-p)!}(p + (n-p)) = \frac{n!}{p!(n-p)!} = \binom{n}{p}.$$

Coefficients binomiaux

Le corollaire (conséquence) de ce théorème est le triangle de Pascal

$n \backslash p$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	2	1	0	0	0	0
3	1	3	3	1	0	0	0
4	1	4	6	4	1	0	0
5	1	5	10	10	5	1	0
6	1	6	15	20	15	6	1

Ainsi l'élément à la ligne n et à la colonne p s'obtient en sommant celle à la ligne $n-1$ et colonne $p-1$ et celle de la ligne $n-1$ et colone p.
Dans ce tableau, la première colonne vaut 1 car $\binom{n}{0} = 1$. La diagonale du tableau vaut 1 car $\binom{n}{n} = 1$. La surdiagonale vaut 0 car $p > n$.

Remarque

La formule de Pascal permet de voir que $\binom{n}{p}$ est un entier.

Le binôme de Newton

Le binôme de Newton est une méthode pour calculer la puissance entière d'une somme. Les formules de développement connues par coeur sont
$(a+b)^0 = 1; (a+b)^1 = a+b; (a+b)^2 = a^2 + 2ab + b^2$;
$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$;
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.
Le binôme de Newton permet de généraliser ce développement au cas $(a+b)^n$.

Théorème

Pour tout a, b réels et pour tout $n \in \mathbb{N}$

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p := \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$$

Le binôme de Newton

Exemple

$(1+x)^5$ *pour tout réel* x

$$\begin{aligned}(1+x)^5 &= \sum_{p=0}^{5}\binom{5}{p}1^p x^{5-p} = \sum_{p=0}^{5}\binom{5}{p}x^p 1^{5-p}\\ &= \binom{5}{0}x^0+\binom{5}{1}x^1+\binom{5}{2}x^2+\cdots+\binom{5}{5}x^5\\ &= x^0+5x+10x^2+10x^3+5x^4+x^5 \text{ par le triange de Pascal.}\end{aligned}$$

Exemple

Soit $n\in\mathbb{N}^*$ *et* $x\in\mathbb{R}$, *on veut calculer* $A_n=\sum_{k=0}^{n}\binom{n}{k}$. *Ici c'est le binôme de Newton avec* $a=b=1$. *En effet*

$$(1+1)^n=\sum_{k=0}^{n}\binom{n}{k}1^k1^{n-k}=\sum_{k=0}^{n}\binom{n}{k}\Longrightarrow 2^n=\sum_{k=0}^{n}\binom{n}{k}$$

Le binôme de Newton

Exemple

Soit à calculer $S_n = \sum_{p=0}^{n} \binom{n}{p} 2^p$ *?*

On a $$\sum_{p=0}^{n} \binom{n}{p} 2^p = \sum_{p=0}^{n} \binom{n}{p} 2^p 1^{n-p} = (2+1)^n = 3^n$$

Exemple

Soit $S_n = \sum_{i=2}^{2n} \binom{2n}{i} (-1)^i$*? Elle ressemble à un binôme de Newton.*

En effet $(1+(-1))^{2n} = \sum_{i=2}^{2n} \binom{2n}{i} 1^{2n-i}(-1)^i = \sum_{i=2}^{2n} \binom{2n}{i} (-1)^i$ *ainsi*

$0^{2n} = \binom{2n}{0}(-1)^0 + \binom{2n}{1}(-1)^1 + \sum_{i=2}^{2n} \binom{2n}{i}(-1)^i$*. En d'autres termes*

$0 = 1 + 2n(-1) + \sum_{i=2}^{2n} \binom{2n}{i}(-1)^i$*. D'où* $-1 + 2n = \sum_{i=2}^{2n} \binom{2n}{i}(-1)^i$*.*

a) **Somme double indexée par un rectangle**

Soit $(a_{i,j})_{i\in[\![m,n]\!],j\in[\![p,q]\!]}$ une famille de nombres indexée par les entiers i et j. La somme de tous ces nombres est notée $\sum_{m\leq i\leq n, p\leq j\leq q} a_{ij}$. Pour cette somme, en notant par $L_i := \sum_{j=p}^{q} a_{ij}$ avec $i \in [\![m,n]\!]$ et par $C_j = \sum_{i=m}^{n} a_{ij}$ avec $j \in [\![p,q]\!]$. Alors $\sum_{m\leq i\leq n, p\leq j\leq q} a_{ij} = \sum_{i=m}^{n} L_i = \sum_{j=p}^{q} C_j$.

En particulier, on a l'égalité des deux écritures

$$\sum_{i=m}^{n}\sum_{j=p}^{q} a_{ij} = \sum_{j=p}^{q}\sum_{i=m}^{n} a_{ij} := \sum_{m\leq i\leq n, p\leq j\leq q} a_{ij}.$$

Sommes doubles

Exemple

Soit $n \in \mathbb{N}$, *calculons* $S_n = \sum_{0 \leq i,j \leq n} 2^i$:

- *D'une part*

$$\begin{aligned} \sum_{i=0}^{n}\sum_{j=0}^{n} 2^i &= \sum_{i=0}^{n}(n+1)2^i = (n+1)\sum_{i=0}^{n} 2^i \\ &= (n+1)\frac{1-2^{n+1}}{1-2} = (n+1)(2^{n+1}-1) \end{aligned}$$

- *D'autre part*

$$\sum_{j=0}^{n}\sum_{i=0}^{n} 2^i = \sum_{j=0}^{n}\frac{1-2^{n+1}}{1-2} = \sum_{j=0}^{n} 2^{n+1} - 1 = (n+1)(2^{n+1}-1)$$

b) **Somme double indexée par un triangle**

Soit $(a_{i,j})_{m\leq i\leq j\leq n}$ une famille de nombres indexée par les entiers i et j appartenant à $[\![m,n]\!]$, mais seulement pour les couples (i,j) tel que $i\leq j$.

Pour calculer la somme $\displaystyle\sum_{m\leq i\leq j\leq n} a_{ij}$ on peut poser $L_i=\displaystyle\sum_{j\geq i}^{n} a_{ij}$ et

$C_j=\displaystyle\sum_{i\leq j}^{n} a_{ij}$. Ainsi on pourra avoir deux façons d'expliciter la somme

$\displaystyle\sum_{m\leq i\leq j\leq n} a_{ij}$ soit en sommant ligne par ligne c'est-à-dire $\displaystyle\sum_{i=m}^{n}\sum_{j=i}^{n} a_{ij}$ ou bien

en sommant colonne par colonne c'est-à-dire $\displaystyle\sum_{j=m}^{n}\sum_{i=m}^{j} a_{ij}$.

En résumé, la somme double indexée par un triangle s'écrit :

$$\sum_{m\leq i\leq j\leq n} a_{ij}=\sum_{i=m}^{n}\sum_{j=i}^{n} a_{ij}=\sum_{j=m}^{n}\sum_{i=m}^{j} a_{ij}.$$

Sommes doubles

Exemple

Soit $n \in \mathbb{N}^*$, calculons la quantité $D_n = \sum_{i=1}^{n} \sum_{j=i}^{n} \frac{i}{j}$. Ici on remarque que les indices ont une contrainte triangulaire $1 \leq i \leq j \leq n$.

$$D_n = \sum_{1 \leq i \leq j \leq n} \frac{i}{j} = \sum_{j=1}^{n} \sum_{i=1}^{j} \frac{i}{j} = \sum_{j=1}^{n} \frac{1}{j} \sum_{i=1}^{j} i = \sum_{j=1}^{n} \frac{1}{j} \frac{j(j+1)}{2} = \sum_{j=1}^{n} \frac{j+1}{2}$$

$$\text{D'où } D_n = \frac{1}{2}\left(\sum_{j=1}^{n} j + \sum_{j=1}^{n} 1\right) = \frac{1}{2}\left(\frac{n(n+1)}{2} + \frac{2n}{2}\right) = \frac{n(n+3)}{4}.$$

Produit de deux sommes finies

Soient $(a_i)_{i\in[\![1,n]\!]}$ et $(b_j)_{j\in[\![1,n]\!]}$ deux familles de nombres réels. Comment développer le produit suivant

$$P = \left(\sum_{k=1}^{n} a_k\right)\left(\sum_{k=1}^{n} b_k\right)?$$

Attention : Il faut pas commettre l'erreur en disant que $P = \sum_{k=1}^{n} a_k b_k$. C'est Faux.

Pour calculer formellement un tel produit il faut commencer par changer le nom d'un des indices. Puis développer le produit en utilisant la "distributivité" $P = \left(\sum_{j=1}^{n} a_j\right)\left(\sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{n}\left(a_j \sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{n}\sum_{k=1}^{n} a_j b_k.$

Les ensembles

Les ensembles

Definition

Un ensemble est une collection bien définie d'objets qu'on appelle éléments.

Exemple

soit Ω, *l'ensemble de tous les résultats en faisant la somme de 2 dés. Alors* $\Omega = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ *et les nombres* $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ *sont les éléments de* Ω.

Les ensembles qu'on a fréquemment l'habitude d'employer sont
$\mathbb{N} = \{0, 1, 2, 3, 4 \cdots\}$ des entiers naturels.
$\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4 \cdots\}$ des entiers relatifs.
$\mathbb{Q}$ l'ensemble des nombres rationnels c'est-à-dire s'écrivant sous la forme d'une fraction $\frac{a}{b}$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
$\mathbb{R}$ l'ensemble formé par tous les nombres réels.

Les ensembles

Il existe un ensemble ne contenant aucun élément, qu'on appelle l'ensemble vide et qui est noté par $\emptyset$.

Definition

(Il s'agit d'un rappel)
Le symbole $\in$ indique qu'un élément appartient à un ensemble. À l'inverse le symbole $\notin$ indique qu'un élément n'appartient pas à un ensemble.

Exemple : $a \in \{a, e, i, o, u\}$; $k \notin \{a, e, i, o, u\}$; $2 \in \mathbb{N}$; $\frac{1}{2} \notin \mathbb{N}$.

Les sous-ensembles (notion d'inclusion)

Definition

Soit Ω un ensemble. On dit que A est un sous-ensemble de Ω si et seulement si tous les éléments de A sont aussi des éléments de Ω. Ainsi l'ensemble A est inclus dans l'ensemble Ω. La notation $A \subseteq \Omega$ est utilisée pour symboliser l'inclusion de A dans Ω.

Remarque

Le symbole $\not\subset$ indique qu'un ensemble n'est pas inclus dans un autre. Ainsi $A \not\subset B$ exprime donc qu'au moins un élément de A n'est pas un élément de B.

Les sous-ensembles (notion d'inclusion)

Exemple

En revenant sur l'ensemble Ω *comme étant la somme de deux dés c'est-à-dire* $\Omega = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. *On peut citer les quelques sous-ensembles suivants :*

$\Omega_1 = \{2, 4, 6, 8, 10, 12\}$ *: ensemble des résultats pairs*

$\Omega_2 = \{2, 3, 4, 5, 6\}$ *: ensemble des résultats inférieurs ou égaux à 6.*

$\Omega_3 = \emptyset$ *: ensemble des résultats supérieurs à 12*

$\Omega_4 = \{11\}$ *: ensemble des résultats divisible par 11.*

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

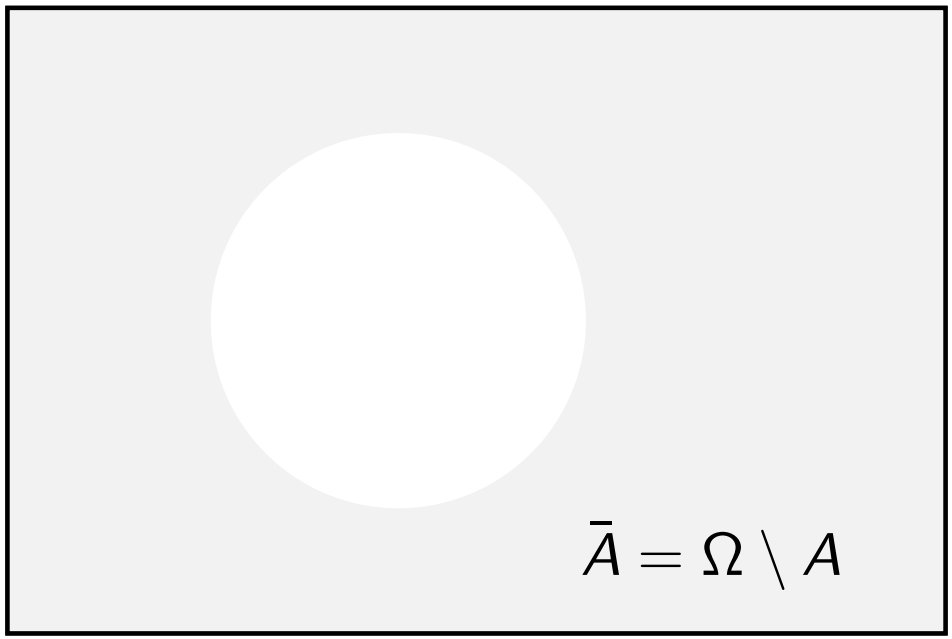
$\mathbb{Z} \not\subset \mathbb{N}$; $\{0, 1, 2, 3, 5, 6\} \not\subset \{1, 3, 5, 7, 9, 11\}$

Opérations sur les ensembles

Nous présentons ici les opérations ensembliste les plus importantes.

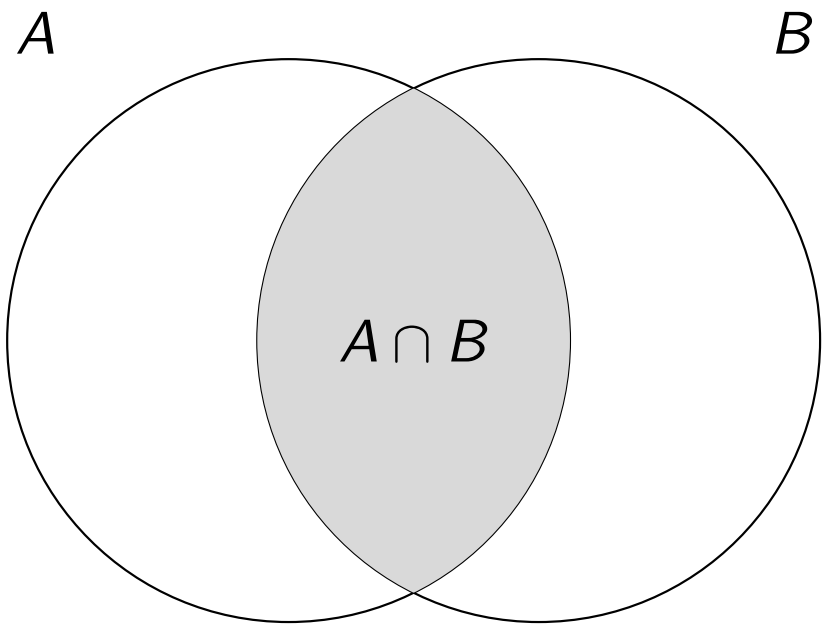
a) **Complément d'un ensemble**

Soit Ω un ensemble. On définit le complément d'une partie A de Ω, noté $\bar{A}$, l'ensemble de tous les éléments qui ne sont pas dans A.



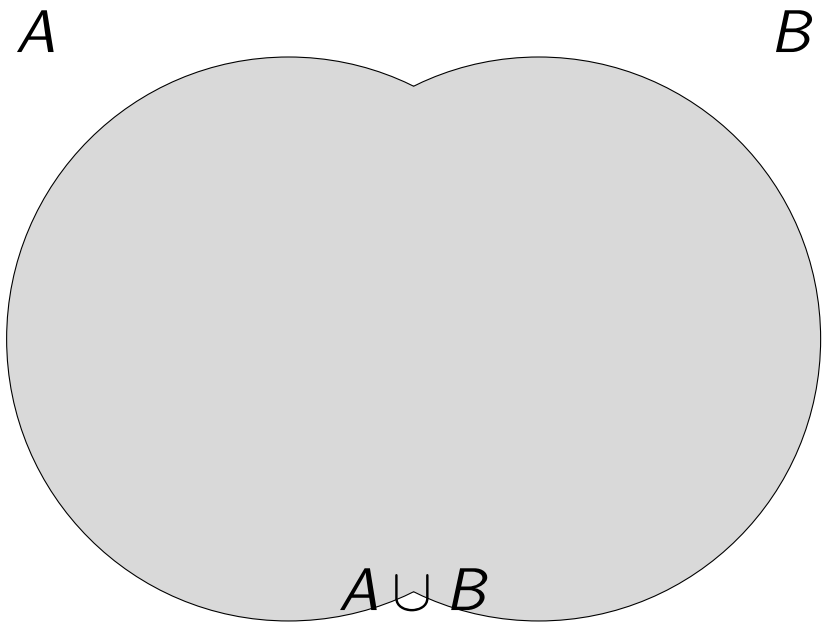
b) **Intersection d'ensembles**

Soient A et B deux ensembles. On appelle intersection de A et B, notée $A \cap B$, l'ensemble de tous les éléments appartenant à la fois à A et à B.



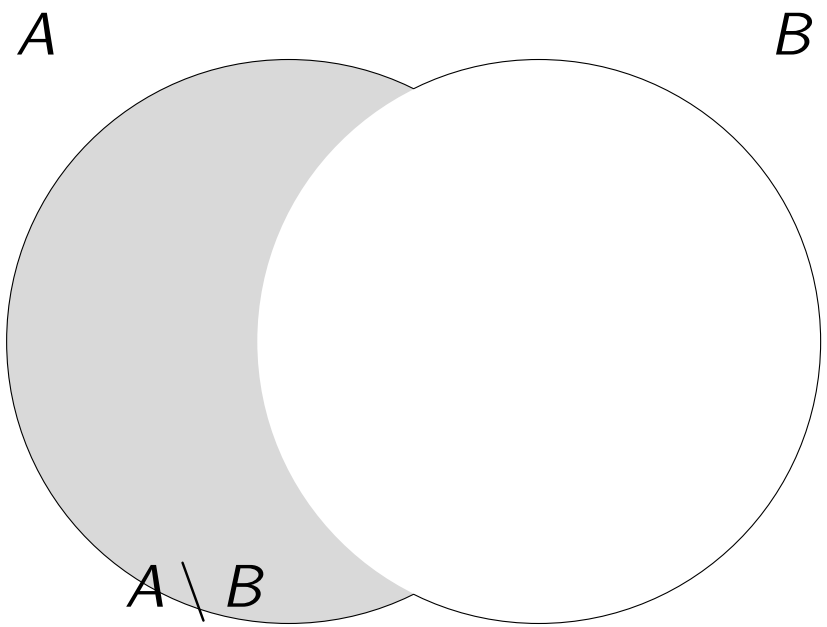
c) **Union de deux ensembles**

Soient A et B deux ensembles. On appelle union des deux ensembles A et B, l'ensemble noté $A \cup B$, représentant tous les éléments appartenant soit à A ou à B.



d) **Différence de deux ensembles**

Soient A et B deux ensembles. On appelle différence de A et B, notée $A \setminus B$, l'ensemble de tous les éléments de A qui n'appartiennent pas à B.



Opérations sur les ensembles

Remarque

(Différence symétrique) Soient A et B deux ensembles, on appelle différence symétrique de A et B, notée $A\Delta B$ (lire A delta B), l'ensemble constitué par la réunion des éléments de A qui ne sont pas dans B, et des éléments de B qui ne sont pas dans A.

$$A\Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) = (A \cap \bar{B}) \cup (B \cap \bar{A}).$$

Exercice (à faire)
Reprenons l'ensemble Ω concernant les dés. Soient les sous-ensembles de Ω : Ω_1, Ω_2, Ω_3, Ω_4 précédemment définis.

- Ecrire les éléments des sous-ensembles obtenus par les opérations suivantes : complémentaire ; intersection ; union ; différence.

Produit cartésien de 2 ensembles

Definition

On appelle produit cartésien de deux ensembles E et F, l'ensemble noté $E \times F$ des couples (a, b) où a est un élément de E et b un élément de F.
Par exemple, si $E = \{1, 2\}$ et $F = \{a, b, c\}$, alors
$E \times F = \{(1, a); (1, b); (1, c); (2, a); (2, b); (2, c)\}$.
Ce produit n'est pas commutatif, c'est-à-dire $E \times F$ peut être différent de $F \times E$.

Exemple

Le plan, $\mathbb{R}^2$, est le produit cartésien $\mathbb{R} \times \mathbb{R}$.

Remarque

Lorsque E et F sont deux ensembles finis, alors le nombre d'éléments de $E \times F$ est le produit du nombre d'éléments de E et du nombre d'éléments de F.

Produit cartésien d'ensembles

Definition

Soit E un ensemble qui possède un nombre fini d'éléments. On appelle cardinal de E, le nombre d'éléments de E et on le note *card* E

Propriété

Soient $E_1, E_2, E_3, \cdots, E_p$, p *ensembles finis, alors*

$$card(E_1 \times E_2 \times \cdots \times E_p) = card(E_1) \times card(E_2) \times \cdots \times card(E_p).$$

Ensemble des parties d'un ensemble (recouvrement, partition)

Definition

Si A est un ensemble, l'ensemble des parties de A est l'ensemble constitué de tous les sous-ensembles de A. Il est noté $\mathcal{P}(A)$.

Exemple

Si $A = \{1, 2, 3\}$, *les parties de A sont*
$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$.
On a donc $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Propriété

- *Si A contient n éléments,* $\mathcal{P}(A)$ *contient exactement* 2^n *éléments.*
- *Si A est infini,* $\mathcal{P}(A)$ *l'est aussi.*

Recouvrement, partition

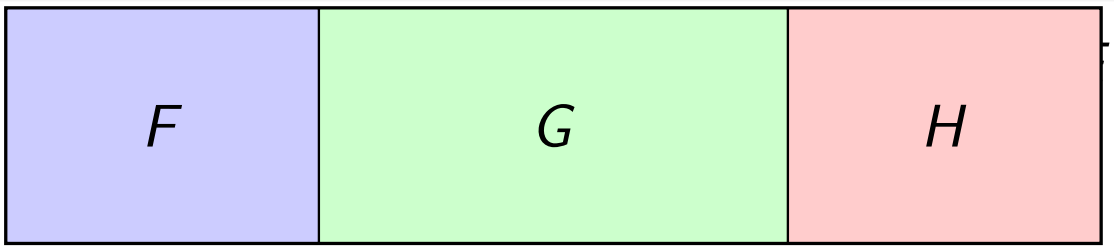
a) **Recouvrement** : Soit X un ensemble, A une partie de X. Un recouvrement de A est une famille de parties de X dont la réunion contient A. En d'autres termes, il existe une famille $(U_i)_{i\in I}$ de parties de X telles que $A \subset \bigcup_{i\in I} U_i$. Ce recouvrement est dit fini si I est fini.

En particulier, un recouvrement de X vérifie $X = \bigcup_{i\in I} U_i$.

b) **Partition** : Un recouvrement $(U_i)_{i\in I}$ est appelé partition si les U_i sont disjoints deux à deux c'est-à-dire $i \neq j$, $U_i \bigcap U_j = \emptyset$.

Exemple

Si E est le rectangle ci-dessous, alors les petits rectangles coloriés F, G, H constitituent une partition de E.



Manipulation des ensembles à l'aide des quantificateurs

Pour exprimer avec précision les propriétés des ensembles et des éléments qui les composent, on utilise souvent les quantificateurs. Il en existe deux :

- La locution "pour tout" ou "quelque soit", appelée quantificateur universel et notée $\forall$.
- La locution "il existe", appelée quantificateur existentiel et notée $\exists$.

Exemple

$\forall x \in E$, $P(x)$ se lit " pour tout x appartenant à l'ensemnle E, la proriété P est vraie". Ici le symbole "$\forall$" signifie donc que la propriété P est vérifiée pour tout x de l'ensemble E.

Exemple

$\exists x \in E$, $P(x)$ se lit " il existe x appartenant à l'ensemnle E, tel que la proriété P est vraie". Ici le symbole " $\exists$ " signifie donc qu'il existe (au moins) un x de l'ensemble E vérifiant la propriété P.

Manipulation des ensembles à l'aide des quantificateurs

Remarque

a) *Attention, la locution "il existe" ne signifie pas "il existe un et un seul", mais bien "il existe au moins un". Autrement dit, cette locution assure qu'il existe au moins un élément, et donc éventuellement plusieurs, vérifiant une propriété donnée, mais n'assure pas que cet élément soit unique. Pour l'expression "il existe un et un seul " ou "il existe un unique " se note* $\exists!$.

Manipulation des ensembles à l'aide des quantificateurs

Remarque

b) *Attention l'ordre d'utilisation des quantificateurs a une importance. En effet dire :* $\forall\, n \in \mathbb{Z}, \exists k \in \mathbb{Z},\ k \geq n$ *se lit "pour tout entier n, il existe un entier k tel que k est plus grand que n" ou encore " tout entier relatif n admet un plus grand entier relatif k". Cette proposition est vraie puisque* $n+1$ *est toujours plus grand que n, quel que soit l'entier n.*
En revanche, dire : $\exists\, n \in \mathbb{Z}, \forall\, k \in \mathbb{Z},\ k \geq n$ *se lit "il existe un entier n tel que pour tout entier k, k est plus grand que n" ou encore "il existe un entier n qui est plus petit que tout entier k". Bien évidemment cette proposition est fausse (en effet il suffit de choisir* $k = n - 1$*).*

Les bases de logique

Origines de la logique

L'objectif ici est de bien définir le vocabulaire, les notations et le propriétés que nous utiliserons non seulement dans ce chapitre, mais également dans toutes les preuves de résultats que nous développerons que ce soit en cours ou en travaux dirigés. A partir de ce chapitre, il faudra donc construire les démonstrations de la façon la plus rigoureuse possible, en utilisant les bons quantificateurs, dans le bon ordre, mais également des stratégies de preuves (absurde, contraposée, récurrence par exemple).

Definition (Assertion)

Une **assertion** est un énoncé mathématique auquel on peut attribuer une valeur de vérité

vrai (V) ou Faux (F),

mais jamais les deux à la fois. C'est le principe du **tiers-exclu**.

Assertions et prédicats

Exemple

1. *L'énoncé "Paris est la capitale de la France", est* ***vrai (V)***.
2. *L'énoncé "24 est un multiple de 2", est* ***vrai (V)***.
3. *L'énoncé "19 est un multiple de 2", est* ***faux (F)***.

Definition (Prédicat)

Un **prédicat** est un énoncé mathématique contenant des lettres appelées "variables" tel que, quand on remplace chacune des lettres par un élément donné d'un ensemble, on obtient une assertion.

Assertions et prédicats

Exemple

1. *L'énoncé : $P(n)$ =“n n'est pas un multiple de 2”, est un **prédicat**, car il devient une **assertion** quand on donne une valeur à n. Par exemple,*
   $P(10)$=“10 est un multiple de 2” est une assertion vraie.
   $P(11)$=“11 est un multiple de 2” est une assertion fausse.
2. *L'énoncé $P(x, A)$=“$x \in A$”, est un **prédicat** à deux variables. Il devient une **assertion** quand on donne une valeur aux deux variables. Par exemple,*
   $P(1, \mathbb{N})$ est une assertion vraie,
   $P(\sqrt{2}, \mathbb{Q})$ est une assertion fausse.

Remarque

Une assertion peut s'interpréter comme un prédicat sans variable, c'est-à-dire comme un prédicat toujours vrai ou toujours faux.

Les connecteurs logiques

Definition (Négation d'un prédicat)

Soit P un prédicat, la négation de P est le prédicat non(P), qui est faux lorsque P est vrai ; vrai lorsque P est faux.

On résume en général ceci dans une table de vérité, comme suit

P	non P
V	F
F	V

Table de vérité pour non (P)

Exemple

1. *P="24 est un multiple de 2" est une assertion vraie (V), non (P)="24 n'est pas un multiple de 2" est une assertion fausse (F).*
2. *A partir du prédicat "$x \in A$", nous pouvons définir le prédicat non($x \in A$) qui est "$x \notin A$".*

Les connecteurs logiques

Definition (Conjonction)

Soient P et Q deux prédicats. Le prédicat "P et Q" est appelé **conjonction** de P et Q. C'est un prédicat qui est :

- vrai lorsque P et Q sont vrais simultanément,
- faux dans tous les autres cas.

Nous pouvons résumer cela dans une table de vérité :

P	Q	P et Q
V	V	V
V	F	F
F	V	F
F	F	F

Table de vérité pour la conjonction

Notation (à retenir)

Nous écrivons parfois $P \wedge Q$ pour "P et Q".

Les connecteurs logiques

Exemple

1. *Soient P le prédicat "$x \in [0,4]$" et Q le prédicat "$x \in [2,8]$", le prédicat $P \wedge Q$ est "$x \in [2,4]$".*
2. *Soient P le prédicat "$x \in A$" et Q le prédicat "$x \in B$", le prédicat $P \wedge Q$ est "$x \in A \cap B$".*

Definition (Disjonction)

Soient P et Q deux prédicats. Le prédicat "P ou Q" est appelé **disjonction** de P et Q. C'est un prédicat qui est :

- vrai lorsque l'un au moins des deux prédicats est vrai,
- faux lorsque les deux prédicats sont faux simultanément.

Les connecteurs logiques

Nous pouvons résumer cela dans une table de vérité :

P	Q	P ou Q
V	V	V
V	F	V
F	V	V
F	F	F

Table de vérité pour la disjonction

Notation (à retenir)

Nous écrivons parfois $P \vee Q$ pour "P ou Q".

Exemple

1. *Soient P le prédicat "$x \in [0,4]$" et Q le prédicat "$x \in [2,8]$", le prédicat $P \vee Q$ est "$x \in [0,8]$".*
2. *Soient P le prédicat "$x \in A$" et Q le prédicat "$x \in B$", le prédicat $P \vee Q$ est "$x \in A \bigcup B$".*

Definition (Implication)

Soient P et Q deux prédicats. Le prédicat "$P \Rightarrow Q$" est appelé **implication** de P et Q. C'est un prédicat qui est :
-faux lorsque P est vrai et Q est faux,
-vrai dans tous les autres cas.

Nous pouvons résumer cela dans une table de vérité :

P	Q	P $\Rightarrow$ Q
V	V	V
V	F	F
F	V	V
F	F	V

Table de vérité pour l'implication

Les connecteurs logiques

Remarques

1. *Nous disons que P est une condition suffisante pour Q.*
2. *$Q \Rightarrow P$ s'appelle l'implication réciproque de $P \Rightarrow Q$.*
3. *si P est faux et Q est vrai, le prédicat $P \Rightarrow Q$ peut paraître curieux.*

Definition (Équivalence)

Soient P et Q deux prédicats. Le prédicat "$P \Leftrightarrow Q$" est appelé **équivalence** de P et Q. C'est un prédicat qui est :

- vrai lorsque P et Q sont simultanément vrais ou faux,
- faux dans tous les autres cas.

Les connecteurs logiques

Nous pouvons résumer cela dans une table de vérité :

P	Q	P $\Leftrightarrow$ Q
V	V	V
V	F	F
F	V	F
F	F	V

Table de vérité pour l'équivalence.

Remarques

1. $(P \Rightarrow Q)$ *et* $(Q \Rightarrow P)$ *se note* $P \Rightarrow Q \Rightarrow R$,
2. $(P \Leftrightarrow Q)$ *et* $(Q \Leftrightarrow R)$ *se note* $P \Leftrightarrow Q \Leftrightarrow R$.

Propriétés

Definition (Logiquement équivalents)

Soient P_1 et P_2 deux prédicats.Si
- P_1 est vrai lorsque P_2 est vrai,
- P_2 est faux lorsque P_2 est faux,

on dit que P_1 et P_2 ont la même table de vérité, ou qu'elles sont logiquement équivalentes, et on note

$$P_1 \equiv P_2.$$

Dans le cas contraire, on note

$$P_1 \not\equiv P_2$$

Exemple

1. *Soit P un prédicat, $non(non(P)) \equiv P$.*
2. *Soient P et Q deux prédicats, $(P$ et $(P$ ou $Q)) \equiv P$.*

Propriétés

Considérons maintenant un prédicat P, qui peut prendre la valeur de vérité vrai ou faux. Considérons ensuite le prédicat composé

$$R = \text{“}P \text{ ou non} P\text{”}.$$

Ce prédicat est toujours vrai indépendamment du choix de P. En effet, avec la table de vérité, nous avons,

P	non (P)	P ou non(P)
V	F	V
F	V	V

Table de vérité pour une tautologie

Ce prédicat R est appelé **tautologie**.

Definition (Tautologie)

Un prédicat composé R qui est vrai quelles que soient les valeurs de vérité qui le composent, est appelé une **tautologie**.

Propriétés

D'un autre côté, sinon nous considérons le prédicat composé

$$Q = \text{“}P \text{ et non}(P)\text{”}.$$

Ce prédicat est toujours faux. En effet, avec la table de vérité, nous avons,

P	non (P)	P et non(P)
V	F	F
F	V	F

Table de vérité pour une incompatibilité

Nous disons que les prédicats P et non$P$ sont incompatibles.

Definition (Incompatibilité)

On dit que deux prédicats P et non$P$ sont incompatibles si leur conjonction est fausse quelles que soient les valeurs de vérité des prédicats qui les composent.

Propriétés

Proposition (Lois de De Morgan)

Soient P et Q deux prédicats. Nous avons les équivalences logiques suivantes

$$\begin{aligned} \text{non}\,(P \ \text{ou} \ Q) &\equiv (\text{non}\,P \ \text{et} \ \text{non}\,Q) \\ \text{non}\,(P \ \text{et} \ Q) &\equiv (\text{non}\,P \ \text{ou} \ \text{non}\,Q) \end{aligned}$$

Ce sont les ***lois de De Morgan*** *pour les prédicats.*

Proposition (Équivalences logiques avec trois prédicats)

Soient P, Q et R trois prédicats. Nous avons les équivalences logiques suivantes

$$\begin{aligned} (P \ \text{ou} \ (Q \ \text{et} \ R) &\equiv (P \ \text{ou} \ Q) \ \text{et} \ (P \ \text{ou} \ R) \\ (P \ \text{et} \ (Q \ \text{ou} \ R) &\equiv (P \ \text{et} \ Q) \ \text{ou} \ (P \ \text{et} \ R) \end{aligned}$$

Propriétés

Proposition (Équivalences logiques avec trois prédicats)

Soient P et Q deux prédicats. Nous avons les équivalences logiques suivantes

$$P \Rightarrow Q \equiv (non\ P \quad ou \quad Q),$$

nous disons que Q est une ***condition nécessaire*** *pour P.*

$$\begin{array}{lcl} non(P \Rightarrow Q) & \equiv & (P \ \ et \ \ non\ Q) \\ (P \Leftrightarrow Q) & \equiv & non(P) \Rightarrow non(Q) \\ (P \Leftrightarrow Q) & \equiv & ((P \Rightarrow Q) \ \ et \ \ (Q \Rightarrow P)) \end{array}$$

Notons que $non(P) \Rightarrow nonQ)$ est la ***contraposée*** *de $P \Rightarrow Q$.*

Quantificateurs mathématiques

A partir d'un prédicat $P(x)$ défini sur un ensemble E, nous construisons de nouvelles assertions, que l'on appelle assertions quantifiées, en utilisant les quantificateurs "quel que soit" et "il existe".

Definition (Quantificateur $\forall$)

Le quantificateur "quel que soit" noté $\forall$ permet de définir l'assertion quantifiée "$\forall x \in E,\ \ P(x)$,"
qui est vraie pour tous les éléments x appartenant à E, le prédicat $P(x)$ est vraie.

Exemple

1. " $\forall x \in [-3,1],\ \ x^2+2x-3 \leq 0$ " *est vraie,*
2. " $\forall n \in \mathbb{N},\ \ (n-3)n \geq 0$ " *est fausse,*
3. " $\forall n \in \mathbb{N},\ \ (n^2$ *pair* $\Rightarrow n$ *pair)* " *est vraie.*

Quantificateurs mathématiques

Definition (Quantificateur ∃)

Le quantificateur "il existe" noté ∃ permet de définir l'assertion quantifiée "$\exists\, x \in E,\ \ P(x)$,"
qui est vraie si l'on peut trouver au moins un élément x appartenant à E, tel que le prédicat $P(x)$ soit vraie.

Remarque

S'il existe un et un seul élément, on peut écrire $\exists!\, x \in E,\ \ P(x)$.
Nous dirons alors qu'il existe un unique élément x *de* E *vérifiant* $P(x)$.

Exemple

1. *L'assertion quantifiée "*$\exists\, x \in \mathbb{R},\ \ x^2 = 4$*" est vraie.*
2. *L'assertion quantifiée "*$\exists!\, x \in \mathbb{R}_+^*,\ \ \ln(x) = 1$*" est vraie.*

Quantificateurs mathématiques

Remarque

Notons que si "$\forall\, x \in E,\ P(x)$" est vraie, alors "$\exists\, x \in E,\ P(x)$" est vraie.

Attention :

il faudra manipuler avec précaution les assertions de la forme "$\exists\,!\, x \in E,\ P(x)$" pour lesquelles la notation $\exists\,!$ n'est pas un quantificateur bien qu'il en ait l'air !

En effet, si nous posons

$$R_1 = \text{"}\exists\, x \in E,\ P(x)\text{"} \text{ (c'est l'existence)}$$

et

$$R_2 = \text{"}\forall\, x \in E,\ \forall\, x' \in E,\ ((P(x) \text{ et } P(x')) \Rightarrow (x = x')\text{"} \text{ (c'est l'unicité),}$$

nous avons alors

$$(\exists\,! x \in E, P(x)) \equiv (R_1 \text{ et } R_2).$$

Quantificateurs mathématiques

Proposition (Équivalences logiques et quantificateurs)

Soit $P(x)$, un prédicat, nous avons les équivalences topologiques suivantes :

$$non(\forall\, x \in E,\ P(x)) \quad \equiv \quad (\exists\, x \in E,\ non(P(x)))$$
$$non(\exists\, x \in E,\ P(x)) \quad \equiv \quad (\forall\, x \in E,\ non(P(x)))$$

Exemple

Soient $P(x)$ et $Q(x)$ deux prédicats sur E. Nous avons,

$non(\forall\, x \in E,\ (P(x) \Rightarrow Q(x)) \equiv (\exists\, x \in E,\ (P(x)$ *et* $non(Q(x)))$

$non(\exists\, !\, x \in E,\ P(x)) \equiv (\forall x \in E\ non(P(x))$ *ou* $(\exists\, x \neq y,\ P(x) \wedge P(y)))$

Quantificateurs mathématiques

Definition (Prédicats à deux variables)

Soit $P(x, y)$ un prédicat à deux variables, $x \in E$ et $y \in F$.
L'assertion quantifiée

$$\forall\, x \in E,\ \forall\, y \in F,\ P(x, y),$$

est vraie lorsque tous les éléments $x \in E$ et tous les éléments $y \in F$, vérifient $P(x, y)$.
L'assertion quantifiée

$$\exists\, x \in E,\ \exists\, y \in F,\ P(x, y),$$

est vraie lorsqu'il existe au moins un élément $x \in E$ et qu'il existe au moins un élément $y \in F$ qui vérifient $P(x, y)$.

Quantificateurs mathématiques

Remarque

Nous pouvons combiner des quantificateurs de natures différentes. Mais attention, il faut respecter les règles suivantes :

$$(\forall\, x \in E,\ \forall\, y \in F,\ P(x,y)) \quad \equiv \quad (\forall\, y \in F,\ \forall\, x \in E,\ P(x,y)),$$
$$(\exists\, x \in E,\ \exists\, y \in F,\ P(x,y)) \quad \equiv \quad (\exists\, y \in F,\ \exists\, x \in E,\ P(x,y)).$$

Attention :

il ne faut pas permuter des quantificateurs différents !

$$(\forall\, x \in E,\ \exists\, y \in F,\ P(x,y)) \quad \not\equiv \quad (\exists\, y \in F,\ \forall\, x \in E,\ P(x,y)).$$

Raisonnement par hypothèse auxiliaire

Pour montrer qu'un énoncé Q est vrai, nous nous appuyons sur la tautologie suivante $(P \text{ et } (P \Rightarrow Q)) \Rightarrow Q$. C'est bien une tautologie, comme le montre la table de vérité suivante

P	Q	P ⇒ Q	P et (P ⇒ Q)	(P et (P ⇒ Q)) ⇒ Q
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

Table de vérité pour la tautologie (P et (P ⇒ Q)) ⇒ Q

1. Nous montrons que P est vrai (en pratique il s'agit d'un énoncé évident),
2. puis nous montrons que $P \Rightarrow Q$ est vrai,
3. nous nous retrouvons sur la première ligne de la table de vérité, ce qui montre que Q est vrai.

Raisonnement par l'absurde

Pour montrer qu'un énoncé P est vrai, nous nous appuyons sur l'équivalence logique $((\text{non}(P) \Rightarrow Q)$ et $(\text{non}(P) \Rightarrow \text{non}(Q))) \equiv P$.
Vérifions cela dans la table de vérité ci-dessous

P	Q	non(P)	non(Q)	non(P) ⇒ Q	non(P) ⇒ non(Q)	(non(P) ⇒ Q) et (non(P) ⇒ non(Q))
V	V	F	F	V	V	V
V	F	F	V	V	V	V
F	V	V	F	V	F	F
F	F	V	V	F	V	F

Table de vérité pour la tautologie (non(P) ⇒ Q) et (non(P) ⇒ non(Q))

Il paraît clair que la première et la dernière colonne sont identiques. Nous supposons alors que non(P) est vrai (lignes 3 et 4 du tableau ci-dessus), et nous cherchons alors Q, qui sous cette hypothèse serait à la fois vrai ou faux. Nous disons alors que l'on a obtenu une contradiction ou que l'hypothèse est contradictoire.

Raisonnement par l'absurde

Remarque

Dans la pratique, nous montrons que si nonP est vrai alors on aboutit à une contradiction et on en déduit que P est vrai.

Raisonnement par contraposée

Il faut montrer des résultats faisant apparaître une implication $P \Rightarrow Q$. Ce raisonnement s'appuie sur l'équivalence logique
$(P \Rightarrow Q) \equiv (\text{non}(Q) \Rightarrow \text{non}(P))$. Pour montrer qu'un énoncé Q est vrai, nous utilisons l'équivalence logique ci-dessus.

Raisonnement par contre exemple

Ce raisonnement sert à montrer qu'un énoncé de la forme $\forall\, x \in E,\ \ P(x)$ est faux. Pour cela, nous montrons que sa négation est vraie. Autrement dit $\text{non}(\forall\, x \in E,\ \ P(x)) \ \equiv\ (\exists\, x \in E,\ \text{non}(P(x)))$. Pour cela nous montrons qu'il existe un élément $x \in E$ qui ne vérifie pas $P(x)$.

Exemple

1. *Montrons que* $\forall\, x \in \mathbb{R},\ \ \forall\, \varepsilon > 0,\ \ (|x| < \varepsilon \ \Rightarrow\ x = 0)$ *est faux. La négation de cet énoncé est* $\exists\, x \in \mathbb{R},\ \ \exists\, \varepsilon > 0,\ \ (|x| < \varepsilon \ \text{ et } \ x \neq 0)$. *Nous rappelons en effet que la négation de* $(P \Rightarrow Q)$ *est* $(P \text{ et non}(Q))$.
   Si $x = 1$ *et* $\varepsilon = 2$, *nous avons* $|x| < \varepsilon$ *et* $x \neq 0$, *la négation de l'énoncé est vraie, donc l'énoncé est faux.*
2. *Attention, il ne faut pas confondre* $\forall\, x \in \mathbb{R},\ \ \forall\, \varepsilon > 0,\ \ (|x| < \varepsilon \ \Rightarrow\ x = 0)$ *avec* $\forall\, x \in \mathbb{R},\ \ ((\forall\, \varepsilon > 0,\ \ |x| < \varepsilon) \ \Rightarrow\ x = 0)$.

Raisonnement par récurrence

Ce raisonnement sert à montrer qu'un énoncé du genre

$$\text{“pour tout entier naturel } n \geq n_0,\ P(n)\text{” est vrai.}$$

Il y a deux méthodes pour le prouver.

1. La récurrence classique :
   1. Nous vérifions que l'assertion $P(n_0)$ est vraie.
   2. Supposons que $P(k)$ soit vraie pour un certain $k \geq n_0$. Il faut montrer $P(k+1)$ soit vraie.
2. La récurrence forte :
   1. Nous vérifions que l'assertion $P(n_0)$ est vraie.
   2. Nous supposons que la propriété est vraie pour tous les entiers entre n_0 et k c'est-à-dire on suppose $P(n_0), P(n_0+1), P(n_0+2), \cdots, P(k)$ sont vraies.
   3. On démontre alors que cela implique que $P(k+1)$ est vraie :

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \Longrightarrow P(k+1)$$

Les Applications d'un ensemble vers un autre ensemble

Applications

Soient E et F deux ensembles.

Definition

Une application $f : E \to F$, est définie pour chaque élément $x \in E$, un unique élément de F noté $f(x)$, où E est l'ensemble de départ et F est l'ensemble d'arrivée.

Exemple

1. $$\begin{array}{rccll} f : \mathbb{R} & \to & \mathbb{R} & & \\ x & \mapsto & f(x) = x & & f \text{ est une application.} \end{array}$$

2. $$\begin{array}{rccll} g : \mathbb{N} & \to & \mathbb{N} & & \\ n & \mapsto & f(n) = n - 1. & & g \text{ n'est pas une application.} \end{array}$$

Applications

Remarque

1. *Le graphe de* $f : E \to F$ *est* $\Gamma_f = \{(x; y) \in E \times F \text{ tel que } y = f(x)\}$.
2. *Soit* $f : E \to F$ *et* $g : G \to H$ *deux applications.* $f = g$ *si et seulement si* $E = G$ *et* $F = H$ *et* $\forall\, x \in E, f(x) = g(x)$.
3. *Soit* $f : E \to F$ *une application. Fixons* $y \in F$*, tout élément* $x \in E$ *tel que* $y = f(x)$ *est un antécédent de* y.

Notation

- *On note* $\mathcal{F}(E, F)$ *l'ensemble de toutes les applications de* E *dans* F.
- *On note* **id** *l'application identité*

$$\begin{array}{rccc} id : & E & \to & F \\ & x & \mapsto & f(x) = x \end{array}$$

Image directe et image réciproque

Soient E et F deux ensembles.

Definition (Image directe)

Soit $A \subset E$ et $f : E \to F$, l'image directe de A par f est l'ensemble :

$$f(A) = \{f(x), \text{ tel que } x \in A\} \subset F.$$

Definition (Image réciproque)

Soit $B \subset F$ et $f : E \to F$, l'image réciproque de A par f est l'ensemble :

$$f^{-1}(B) = \{x \in E \text{ tel que } f(x) \in B\} \subset E.$$

Image directe et image réciproque

Exemple

Soit l'application $f : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & f(x) = 2x + 1. \end{array}$ *Soit* $A = \{0, 1, 2\}$, *alors*

$f(A) = \{f(x)$ *tel que* $x \in A\} = \{f(0), f(1), f(2)\} = \{1, 3, 5\}$.

Soit $B = \{5\}$, *alors*

$f^{-1}(B) = \{x \in E \ t.q \ f(x) \in B\} = \{x \in E \ t.q \ f(x) = 5\} = \{2\}$.

Propriété

Soit $f : E \to F$ *une application. Soient* A_1 *et* A_2 *deux parties de* E. *Alors,*

1. $f(A_1 \bigcup A_2) = f(A_1) \bigcup f(A2)$.
2. $f(A_1 \bigcap A_2) \subset f(A_1) \bigcap f(A_2)$.
3. $A_1 \subset A_2 \Longrightarrow f(A_1) \subset f(A_2)$.
4. $A_1 \subset f^{-1}(f(A_1))$.

Image directe et image réciproque

Propriété

Soient B_1 et B_2 deux parties de F.

1. $f^{-1}(B_1 \bigcup B_2) = f^{-1}(B_1) \bigcup f^{-1}(B_2)$.
2. $f^{-1}(B_1 \bigcap B_2) = f^{-1}(B_1) \bigcap f^{-1}(B_2)$.
3. $B_1 \subset B_2 \Longrightarrow f^{-1}(B1) \subset f^{-1}(B_2)$.

Injection

Definition

Soit $f : E \to F$ une application. On dit que f est injective (ou une injection) si tout élément de F admet au plus un antécédent, c'est-à-dire, $\forall\, x, x' \in E :\ f(x) = f(x') \Longrightarrow x = x'$. Ou
$\exists\, x, x' \in E :\ x \neq x' \Longrightarrow f(x) \neq f(x')$.

Exemple

a) *l'application* $\begin{array}{lll} f : \mathbb{N} & \to \mathbb{N} \\ n & \mapsto 2n+1 \end{array}$ *est injective car :*

$\forall\, n, n' \in E :\ f(n) = f(n') \Longrightarrow 2n+1 = 2n'+1 \Longrightarrow 2n = 2n' \Longrightarrow n = n'$.

b) *l'application* $\begin{array}{lll} g : \mathbb{R} & \to \mathbb{R} \\ x & \mapsto 5x+3 \end{array}$ *est injective car :*

$\forall\, x, x' \in E :\ f(x) = f(x') \Longrightarrow 5x+3 = 5x'+3 \Longrightarrow 5x = 5x' \Longrightarrow x = x'$.

Surjection

Definition

Soit $f : E \to F$ une application. On dit que f est surjective (ou une surjection) si tout élément de F admet un antécédent, c'est-à-dire, $\forall\, y \in F,\ \exists\, x \in E :\ f(x) = y$.

Exemple

- $\begin{array}{lll} f : \mathbb{N} & \to \mathbb{N} \\ n & \mapsto 2n+1 \end{array}$ *f n'est pas surjective, en effet si on suppose qu'elle est surjective c'est-à-dire*

  $\forall\, y \in \mathbb{N},\ \exists\, n \in \mathbb{N} :\ f(n) = y \Longrightarrow 2n+1 = y \implies n = \dfrac{y-1}{2}$. *Ce qui est absurde car ce dernier n'est pas forcément entier.*

- $\begin{array}{lll} g : \mathbb{R} & \to \mathbb{R} \\ x & \mapsto 5x+3 \end{array}$ *g est surjective car :*

  $\forall\, y \in \mathbb{R},\ \exists\, x \in \mathbb{R} : g(x) = y \implies 5x+3 = y \Longrightarrow x = \dfrac{y-3}{5} \in \mathbb{R}.$

Bijection

Definition

Soitf : $E \to F$ une application. On dit que f est bijective (ou une bijection) si f est à la fois surjective et injective, c'est-à-dire,
$\forall\, y \in F,\ \exists!\, x \in E : f(x) = y$.
En d'autre termes tout élément de F a un unique antécédent par f.

Exemple

a) $f : \begin{array}{l} \mathbb{N} \to \mathbb{N} \\ n \mapsto 2n+1 \end{array}$ *f n'est pas bijective car elle n'est pas surjective.*

b) *L'application g précédemment définie est bijective.*

La composition d'application

Definition

Soient E, F, G trois ensembles et f, g deux applications telles que : $f : E \to F \quad g : F \to G$. On peut déduire une application de E dans G notée $g \circ f$ appelée application composée de f et g par $\forall\, x \in E,\ g \circ f(x) = g(f(x))$.

Exemple

Soit $f : \begin{array}{l} \mathbb{R} \to \mathbb{R}_+ \\ x \mapsto x^2 + 1 \end{array}$ *et* $g : \begin{array}{l} \mathbb{R}_+ \to \mathbb{R} \\ x \mapsto \sqrt{x}, \end{array}$ *alors* $g \circ f : \begin{array}{l} \mathbb{R} \to \mathbb{R} \\ x \mapsto \sqrt{x^2 + 1}. \end{array}$

La composition d'application

Proposition

Soit $f : E \to F$ et $g : F \to G$ deux applications.

1. *La composée de deux injections est une injection, c'est-à-dire, (Si f et g sont injectives, alors $g \circ f$ est injective).*
2. *La composée de deux surjections est une surjection, c'est-à-dire, (Si f et g sont surjectives, alors $g \circ f$ est surjective).*
3. *La composée de deux bijections est une bijection, c'est-à-dire, (Si f et g sont bijectives, $g \circ f$ est bijective).*
4. *Si f et g sont bijectives. Alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

La composition d'application

Démonstration :

1. Supposons que f et g sont injectives, montrons que $g \circ f$ est injective. $\forall\, x_1,\, x_2 \in E,\ (g \circ f)(x_1) = g \circ f(x_2)$ puisque g est injective on aura : $g(f(x_1)) = g(f(x_2)) \Longrightarrow f(x_1) = f(x_2)$. Or f est injective ainsi on en déduit l'implication : $(g \circ f)(x_1) = (g \circ f)(x_2) \Longrightarrow x_1 = x_2$, ce qui montre alors que $g \circ f$ est injective.
2. (Exercice à faire)
3. (Exercice à faire)
4. (Exercice à faire)

La composition d'application

Proposition

1. *Si $g \circ f$ est injective, alors f est injective.*
2. *Si $g \circ f$ est surjective, alors f est surjective.*
3. *Si $g \circ f$ est bijective, alors f est injective et g est surjective.*

Remarque

Lorsqu'une application f est bijective cela veut dire que l'application réciproque f^{-1} existe. De plus, f^{-1} est aussi bijective de F sur E et $(f^{-1})^{-1} = f$.

Proposition

Si $f : E \to F$ est une bijection, alors $f^{-1} \circ f = Id$ de E et $f \circ f^{-1} = Id$ de F.

Nombres complexes

Nombres complexes : forme algébrique

Definition ($\mathbb{R}^2$)

L'ensemble $\mathbb{R}^2$ est l'ensemble des couples (a, b) de nombres réels.
Deux éléments (a, b) et (a', b') de $\mathbb{R}^2$ sont égaux si et seulement si $a = a'$ et $b = b'$.

Maintenant que nous avons défini $\mathbb{R}^2$ essayons de mettre cet ensemble en relation avec les complexes.

Definition (Nombres complexes)

L'ensemble des nombres complexes, noté $\mathbb{C}$ est l'ensemble $\mathbb{R}^2$ muni d'une addition et d'une multiplication définies pour tous (a, b) et $(a', b') \in \mathbb{R}^2$ par

1. $(a, b) + (a', b') = (a + a', b + b')$,
2. $(a, b)(a', b') = (aa' - bb', ab' + a'b)$.

Nombres complexes : forme algébrique

Notation (Convention pour les réels)

1. *Pour tout $x \in \mathbb{R}$, nous conviendrons d'identifier le nombre complexe $(x, 0)$ et le réel x.*
2. *L'ensemble des réels est donc identifié à l'ensemble des nombres complexes de la forme $(x, 0)$ où $x \in \mathbb{R}$.*

Notation (Imaginaire)

Le nombre complexe $(0, 1)$ est noté i.

Nombres complexes : forme algébrique

En conséquence, nous avons alors la possibilité d'écrire :

1. pour tout $(a, b) \in \mathbb{R}^2$,
$$(a, b) = (a, 0) + (0, b),$$
2. pour tout $b \in \mathbb{R}$,
$$i(b, 0) = (0, 1)(b, 0) = (0, b),$$
3. Et finalement nous pouvons écrire pour tout $(a, b) \in \mathbb{R}^2$,
$$(a, b) = a + ib.$$

Partie réelle, partie imaginaire et conjugué

Propriété (Égalité de deux complexes)

Soient a, a', b, b' des réels quelconques, nous avons les deux propriétés suivantes

1. $a + ib = 0$ *équivaut à* $a = 0$ *et* $b = 0$,
2. $a + ib = a' + ib'$ *équivaut à* $a = a'$ *et* $b = b'$.

Definition (Partie réelle partie imaginaire)

Soit $z \in \mathbb{C}$ un nombre complexe. Il existe un couple unique $(a, b) \in \mathbb{R}^2$ tel que $z = a + ib$.

1. $a + ib$ est appelée forme algébrique du complexe z,
2. a est appelée partie réelle de z, on la note $\mathrm{Re}(z)$,
3. b est appelée partie imaginaire de z, on la note $\mathrm{Im}(z)$.

Partie réelle, partie imaginaire et conjugué

Nous noterons l'ensemble des imaginaires purs $i\mathbb{R}$.

Propriété (Réel et Imaginaire pur)

1. *Un nombre complexe est réel lorsque sa partie imaginaire pure est nulle, c'est à dire : $z \in \mathbb{R}$ si et seulement si $Im(z) = 0$.*
2. *Un nombre complexe est imaginaire pur lorsque sa partie réelle est nulle, c'est à dire $z \in i\mathbb{R}$ si et seulement si $Re(z) = 0$.*

Propriété (Addition et produit : forme algébrique)

Soient a, a', b, b' des réels quelconques, nous avons les deux propriétés suivantes

1. *Somme : $(a + ib) + (a' + ib') = (a + a') + i(b + b')$,*
2. *Produit : $(a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b)$,*
3. *Carré de i : $i^2 = -1$. Le nombre i ne peut pas être un réel (c'est un nombre négatif égal à un carré).*

Definition (Conjugué)

Soit $z \in \mathbb{C}$ un nombre complexe de notation algébrique $z = a + ib$, avec $a, b \in \mathbb{R}$. Nous appelons conjugué de z le nombre complexe $a - ib$, que nous noterons $\overline{z}$.

Nous avons quelques propriétés pour les conjugués.

Propriété (Propriétés du conjugué)

Soit $z \in \mathbb{C}$,

1. *le conjugué de $\overline{z}$ est, $\overline{(\overline{z})} = z$,*
2. $Re(z) = \frac{1}{2}(z + \overline{z})$ *et* $Im(z) = \frac{1}{2i}(z - \overline{z})$,
3. $z \in \mathbb{R}$ *si et seulement si* $z = \overline{z}$,
4. $z \in i\mathbb{R}$ *si et seulement si* $z = -\overline{z}$.

Ainsi, deux nombres complexes z et z' sont égaux si et seulement si $\mathrm{Re}(z) = \mathrm{Re}(z')$ et $\mathrm{Im}(z) = \mathrm{Im}(z')$.

Calculs sur les complexes

Nous avons plusieurs propriétés supplémentaires sur l'addition et la multiplication des complexes.

Propriété (Propriétés de l'addition)

Soient $z, z', z'' \in \mathbb{C}$, l'addition dans $\mathbb{C}$ est

1. *Commutative :* $z + z' = z' + z$,
2. *Associative :* $z + (z' + z'') = (z + z') + z''$,
3. 0 *est l'élément neutre :* $z + 0 = z$,
4. *Symétrique : tout complexe z admet un symétrique dans $\mathbb{C}$, c'est $-z$ (l'opposé de z), sous forme algébrique, si $z = a + ib$, avec $a, b \in \mathbb{R}$, alors $-z = -a - ib$.*

Calculs sur les complexes

Propriété (Propriétés de la multiplication)

Soient $z, z', z'' \in \mathbb{C}$, la multiplication dans $\mathbb{C}$ est

1. *Commutative :* $zz' = z'z$,
2. *Associative :* $z(z'z'') = (zz')z''$,
3. 1 *est l'élément neutre :* $z \times 1 = z$,
4. *Pour tout nombre complexe* $z \neq 0$, *il existe* $z' \in \mathbb{C}$, $z' \neq 0$ *tel que* $zz' = 1$. *Nous notons ce nombre* $\frac{1}{z}$ *ou encore* z^{-1}, *et c'est l'inverse de* z. *Sous forme algébrique, pour* $z = a + ib \neq 0$, *alors* $\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}$.

Calculs sur les complexes

Propriété (Sommes et produits de conjugués)

Soient $z, z' \in \mathbb{C}$,

1. $\overline{z+z'} = \overline{z} + \overline{z}'$,
2. $\overline{zz'} = \overline{z}\ \overline{z}'$,
3. *pour* $z' \neq 0$, $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z}'}$.

Propriété (Sommes des $n+1$ premières puissances de z)

Soit $z \in \mathbb{C}$, avec $z \neq 1$, alors

$$1 + z + z^2 + \ldots + z^n = \frac{1 - z^{n+1}}{1 - z}.$$

Nombres complexes : forme géométrique

Dans toute cette section nous allons travailler dans un plan orienté. Nous ne pouvons pas prendre $(O, \overrightarrow{i}, \overrightarrow{j})$ étant donné que désormais, i est choisi comme le nombre imaginaire pur dont le carré vaut -1. Par conséquent, nous allons travailler dans le plan orthonormal direct $(O, \overrightarrow{e_1}, \overrightarrow{e_2})$, où $O(0,0)$ est l'origine, et les vecteurs $\overrightarrow{e_1}$ et $\overrightarrow{e_2}$ sont orthogonaux et de norme 1.
Par conséquent, pour tous réels a et b, $M(a,b)$ désignera le point M de coordonnées (a,b).

Definition (Image et affixe)

1. Soit $z \in \mathbb{C}$, soient $a, b \in \mathbb{R}$, avec $a = \mathrm{Re}(z)$ et $b = \mathrm{Im}(z)$, le point $M(a,b)$ est appelé l'image de z.
2. Soit $M(a,b)$ un point du plan, le nombre complexe $z = a + ib$ est appelé l'affixe de M. On pourra noter quelques fois $\mathrm{aff}(M)$ l'affixe du point M.

Nombres complexes : forme géométrique

Definition (Image et affixe)

1. Soit $z \in \mathbb{C}$, soient $a, b \in \mathbb{R}$, avec $a = \text{Re}(z)$ et $b = \text{Im}(z)$, le vecteur $a\overrightarrow{e_1} + b\overrightarrow{e_2}$ est l'image vectorielle de z.
2. Soit $\overrightarrow{u}$ un vecteur du plan de coordonnées (a, b) dans la base $(\overrightarrow{e_1}, \overrightarrow{e_2})$, Le nombre complexe $a + ib$ est appelé l'affixe du vecteur $\overrightarrow{u}$. On pourra également noter aff($\overrightarrow{u}$) l'affixe du vecteur u.

Par conséquent, pour tout point M du plan, aff(M)=aff($\overrightarrow{OM}$).

Interprétation géométrique

Commençons par la somme de deux complexes :

Propriété (Affixe de la somme de vecteurs)

Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs du plan. Alors

$$aff(\overrightarrow{u} + \overrightarrow{v}) = aff(\overrightarrow{u}) + aff(\overrightarrow{v}).$$

Propriété (Affixe et points)

Soient A et B deux points du plan. Alors l'affixe du vecteur $\overrightarrow{AB}$ est donnée par : $aff(\overrightarrow{AB}) = aff(B) - aff(A)$.

Propriété (Translation et somme)

Soit $p \in \mathbb{C}$ un complexe. Soit $\overrightarrow{u}$ un vecteur d'affixe p. La translation de vecteur $\overrightarrow{u}$ d'un point M du plan d'affixe z, est un point M' du plan d'affixe $z' = z + p$.

Interprétation géométrique

Propriété (Réflexion et conjugué)

La réflexion d'axe $(O, \overrightarrow{e_1})$ d'un point M du plan d'affixe z est le point M' du plan d'affixe $\overline{z}$.

En d'autres termes, l'image par la réflexion d'axe $(O, \overrightarrow{e_1})$ de $M(a, b)$ est $M(a, -b)$.

Module d'un nombre complexe

Definition

Soit $z \in \mathbb{C}$, d'image M. Le module de z, noté $|z|$, est la norme $\|\overrightarrow{OM}\|$.

Propriété

1. *Soient z et $z' \in \mathbb{C}$ deux complexes, d'images respectives M et M' alors $|z - z'| = \|\overrightarrow{MM'}\|$.*
2. *Pour tout complexe $z = a + ib$, où a et b sont réels, $|z| = \sqrt{a^2 + b^2}$.*
3. $|z|^2 = z\overline{z}$ *ou encore* $|z| = \sqrt{z\overline{z}}$; $|z| = |\overline{z}| = |-\overline{z}| = |-z|$.
4. $|zz'| = |z||z'|$ *et si* $z \neq 0$ *alors* $|\frac{1}{z}| = \frac{1}{|z|}$ *et* $|\frac{z'}{z}| = \frac{|z'|}{|z|}$.
5. $|z^n| = |z|^n$ *où* $n \in \mathbb{N}$ *et même* $\mathbb{Z}$ *si* $z \neq 0$.
6. $|z| = 0$ *si et seulement si* $z = 0$.
7. $|Re(z)| \leq |z|$ *et* $|Im(z)| \leq |z|$.

Interprétation géométrique du module

Propriété (Inégalité triangulaire)

Soient z et z' deux complexes, nous avons

$$|z + z'| \leq |z| + |z'|.$$

Propriété (Cercles, disques)

Soit a un nombre complexe, soit $r > 0$ un réel. Notons A l'image de a alors nous avons :

1. $|z - a| = r$ *décrit le cercle de centre A et de rayon r,*
2. $|z - a| \leq r$ *le disque fermé (contenant le bord) de centre A et de rayon r,*
3. $|z - a| < r$ *le disque ouvert (sans les bord) de centre A et de rayon r.*

Remarquons que si $a = 0$, alors $A = O$ (l'origine) et me cercles et disques sont centrés en O.

Racines carrées et équations du second degré

Soit $z \in \mathbb{C}$, une racine carrée de z est un nombre complexe ω tel que $\omega^2 = z$.

Proposition (Racine carrée)

Soient z un nombre complexe quelconque, alors z admet deux racines carrées complexes ω et $-\omega$.

Attention : contrairement au cas réel, qui nous dit que si $x \in \mathbb{R}_+$ est un réel positif ou nul, nous avons deux racines de ce nombre qui sont $\sqrt{x}$ et $-\sqrt{x}$, mais nous privilégions quand même le fait de dire que $\sqrt{x}$ est la racine réelle de x.
Pour les complexes nous ne privilégions pas une racine par rapport à une autre parce que z se trouve n'importe où dans le plan. Parler de complexe positif n'a pas de sens. Donc on ne privilégie pas de racine en particulier, et on parle alors de ω comme une racine de z.

Équation du second degré coef. complexes

Proposition (Équation du second degré coef. complexes)

L'équation du second degré $az^2 + bz + c = 0$, avec a, b et $c \in \mathbb{C}$, et en plus $a \neq 0$ possède deux solutions complexes z_1 et z_2 (qui peuvent être confondues).
Si l'on pose $\Delta = b^2 - 4ac \in \mathbb{C}$ le discriminant, et δ une racine carrée de Δ, alors les solutions sont

$$z_1 = \frac{-b + \delta}{2a} \text{ et } z_2 = \frac{-b - \delta}{2a}.$$

Si on s'autorisait à écrire $\delta = \sqrt{\Delta}$ nous aurions le même réultat que l'on connait quand a, b et c sont réels (voir ci-dessous). Mais on ne le fait pas.
Attention : La difficulté ici c'est le calcul de δ sachant qu'on a pas le droit d'écrire "$\sqrt{\text{nombre complexe}}$".

Équation du second degré coef. complexes

Une méthode classique pour calculer la racine carrée d'un nombre complexe, comme on souhaite le faire pour δ, consiste à :

- Écrire Δ sous la forme $\Delta = a + ib$
- Écrire δ sous la forme $\delta = x + iy$
- Chercher δ revient à résoudre d'une part $\delta^2 = \Delta$ et d'autre part $|\delta^2| = |\Delta|$ ce qui revient à faire $(x + iy)2 = a + ib$ et $|\delta^2| = |\Delta|$ c'est-à-dire poser le système

$$\begin{cases} x^2 - y^2 = & a \\ 2xy = & b \\ x^2 + y^2 = & \sqrt{a^2 + b^2} \end{cases}$$

Exemple (Prenons $z = 3 + 4i$)

$|z| = \sqrt{3^2 + 4^2} = 5$ *Alors* $x = \sqrt{\frac{5+3}{2}} = 2$ *et* $y = \sqrt{\frac{5-3}{2}} = 1$. *D'où les deux racines de* $z = 3 + 4i$ *sont* $\delta = 2 + i$ *et* $\delta = -2 - i$

Si par contre les coefficients du polynôme sont réels, nous avons

Proposition (Équation du second degré coef. réels)

L'équation du second degré $az^2 + bz + c = 0$, *avec* a, b *et* $c \in \mathbb{R}$, *et en plus* $a \neq 0$. *Alors le discriminant* $\Delta = b^2 - 4ac$ *est réel et nous avons trois cas :*

1. *si* $\Delta = 0$, *nous avons une racine double réelle qui vaut* $\dfrac{-b}{2a}$,
2. *si* $\Delta > 0$, *nous avons deux solutions réelles* $\dfrac{-b+\sqrt{\Delta}}{2a}$ *et* $\dfrac{-b-\sqrt{\Delta}}{2a}$,
3. *si* $\Delta < 0$, *nous avons deux solutions complexes (et non réelles)* $\dfrac{-b+i\sqrt{\Delta}}{2a}$ *et* $\dfrac{-b-i\sqrt{\Delta}}{2a}$,

Théorème fondamental de l'algèbre

Theorem (d'Alembert-Gauss)

Soit $P(z) = a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0$ un polynôme à coefficients complexes et de degré n.
Alors l'équation $P(z) = 0$ admet exactement n solutions complexes comptées avec leur multiplicité (racines doubles, racines triples, etc. suivant les cas).
Ceci veut dire qu'il existe z_1, z_2, ... ,z_n, n nombres complexes (parfois confondus) tels que

$$P(z) = a_n(z - z_1)(z - z_2)...(z - z_n).$$

Argument et trigonométrie

Considérons le nombre complexe $z = x + iy$. Supposons que son module $|z| = 1$, alors nous avons $x^2 + y^2 = 1$. Et donc, comme vu précédemment, le point $M(x, y)$ est sur le cercle centré en O et de rayon 1. Nous appelons ce cercle, le cercle unité.
Par définition du cosinus et du sinus, l'abscisse (ou partie réelle de z), x est notée $\cos(\theta)$ et l'ordonnée (ou partie imaginaire de z), y est notée $\sin(\theta)$, où θ est une mesure de l'angle entre l'axe des réels (abscisses) et le vecteur $\overrightarrow{OM}$.

Definition (Argument)

Pour tout complexe $z \in \mathbb{C}$ non nul, un nombre $\theta \in \mathbb{R}$ et tel que $z = |z|(\cos(\theta) + i\sin(\theta))$ est appelé argument de z et on le note $\theta = \arg(z)$.
Cet argument est défini modulo 2π (c'est à dire à $2k\pi$ près, $k \in \mathbb{Z}$).
Nous pouvons imposer quelques fois à cet argument d'être unique si on rajoute la condition $\theta \in]-\pi, \pi]$.

En conséquence : deux nombres réels θ et θ' sont arguments d'un même complexe z si et seulement s'il existe un entier relatif $k \in \mathbb{Z}$ tel que $\theta = \theta' + 2k\pi$. On écrit cette dernière égalité

$$\theta' \equiv \theta \mod (2\pi), \quad \text{que nous lisons “}\theta' \text{ est congru à } \theta \text{ modulo } 2\pi\text{”.}$$

D'autre part, nous avons la relation entre les arguments et les angles :

1. pour tout nombre $z \in \mathbb{C}^*$, d'image M, l'argument de z est l'angle $(\overrightarrow{e_1}, \overrightarrow{OM})$ que l'on note
$$\arg(z) = (\overrightarrow{e_1}, \overrightarrow{OM}).$$
2. D'autre part, étant donné $z \in \mathbb{C}^*$, on considère M d'affixe z. Toute mesure θ de l'angle $(\overrightarrow{e_1}, \overrightarrow{OM})$ est appelé argument de z et noté $\arg(z)$.

Argument et trigonométrie

Nous avons les propriétés suivantes

Propriété (Propriétés des arguments)

Soient z et z' deux nombres complexes ***non nuls****. Nous avons*

1. $\arg(zz') \equiv \arg(z) + arg(z')\ (mod\ 2\pi)$,
2. $\arg(z^n) \equiv n \arg(z)\ (mod\ 2\pi)$,
3. $\arg(\frac{1}{z}) \equiv -\arg(z)\ (mod\ 2\pi)$,
4. $\arg(\frac{z'}{z}) \equiv \arg(z') - \arg(z)\ (mod\ 2\pi)$,
5. $\arg(\overline{z}) \equiv -\arg(z)\ (mod\ 2\pi)$.

Une conséquence directe de la propriété 4 est que si l'on a deux complexes non nuls z et z' alors $\arg(z) = \arg(z')$ si et seulement si $\frac{z'}{z}$ est un réel strictement positif. car les nombres complexes d'argument 0 sont les réels strictement positifs.

Formule de Moivre et notation exponentielle

Propriété (Formule de Moivre)

Pour tout réel θ et tout entier n, nous avons

$$(\cos(\theta)) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta).$$

Nous définissons alors la notation exponentielle

Definition (Notation exponentielle)

Nous définissons l'exponentielle complexe pour tout réel θ par

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

En conséquence, tout nombre complexe s'écrit de la façon suivante

$$z = \rho e^{i\theta},$$

où $\rho = |z|$ est le module de z et $\theta = \arg(z)$ est un argument de z. C'est ce que l'on appelle la forme trigonométrique de z.
Remarquons que si $|z| = 1$, alors nous avons $z = e^{i\theta}$.

Formule de Moivre et notation exponentielle

Propriété (Formule de Moivre)

Pour tout réel θ et tout entier n, nous avons

$$(\cos(\theta)) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta).$$

Nous définissons alors la notation exponentielle

Definition (Notation exponentielle)

Nous définissons l'exponentielle complexe pour tout réel θ par

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

En conséquence, tout nombre complexe s'écrit de la façon suivante

$$z = \rho e^{i\theta},$$

où $\rho = |z|$ est le module de z et $\theta = \arg(z)$ est un argument de z. C'est ce que l'on appelle la forme trigonométrique de z.
Remarquons que si $|z| = 1$, alors nous avons $z = e^{i\theta}$.

Formule de Moivre et notation exponentielle

Nous avons alors les propriétés suivantes

Propriété (Propriétés exponentielles de complexes)

Soient $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$ deux nombres complexes non nuls, nous avons

1. $zz' = \rho\rho' e^{i\theta} e^{i\theta'} = \rho\rho' e^{i(\theta+\theta')}$,
2. $z^n = (\rho e^{i\theta})^n = \rho^n (e^{i\theta})^n = \rho^n e^{in\theta}$,
3. $\dfrac{1}{z} = \dfrac{1}{\rho e^{i\theta}} = \dfrac{1}{\rho} e^{-i\theta}$,
4. $\overline{z} = \rho e^{-i\theta}$,
5. *Formule de Moivre :* $(e^{i\theta})^n = e^{in\theta}$ *(le module est ici égal à 1),*
6. $\rho e^{i\theta} = \rho' e^{i\theta'}$ *si et seulement si* $\rho = \rho$ *et* $\theta \equiv \theta'$ *(mod* 2π*).*

En conséquence,

$$e^{i\theta} = 1 \text{ si et seulement s'il existe } k \in \mathbb{Z}, \text{ tel que } \theta = 2k\pi.$$

Formule de Moivre et notation exponentielle

Donnons maintenant quelques propriétés géométriques sur les arguments, les angles et l'orthogonalité

Propriété (Angle formé par trois points)

Étant donnés trois points A, B et C dans le plan complexe d'affixe respective a, b et c, avec $A \neq C$ et $B \neq C$, on a alors

$$(\overrightarrow{CA}, \overrightarrow{CB}) = \arg\left(\frac{c-b}{c-a}\right).$$

Propriété (Alignement)

Étant donnés trois points A, B et C dans le plan complexe d'affixe respective a, b et c, avec $A \neq C$ et $B \neq C$, on a alors :

"A, B et C sont alignés si et seulement si $\left(\frac{c-b}{c-a}\right)$ *est réel".*

Propriété (Perpendiculaire)

Étant donnés trois points A, B et C dans le plan complexe d'affixe respective a, b et c, avec $A \neq C$ et $B \neq C$, on a alors

"les droites (CA) et (CB) sont perpendiculaires si et seulement si $\left(\dfrac{c-b}{c-a}\right)$ est imaginaire pur".

Rappelons ici quelques angles connus

Mesure de l'angle	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π
Valeur du cosinus	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	-1
Valeur du sinus	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	0
Valeur de la tangente	0	$\frac{1}{\sqrt{3}}$	1	$\sqrt{3}$	$\times$	0

Racines nièmes d'un complexe

Nous avons vu un peu plus haut les racines carrées d'un nombre complexe. Allons plus loin ici en étudiant les racines nièmes.

Definition (Racine nième)

Soient $z \in \mathbb{C}$ un nombre complexe, et $n \in \mathbb{N} \setminus \{0, 1\}$ (c'est à dire que $n \neq 0$ et 1). Une racine nième de z est un nombre complexe ω tel que

$$\omega^n = z.$$

Propriété (Racines nième d'un complexe)

Tout nombre complexe $z \in \mathbb{C}$ non nul, qui s'écrit $z = \rho e^{i\theta}$ admet exactement n racines nièmes, ce sont les nombres ω_k définis pour tout $k = 0, ..., n-1$ par

$$w_k = \sqrt[n]{\rho} e^{i\frac{\theta+2k\pi}{n}}$$

Remarquons que si l'on pose $\omega_0 = \sqrt[n]{\rho} e^{i\theta/n}$ et $\tilde{\omega} = e^{i2\pi/n}$ alors $\omega_k = \omega_0 \tilde{\omega}^k$.

Racines nièmes d'un complexe

Un cas particulier est la propriété suivante :

Propriété (Racines nième de 1)

Les n racines nièmes de 1 *sont* $\omega_k = e^{2ik\pi/n}$, $k = 0, ..., n-1$.

Quelques applications trigonométriques

Rappelons les formules de l'addition de sinus et cosinus.

Propriété (Formules d'addition)

Pour tous réels a et b nous avons

$$\begin{aligned}
\cos(a+b) &= \cos(a)\cos(b) - \sin(a)\sin(b),\\
\sin(a+b) &= \sin(a)\cos(b) + \sin(b)\cos(a),\\
\cos(a-b) &= \cos(a)\cos(b) + \sin(a)\sin(b),\\
\sin(a-b) &= \sin(a)\cos(b) - \sin(b)\cos(a).
\end{aligned}$$

Pour la tangente nous avons

Propriété (Formule de la tangente)

Pour tous réels $a \neq \frac{\pi}{2}\ mod(\pi)$, $b \neq \frac{\pi}{2}\ mod(\pi)$ et $a+b \neq \frac{\pi}{2}\ mod(\pi)$ nous avons

$$\tan(a+b) = \frac{\tan(a)+\tan(b)}{1-\tan(a)\tan(b)}.$$

Formules de duplication de l'argument

Propriété (Formules de duplication)

Pour tous réels a nous avons

$$\begin{aligned}
\cos(2a) &= \cos^2(a) - \sin^2(a) = 2\cos^2(a) - 1 = 1 - 2\sin^2(a), \\
\sin(2a) &= 2\sin(a)\cos(a), \\
\tan(2a) &= \frac{2\tan(a)}{1-\tan^2(a)}, \quad a \neq \pi \, mod\,(\pi), \quad et \quad a \neq \frac{\pi}{4} \, mod\,(\pi/2)
\end{aligned}$$

Propriété (Formules d'Euler)

Pour tout réel θ, nous avons

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad et \quad \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Formules de duplication de l'argument

Il y a quelques applications aux formules d'Euler et notamment les formules de linéarisation

Propriété (Formules de linéarisation)

Pour tous réels a et b nous avons

$$\begin{aligned}
\cos(a)\cos(b) &= (\cos(a+b)+\cos(a-b))/2,\\
\sin(a)\sin(b) &= (\cos(a-b)-\cos(a+b))/2,\\
\sin(a)\cos(b) &= (\sin(a+b)+\sin(a-b))/2,\\
\sin(a)\cos(a) &= \sin(2a)/2,\\
\cos^2(a) &= \frac{1+\cos(2a)}{2},\\
\sin^2(a) &= \frac{1-\cos(2a)}{2}.
\end{aligned}$$

Formules de duplication de l'argument

et si on pose $p = a + b$ et $q = a - b$, nous obtenons

Propriété (Formules de conversion de somme en produit)

Pour tous réels p et q nous avons

$$\cos(p) + \cos(q) = 2\cos(\frac{p+q}{2})\cos(\frac{p-q}{2}),$$

$$\cos(p) - \cos(q) = -2\sin(\frac{p+q}{2})\sin(\frac{p-q}{2}),$$

$$\sin(p) + \sin(q) = 2\sin(\frac{p+q}{2})\cos(\frac{p-q}{2}),$$

$$\sin(p) - \sin(q) = 2\cos(\frac{p-q}{2})\cos(\frac{p+q}{2}),$$

Nombres complexes en géométrie

Nous considérons le plan rapporté au repère orthonormal $(O, \overrightarrow{e_1}, \overrightarrow{e_2})$. Tout point M de coordonnées (x, y) peut être repéré par son affixe $z = x + iy$.

Propriété (Homothétie)

L'homothétie de centre A, tel que aff(A)= z_0, et de rapport $k \in \mathbb{R}\backslash\{0, 1\}$ est l'application du plan dans lui-même qui à tout point M d'affixe z associe le point M' d'affixe z' tel que :
$z' - z_0 = k(z - z_0)$ ou aussi $z' = kz + (1 - k)z_0$.

Propriété (Homothétie de rapport a)

L'application $z \mapsto z' = az + b$ où $a \in \mathbb{R}\backslash\{0, 1\}$, $b \in \mathbb{C}$ représente une homothétie de rapport a.
Si $a = 1$ nous avons une translation $z \mapsto z' = z + b$, où $b = z_0$.

Conséquence : la réciproque d'une homothétie h, représentée par $z \mapsto az + b$ est une homothétie de même centre.

Propriété (Composée d'homothéties)

Soient f et g deux homothéties (ou translations) du plan, représentées respectivement par

$$\varphi : z \mapsto az + b \text{ et } \psi : z \mapsto a'z + b, \text{ avec } aa' \neq 0.$$

La composée $g \circ f$ est représentée par

$$\psi \circ \phi : z \mapsto a'(az + b) + b' = aa'z + a'b + b'.$$

Rotation, interprétation de $z \mapsto az + b$, avec $|a| = 1$

Propriété (Rotation)

Étant donné un point A d'affixe z_0, la rotation de centre A et d'angle α, est l'application qui transforme un point M d'affixe z en M' d'affixe z' telle que

$$z' - z_0 = (z - z_0)e^{i\alpha}$$

Conséquence : l'application $z \mapsto az + b$, avec $|a| = 1$ s'interprète géométriquement comme

1. une rotation d'angle $\alpha = \arg(a)$, lorsque $a \neq 1$,
2. la translation de vecteur $\overrightarrow{u}$, avec $b = \text{aff}(\overrightarrow{u})$ lorsque $a = 1$

La réciproque d'une rotation de centre A et d'angle α est la rotation de même centre A et d'angle $-\alpha$.

Chapitre 6 :Arithmétique

Arithmétique

Le but de ce chapitre est de formaliser ce que nous faisons (plus ou moins naturellement) depuis l'école primaire sans trop vraiment se poser de questions : que ce soient la manipulation des nombres premiers, les divisions euclidiennes, le calcul des PPCM (Plus Petit Commun Multiple) et des PGCD (Plus Grand Commun Diviseur), des calculs qui nous semblent aussi vieux que le monde, et qui sont pourtant d'une grande modernité.

Nombres premiers

Commençons par les nombres premiers, qui conservent encore beaucoup de secrets pour les chercheurs du monde entier et dont l'une des applications dans la vie quotidienne est la cryptographie.

Definition (Multiple)

Nous disons qu'un nombre entier relatif $a \in \mathbb{Z}$ est un **multiple** de $b \in \mathbb{Z}$ (ou que b est un **diviseur** de a) s'il existe $k \in \mathbb{Z}$ tel que

$$a = kb.$$

Exemple

1. 6 *est multiple de* 3 *car* $6 = 2 \times 3$, $k = 2$.
2. 0 *est multiple de tout entier* n, *car* $0 = 0 \times n$, *pour tout* $n \in \mathbb{N}$, *et* $k = 0$.
3. *Tout nombre entier est un multiple de* 1 *et de lui-même :* $n = 1 \times n$, *pour tout* $n \in \mathbb{N}$.

Nombres premiers

Definition (Nombre premier)

Nous disons qu'un nombre entier naturel $p \geq 2$ est un **nombre premier** lorsqu'il possède comme seuls diviseurs positifs 1 et lui-même.

Théorème (Entiers et nombres premiers)

Tout nombre entier $n \geq 2$ est le produit de nombres premiers.

Théorème (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Remarque (Pour ceux qui sont intéressés)

Il existe plusieurs façon de les trouver (avec plus ou moins d'efficacité) :

1. *le crible d'Eratosthène*
2. *le crible de Sundaram,*

et plusieurs tests permettant de voir si un nombre donné est premier ou non

1. *le test probabiliste de primalité,*
2. *le test de primalité de Fermat,*
3. *le test de primalité de Solovay-Strassen,*
4. *le test de primalité de Miller-Rabin,*
5. *Le test de primalité AKS (Agrawal-Kayal-Saxena ou test cyclotomique AKS)...*

Division Euclidienne

Théorème (Division euclidienne)

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ (b entier ≥ 1).Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$\begin{cases} a & = & bq + r, \\ 0 & \leq & r < b. \end{cases}$$

C'est ce que nous appelons la division euclidienne de a par b.

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array} \quad \text{ou} \quad \text{encore} \quad \begin{array}{r|l} \textbf{dividende} & \textbf{diviseur} \\ \hline \textbf{reste} & \textbf{quotient} \end{array}$$

Remarque

$r = 0$ est équivalent à dire que b divise a (ou que a est multiple de b).

PGCD-PPCM

Definition (pgcd)

Soient a, $b \in \mathbb{Z}$ deux entiers non tous les deux nuls.
Le plus grand entier qui divise à la fois a et b s'appelle **le plus grand commun diviseur** de a et b et se note **pgcd**(a, b).

Exemple

1. *Pour tous* k *et* $a \in \mathbb{Z}$, $pgcd(a, ka) = a$.
2. *Pour tout* $a \in \mathbb{Z}$, $pgcd(a, 0) = a$.
3. *Pour tout* $a \in \mathbb{Z}$, $pgcd(a, 1) = 1$.

Definition (ppcm)

Soient a, $b \in \mathbb{N}^*$.
Le plus petit entier multiple à la fois de a et de b s'appelle **le plus petit commun multiple** de a et b et se note **ppcm**(a, b)

PGCD-PPCM

Théorème (Existence et unicité du ppcm)

Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ deux entiers, alors il existe un unique $M \in \mathbb{N}^*$ tel que pour tous $m \in \mathbb{N}^*$,

$$m \text{ est multiple de } a \text{ et de } b \Leftrightarrow m \text{ est multiple de } M.$$

Ce nombre M =ppcm(a, b).

Théorème (Existence et unicité du pgcd)

Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ deux entiers, alors il existe un unique $D \in \mathbb{N}^*$ tel que pour tous $d \in \mathbb{N}^*$,

$$d \text{ est divise } a \text{ et } b \Leftrightarrow d \text{ divise } M.$$

Ce nombre D =pgcd(a, b).

Algorithme d'Euclide

Proposition (Égalité de pgcd)

Soient a, $b \in \mathbb{N}^*$. Soient $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$, alors

$$pgcd(a, b) = pgcd(b, r).$$

Ceci nous permet de trouver le pgcd entre deux nombres entiers strictement positifs, en utilisant l'algorithme d'Euclide.

Algorithme d'Euclide :

Nous souhaitons calculer le pgcd de a et $b \in \mathbb{N}^*$.

Nous supposons que $a \geq b$ (sinon nous faisons jouer le rôle de b à a et inversement).

Nous calculons les divisions euclidiennes successives.

Le pgcd sera le dernier reste non nul !

Algorithme d'Euclide

Voici comment nous procédons.

1. La division de a par b nous donne l'existence de q_1 et r_1 tels que $a = bq_1 + r_1$. Nous avons alors $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$.
   Nous avons alors deux sous cas.
   1. Si $r_1 = 0$ alors $\text{pgcd}(a, b) = b$.
   2. Sinon, on continue à l'étape suivante.
2. La division de b par r_1 nous donne l'existence de q_2 et r_2 tels que $b = r_1 q_2 + r_2$. Nous avons alors $\text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$.
   Nous avons alors deux sous cas.
   1. Si $r_2 = 0$ alors $\text{pgcd}(b, r_1) = r_1$.
   2. Sinon, on continue à l'étape suivante.
3. La division de r_1 par r_2 nous donne l'existence de q_2 et r_3 tels que $r_1 = r_2 q_3 + r_3$. Nous avons alors $\text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3)$.

   $\vdots$

   et nous continuons jusqu'à arriver au reste nul, c'est à dire
4. La division de r_{k-1} par r_k nous donne l'existence de q_{k+1} et $r_{k+1} = 0$ tels que $r_{k-1} = r_k q_{k+1} + 0$.

Algorithme d'Euclide

Nous avons alors

$$\text{pgcd}(a, b) = \text{pgcd}(r_{k-1}, r_k) = \text{pgcd}(rk, 0) = r_k.$$

Remarque

A chaque étape on sait que le reste est plus petit que le quotient, et donc que pour tout $i \geq 1$, nous avons $0 \leq r_{i+1} < r_i$. Nous sommes donc sûrs d'obtenir un reste nul un moment donné (fini, car $r_i \in \mathbb{N}^*$ est un nombre fini).

Algorithme d'Euclide

Exemple

$$183 = 117 \times 1 + 66$$
$$117 = 66 \times 1 + 51$$
$$66 = 51 \times 1 + 15$$
$$51 = 15 \times 3 + 6$$
$$15 = 6 \times 2 + 3$$
$$6 = 3 \times 2 + 0$$

Le dernier reste non nul est 3, donc :

$$\boxed{PGCD(183, 117) = 3}$$

Algorithme d'Euclide

Definition (Nombres premiers entre eux)

Deux nombres distincts a et $b \in \mathbb{N}^*$ sont premiers entre eux si et seulement si

$$\text{pgcd}(a, b)=1.$$

Remarque

Si deux entier ne sont pas premiers entre eux, nous pouvons nous y ramener en divisant par leur pgcd.

Identité et théorème de Bézout

Théorème (Identité de Bézout)

Soient a et $b \in \mathbb{N}$. Alors il existe u et $v \in \mathbb{Z}$ tels que

$$au + bv = pgcd(a, b).$$

Ces entiers relatifs u et v ne sont pas uniques. Ils sont appelés ***coefficients de Bézout***.

Remarque

Les coefficients de Bézout u et v s'obtiennent en remontant l'algorithme d'Euclide.
Il faut pour cela isoler le dernier reste non nul de l'algorithme. Puis remplacer à chaque fois la valeur du reste de l'étape précédente.

Identité et théorème de Bézout

Exemple

Si $a = 600$ *et* $b = 124$. *L'algorithme d'Euclide nous donne :*

$$\begin{aligned}
&i- \quad 600 = 124 \times 4 + 104,\\
&ii- \quad 124 = 104 \times 1 + 20,\\
&iii- \quad 104 = 20 \times 5 + 4,\\
&iv- \quad 20 = 4 \times 5 + 0.
\end{aligned}$$

Donc pgcd$(600, 124) = 4$.

Ensuite nous remontons cet algorithme : en partant de

iii- $4 = 104 - 20 \times 5$.

Puis nous remplaçons 20 *par sa valeur trouvée en l'isolant dans ii- :*

ii-$4 = 104 - (124 - 104 \times 1) \times 5$. *Ce qui nous donne :*

ii-$4 = 104 \times 6 + 124 \times (-5)$.

Nous remplaçons ensuite 104 *par sa valeur trouvée en l'isolant dans i- :*

i- $4 = (600 - 124 \times 4) \times 6 + 124 \times (-5)$. *Ce qui au final nous donne :*

$4 = (600 \times 6 + 124 \times (-29)$

et nous avons $u = 6$ *et* $v = -29$.

Identité et théorème de Bézout

Théorème (Théorème de Bézout)

Soient a et $b \in \mathbb{N}$. Ces entiers a et b sont premiers entre eux si et seulement s'il existe u et $v \in \mathbb{Z}$ tels que

$$au + bv = 1.$$

Théorème de Gauss et décomposition en facteurs premiers

Théorème (Théorème de Gauss)

Soient a, b et $c \in \mathbb{N}^*$. Si a divise bc et si a et c sont premiers entre eux, alors a divise b.

Une des applications de ce théorème est la résolution des équations diophantiennes.

Proposition (Équations diophantiennes)

Soient a, b, et $c \in \mathbb{Z}$. Considérons l'équation

$$ax + by = c,$$

1. *Cette équation possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si le $pgcd(a, b)$ divise c.*
2. *Si $pgcd(a, b)$ divise c, alors il existe une infinité de solutions entières qui sont de la forme $(x_0 + \alpha k, y_0 + \beta k)$ où x_0, y_0, α et $\beta \in \mathbb{Z}$ et k parcourt $\mathbb{Z}$.*

Théorème de Gauss et décomposition en facteurs premiers

Une application du théorème de Gauss est la proposition suivante :

Proposition (Nombres premiers et coefficients binomiaux)

Pour tout nombre premier p et pour tout $k \in \mathbb{N}$ tel que $1 \leq k \leq p-1$, alors p divise $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!}$

Théorème (Théorème fondamental de l'arithmétique)

Pour tout entier naturel $n \geq 2$, il existe un unique k-uplet $(p_1, p_2, ..., p_k)$de nombres premiers vérifiant

$$p_1 < p_2 < ... < p_k,$$

et un unique k-uplet $(\alpha_1, \alpha_2, ..., \alpha_k)$ d'entier naturels non nuls tels que

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}.$$

Théorème de Gauss et décomposition en facteurs premiers

Remarque

Une des principales raisons pour laquelle nous choisissons de dire que 1 *n'est pas un nombre premier est que sinon il n'y aurait pas unicité de cette décomposition.*

Exemple

Nous aurions par exemple

$24 = 2^3 \times 3 = 1 \times 2^3 \times 3 = 1^2 \times 2^3 \times 3 = 1^3 \times 2^3 \times 3 = ...$

Congruence

Definition (Congruence)

Soient a et $b \in \mathbb{Z}$, et $n \in \mathbb{N}^*$. Nous disons que a est **congru** à b modulo n si $a - b$ est un multiple de n. On écrira

$$a \equiv b\ [n] \text{ ou } a \equiv b(\text{n}).$$

Remarque

D'après la définition, nous avons donc

$$a \equiv b\ [n] \quad \Leftrightarrow \quad \textit{il existe } k \in \mathbb{Z} \textit{ tel que } a = b + kn.$$

Congruence

Proposition (Propriétés des congruences)

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors nous avons les propriétés suivantes :

1. $a \equiv a\ [n]$ *($\equiv$ est réflexive),*
2. *si* $a \equiv b\ [n]$ *alors* $b \equiv a\ [n]$ *($\equiv$ est symétrique),*
3. *si* $a \equiv b\ [n]$ *et* $b \equiv c\ [n]$ *alors* $a \equiv c\ [n]$ *($\equiv$ est transitive).*

Congruence

Nous avons une autre proposition sur la somme et le produit :

Proposition (Congruence, somme et produit)

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors nous avons les propriétés suivantes :

1. $a \equiv b\ [n]$ *alors* $a + c \equiv b + c\ [n]$,
2. *si* $a \equiv b\ [n]$ *alors* $ac \equiv bc\ [n]$.

Théorème (Congruence et puissance)

Soient $a, b, c \in \mathbb{Z}$ et n et $p \in \mathbb{N}^*$. Nous avons :

$$\text{si } a \equiv b\ [n] \text{ alors } a^p \equiv b^p\ [n]$$

Théorème (Numération en base b)

Soit b un entier, $b \geq 2$. Tout entier non nul x peut s'écrire de manière unique sous la forme

$$x = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0,$$

où n est un entier, a_0, a_1,..., a_n sont des entier appartenant à $[0, b-1]$ et $a_n \neq 0$.
Nous disons alors que $x = \overline{a_0 a_1 \ldots a_n}^b$ est l'écriture de x en base b.

Bases

Remarque

Quelques bases classiques :

1. *système binaire (base 2) :* $\{0, 1\}$,
2. *système quinaire (base 5) :* $\{0, 1, 2, 3, 4\}$,
3. *système octal (base 8) :* $\{0, 1, 2, 3, 4, 5, 6, 7\}$,
4. *système décimal (base 10) :* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$,

Bases

La numération usuelle est la numération décimale, en base 10. Plus généralement, on peut représenter tout nombre dans une base $b \geq 2$. Les chiffres autorisés sont :

$$0, 1, 2, \ldots, b-1.$$

Représentation en base b

Un nombre écrit

$$(a_k a_{k-1} \ldots a_1 a_0)_b$$

signifie :

$$a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

Exemple

$$(231)_5 = 2 \cdot 5^2 + 3 \cdot 5 + 1 = 66.$$

Bases : Conversion base b vers base 10

On développe selon les puissances de b.

Exemple

$$(10101)_2 = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 = 21.$$

Bases : Conversion base 10 vers base b

On utilise la méthode des divisions successives : divisions par b et récupération des restes, lus de bas en haut.

Exemple

$$35 = (100011)_2.$$

Bases : Fractions en base b

Un nombre

$$(a_k \dots a_0.a_{-1}a_{-2}\dots)_b$$

correspond à :

$$a_k b^k + \cdots + a_0 + a_{-1}b^{-1} + a_{-2}b^{-2} + \dots$$

Exemple

$$(10.11)_2 = 2.75.$$

Bases : Addition en base b

On additionne chiffre par chiffre, avec retenues dès que la somme dépasse b.

Exemple (en base 5.)

$$(243)_5 + (132)_5 = (430)_5.$$

Bases : Multiplication en base b

Même principe qu'en base 10, en tenant compte de b.

Exemple

$$(12)_3 \times (21)_3 = (1022)_3.$$

Exemple

1. $x = \overline{101100110101}^{2} = \overline{5465}^{8} = \overline{2765}^{10}$,
2. $x = \overline{173}^{10} = \overline{10101101}^{2} = \overline{255}^{8}$.

Pour avoir la conversion en base 8, on constate que chaque chiffre en base 8 peut 'écrire à l'aide de 3 bits. Ainsi on regroupe 101100110101 par paquet de 3 comme il y a 12 bits : 101 100 110 101. Chaque regroupement se traduit en base 8 :

$101_2 = 5_8$; $100_2 = 4_8$; $110_2 = 6_8$; $101_2 = 5_8$

Ainsi

$$101100110101 = 5465_8$$

Théorème (Congruence et nombre premier)

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$,

$$a^p \equiv a[p].$$

Théorème (Petit théorème de Fermat)

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, a n'étant pas un multiple de p, nous avons

$$a^{p-1} \equiv 1[p].$$

Exemple

On veut calculer 2^{1000} modulo 7 ?
Pour cela on remarque que 7 est un nombre premier. Le fait que 2 n'étant pas un multiple de 7 (c'est-à-dire 2 n'est pas divisible par 7) alors par le petit théorème de Fermat on a $2^6 \equiv 1[7]$. Comme $1000 = 6 \times 166 + 4$, on a $2^{1000} = 2^{6\times 166} \times 2^4 = (2^6)^{166} \times 16 \equiv 1^{166} \times 2 \equiv 2[7]$

Théorème (Théorème des restes chinois)

Soient m_1, m_2,...,m_r des entiers positifs deux à deux premiers entre eux. Alors le système

$$\begin{cases} x & \equiv & a_1 & [m_1], \\ x & \equiv & a_2 & [m_2], \\ \vdots & & & \\ x & \equiv & a_r & [m_r]. \end{cases}$$

possède une unique solution x modulo $M = m_1 \times m_2 \times ... \times m_r$, et

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r \ [M],$$

avec $M_i = \dfrac{M}{m_i}$ et $y_i M_i \equiv 1 \ [m_i]$, pour $i = 1, ..., r$.

Exemple (application du théorème du reste chinois)

Résoudre le système :

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5. \end{cases}$$

On pose : $M = 3 \times 5 = 15, \qquad M_1 = 5, \quad M_2 = 3.$

On cherche les inverses :

$$5e_1 \equiv 1 \pmod 3 \Rightarrow 2e_1 \equiv 1 \Rightarrow e_1 = 2,$$

$$3e_2 \equiv 1 \pmod 5 \Rightarrow 3e_2 \equiv 1 \Rightarrow e_2 = 2.$$

Alors une solution est : $x \equiv a_1 M_1 e_1 + a_2 M_2 e_2 = 2 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2 = 38.$

On réduit modulo 15 *:* $x \equiv 38 \equiv 8 \pmod{15}$.

$$\boxed{x \equiv 8 \pmod{15}}.$$

Exemple (application du théorème du reste chinois)

Résoudre le système :

$$\begin{cases} x \equiv 1 \pmod 2, \\ x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5. \end{cases}$$

On calcule : $M = 2 \times 3 \times 5 = 30, \qquad M_1 = 15,\ M_2 = 10,\ M_3 = 6.$

Inverses :

$$15e_1 \equiv 1 \pmod 2 \ \Rightarrow\ e_1 = 1,$$

$$10e_2 \equiv 1 \pmod 3 \ \Rightarrow\ e_2 = 1,$$

$$6e_3 \equiv 1 \pmod 5 \ \Rightarrow\ e_3 = 1.$$

Solution : $x \equiv 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 53.$

Réduction modulo 30 *:* $x \equiv 53 \equiv 23 \pmod{30}$.

$$\boxed{x \equiv 23 \pmod{30}}.$$

Remarque

Pour l'histoire, ce théorème porte le nom de théorème des restes chinois pour la raison suivante. Sa première apparait sous forme de problème dans le livre "Sunzi suanjing " de Sun Zi (mathématicien chinois du 3ème sièclee), le Sunzi suanjing. Le mathématicien chinois Qin Jiushao en fait mention dans son dans son "Traité mathématique en neuf chapitres" (le Shushu Jiuzhang) publié en 1247. On l'associe souvent au problème soulevé par le général Han Xin qui souhaitait compter son armée : "combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?".

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Définition de polynômes à coefficients réels ou complexes

Dans ce cours nous ne chercherons pas à distinguer la notion de polynômes et de fonction polynômiale pour plus de simplicité.

Definition (Polynôme)

Soient $(a_k)_{0\leq k\leq d}$, $d+1$ complexes ou réels. Nous appelons **polynôme** associé à la fonction polynômiale f définie sur $\mathbb{C}$ ou $\mathbb{R}$ par

$$\begin{aligned} f(x) &= \sum_{k=0}^{d} a_k x^k &&= a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d, \\ &&&= a_d x^d + \ldots + a_2 x^2 + a_1 x + a_0. \end{aligned}$$

l'"objet" noté P défini par

$$P = \sum_{k=0}^{d} a_k X^k = a_d X^d + \ldots + a_2 X^2 + a_1 X + a_0,$$

d'indéterminé X.

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Definition (Monôme)

Nous appelons **monôme** tout polynôme de la forme $a_n X^n$, où $n \in \mathbb{N}$, et $a_n \in \mathbb{R}$ ou $\mathbb{C}$.

Definition ($\mathbb{R}[X]$ et $\mathbb{C}[X]$)

Nous notons $\mathbb{C}[X]$ (respectivement $\mathbb{R}[X]$) l'ensemble des polynômes à coefficients complexes (respectivement réels).

Remarque

1. *Pour P non nul, l'unique entier $d \geq 0$ intervenant dans l'écriture de P en fonction de l'indéterminé X est appelé le degré de P.*
2. *Nous noterons le $d^\circ P$ le degré de P.*

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Definition (Coefficient dominant)

Pour P non nul de $\mathbb{C}[X]$ (ou $\mathbb{R}[x]$), le coefficient dominant de P est le coefficient a_d du terme de plus haut degré dans l'écriture de P en fonction de l'indéterminé X.

Definition (Polynôme unitaire)

Un polynôme est dit unitaire (ou normalisé) lorsque son coefficient dominant est égal à 1.

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Nous pouvons énoncer quelques propriétés relatives aux polynômes.

Proposition (Degré de somme)

Soient P et Q deux polynômes de $\mathbb{C}[X]$ (ou $\mathbb{R}[X]$) alors

$$d^\circ(P+Q) \leq \max(d^\circ P, d^\circ Q).$$

Proposition (Degré de produit)

Soient P et Q deux polynômes de $\mathbb{C}[X]$ (ou $\mathbb{R}[X]$) alors

$$d^\circ(PQ) = d^\circ P + d^\circ Q.$$

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Definition (Polynôme dérivé)

Pour un polynôme de $\mathbb{C}[X]$ (ou $\mathbb{R}[X]$), nous posons

$$P = a_d X^d + ... + a_2 X^2 + a_1 X + a_0.$$

Nous appelons polynôme dérivé de P, le polynôme P' défini par

$$P' = d a_d X^{d-1} + ... + 2 a_2 X^2 + a_1.$$

Notation (Dérivée n-ième)

Le polynôme dérivé de P' est noté P'', et la dérivée n-ième de P est notée $P^{(n)}$.

Proposition (Dérivée de produit et somme)

Soient P et Q deux polynômes de $\mathbb{C}[X]$ (ou $\mathbb{R}[X]$) alors

$$\begin{aligned}(P+Q)' &= P'+Q',\\ (PQ)' &= P'Q+PQ'.\end{aligned}$$

Remarque

Cette formule a évidemment une certaine importance mais pour des exemples concrets elle est assez inutile. En effet,
-si $R = X(X^2+1)$, il est assez maladroit de l'appliquer.
En faisant le calcul nous avons
$R' = 1(X^2+1) + X.2X = X^2+1+2X^2 = 3X^2+1.$
-Alors qu'en développant nous avons :

$$R = X(X^2+1) = X^3+X \text{ et donc } R' = 3X^2+1.$$

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Definition ($P(x)$)

Soient $x \in \mathbb{C}$ (ou $\mathbb{R}$) et $P \in \mathbb{C}[X]$ (ou $\mathbb{R}[x]$) avec

$$P = a_d X^d + ... + a_2 X^2 + a_1 X + a_0.$$

alors

$$P(x) = a_d x^d + ... + a_2 x^2 + a_1 x + a_0.$$

Proposition ($P(x) + Q(x)$)

Soient $x \in \mathbb{C}$ (ou $\mathbb{R}$) et $P \in \mathbb{C}[X]$ (ou $\mathbb{R}[x]$)

$$\begin{aligned} (P+Q)(x) &= P(x) + Q(x), \\ (PQ)(x) &= P(x)Q(x). \end{aligned}$$

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Definition (Composée de polynômes)

Soient P et Q deux polynômes de $\mathbb{C}[X]$ (ou $\mathbb{R}[x]$) avec

$$P = a_d X^d + ... + a_2 X^2 + a_1 X + a_0.$$

Nous appelons composée de P et Q, le polynôme

$$P \circ Q = P(Q) = a_d Q^d + ... + a_2 Q^2 + a_1 Q + a_0.$$

Applications

Proposition (Polynôme nul)

Un polynôme P de $\mathbb{C}[X]$ (ou $\mathbb{R}[x]$) avec

$$P = a_d X^d + ... + a_2 X^2 + a_1 X + a_0.$$

est nul si et seulement si pour tout $i = 0, ..., d$, $a_i = 0$.

Proposition (Égalité de polynômes)

Soient P et Q deux polynômes de $\mathbb{C}[X]$ (ou $\mathbb{R}[x]$) avec $P = a_d X^d + ... + a_2 X^2 + a_1 X + a_0$. et $Q = b_d X^d + ... + b_2 X^2 + b_1 X + b_0$. Alors,

$$P = Q \Leftrightarrow \begin{cases} p & = & q, \\ et & & \\ a_i & = & b_i \quad pour\ tout\ i = \{0, ..., q\}. \end{cases}$$

Division Euclidienne

Il s'agit ici d'utiliser pour les polynômes des résultats analogues à ceux énoncés pour les entiers.

1. L'arithmétique des polynômes est analogue à celle des entiers (à condition de travailler sur les polynômes sur un corps commutatif (ce qui est le cas quand on travaille sur $\mathbb{R}$ ou $\mathbb{C}$).

Posons $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ à partir de maintenant.

Division Euclidienne

Definition (Multiple d'un polynôme)

On dit qu'un polynôme P_m de $\mathbb{K}[X]$ est un multiple d'un polynôme $P_d \in \mathbb{K}[X]$ ou que P_d est un diviseur de P_m lorsqu'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P_m = Q \times P_d$.

Théorème (Division euclidienne)

Soient $A \in \mathbb{K}[X]$ et B un polynôme non nul de $\mathbb{K}[X]$, alors il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ qui vérifie

$$\begin{cases} A & = & BQ + R, \\ d^\circ R & < & d^\circ B. \end{cases}$$

Division euclidienne

Exemple

Divisons le polynôme $A = 6x^3 - 2x^2 + x + 3$ *par* $B = x^2 - x + 1$.

$$
\begin{array}{rr|l}
 & 6x^3 - 2x^2 + x + 3 & x^2 - x + 1 \\
- & 6x^3 - 6x^2 + 6x & \hline 6x + 4 \\
\hline
 & 4x^2 - 5x + 3 & \\
- & 4x^2 - 4x + 4 & \\
\hline
 & -x - 1 &
\end{array}
$$

Nous avons alors $6x^3 - 2x^2 + x + 3 = (x^2 - x + 1)(6x + 4) + (-x - 1)$.

Pgcd, ppcm

Proposition (Pgcd)

Soient A et B deux polynômes de $\mathbb{K}[X]$ avec $A \neq 0$ et $B \neq 0$ alors il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B. Ce polynôme est appelé le plus grand commun diviseur de A et B et on le note $pgcd(A, B)$.

Remarque

1. *$pgcd(A, B)$ est un polynôme unitaire.*
2. *Si A divise B alors $pgcd(A, B) = \frac{1}{a_d} A$ si a_d est le coefficient dominant de A.*
3. *Pour tout $\lambda \in \mathbb{K}^*$, $pgcd(\lambda A, B) = pgcd(A, B)$.*
4. *Si $A = BQ + R$ alors $pgcd(A, B) = pgcd(B, R)$, ce qui nous permet d'utiliser l'algorithme d'Euclide appliqué aux polynômes.*

Pgcd

L'algorithme d'Euclide pour les polynômes s'écrit :

$$\begin{array}{lll} A & = BQ_1 + R_1, & d^\circ R_1 < d^\circ B, \\ B & = R_1 Q_2 + R_2, & d^\circ R_2 < d^\circ R_1, \\ R_1 & = R_2 Q_3 + R_3, & d^\circ R_3 < d^\circ R_2, \\ \vdots & & \\ R_{k-2} & = R_{k-1} Q_k + R_k, & d^\circ R_k < d^\circ R_{k-1}, \\ R_{k-1} & = R_k Q_{k+1} + 0, & \end{array}$$

Le degré du reste diminue à chaque division, et on arrête l'algorithme lorsque le reste est nul, et le pgcd est le dernier reste non nul $\mathbb{R}_k$ ici (rendu unitaire).

Definition (Polynômes premiers entre eux)

Soient A et B deux polynômes de $\mathbb{K}[X]$, on dit que A et B sont premiers entre eux si $\text{pgcd}(A, B) = 1$.

Pgcd

Remarque

Pour A et B quelconques (non nécessairement premiers entre eux), on a $pgcd(A, B) = D$.
On pose $A = A'D$ et $B = B'D$ et $pgcd(A', B') = 1$ et on a A' et B' sont premiers entre eux.

Théorème (Théorème de Bézout)

Soient A et B deux polynômes de $\mathbb{K}[X]$, avec A et B non nuls. On note $D = pgcd(A, B)$, alors il existe deux polynômes U et V de $\mathbb{K}[X]$ tels que

$$AU + BV = D.$$

Pgcd

Corollary (Théorème de Bézout)

Soient A et B deux polynômes de $\mathbb{K}[X]$, avec A et B non nuls. A et B sont premiers entre eux si et seulement s'il existe U et V polynômes tels que

$$AU + BV = 1.$$

Corollary (Diviseur du pgcd)

Soient A, B et C trois polynômes de $\mathbb{K}[X]$, avec A et B non nuls. Si C divise A et C divise B alors C divise le pgcd(A, B).

Pgcd

Théorème (Théorème de Gauss)

Soient A, B et C trois polynômes de $\mathbb{K}[X]$, si A divise BC et $pgcd(A, B) = 1$, alors A divise C.

Ppcm

Proposition (Ppcm)

Soient A et B deux polynômes de $\mathbb{K}[X]$, avec A et B non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que A divise M et B divise M.
Ce polynôme est le plus petit commun multiple de A et B et il est noté $ppcm(A, B)$.

Proposition (Ppcm)

Soient A et B deux polynômes de $\mathbb{K}[X]$, avec A et B non nuls, et $M = ppcm(A, B)$.
Si $C \in \mathbb{K}[X]$ est un polynôme tel que A divise C et B divise C alors M divise C.

Polynômes irréductibles

Les polynômes irréductibles sont les analogues des nombres premiers. Toutefois, les usages étant ceux qu'ils sont il y a une petite nuance de vocabulaire. Alors que le mot "nombre premier" est réservé à des entiers positifs, le mot "polynôme irréductible" n'est pas réservé à des polynômes unitaires : il faut donc bien distinguer ces deux notions.

Definition (Polynôme irréductible)

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On dira qu'un polynôme $P \in \mathbb{K}$ est irréductible lorsqu'il possède deux diviseurs unitaires et ces deux diviseurs unitaires sont le polynôme 1 et le polynôme P divisé par le coefficient dominant de P.

Polynômes irréductibles

Proposition (Polynômes du premier degré irréductibles)

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Dans $\mathbb{K}[X]$, les polynômes du premier degré sont irréductibles.

Proposition (Décomposition en polynômes irréductibles)

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Tout polynôme P non nul peut s'écrire de façon unique (à l'ordre près des facteurs) en produit

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} ... P_k^{\alpha_k},$$

où λ est le coefficient dominant de P.

Racines des polynômes

Definition (Racine ou zéro d'un polynôme)

Soient P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine (ou un zéro) de P lorsque $P(a) = 0$.

Proposition (Racine et diviseur)

Soient P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$, a est une racine de P si et seulement si $x - a$ divise P.

Racines des polynômes

Proposition (racines d'un polynôme de degré n)

Un polynôme de $\mathbb{K}[X]$ non nul de degré n possède au plus n racines.

Definition (Racines multiples)

Soient P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que

1. a est une racine de multiplicité d'ordre au moins k de P lorsque $(x-a)^k$ divise P,
2. a est exactement racine d'ordre de multiplicité k lorsqu'il est de multiplicité d'ordre k sans être de multiplicité d'ordre $k+1$. On dit que k est l'ordre de multiplicité de la racine.

Racines des polynômes

Proposition (Racines double et dérivée)

Soient P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$. L'élément a est une racine au moins double de P si et seulement si a est une racine de P et P'.

Racines des polynômes

Quelle est la différence entre $\mathbb{C}[X]$ et $\mathbb{R}[X]$ en ce qui concerne les racines et les polynômes irréductibles ? Les trois théorèmes suivants permettent de donner un aperçu de quelques différences.

Théorème (Théorème de D'Alembert-Gauss)

Tout polynôme non constant de $\mathbb{C}[X]$ possède au-moins une racine complexe.
Il admet exactement n racines si on compte chaque racine avec sa multiplicité.

Racines des polynômes

Definition (Polynôme scindé)

On dit qu'un polynôme est scindé lorsqu'il peut s'écrire sous forme de produit de facteurs du premier degré.

Nous allons donner le résultat suivant qui énonce que tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 est scindé.

Théorème (Polynômes irréductibles de $\mathbb{C}[X]$)

Les polynômes irréductibles de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}^*$ sont les polynômes de degré 1.
Autrement dit, pour $P \in \mathbb{C}[X]$ de degré $n \in \mathbb{N}^*$ la factorisation de P s'écrit

$$P = \lambda(X - a_1)^{\alpha_1}(X - a_2)^{\alpha_2}...(X - a_k)^{\alpha_k}.$$

où a_1, a_2,...a_k sont les racines de P et α_1, α_2,...,α_k leur multiplicité respective.

Théorème (Polynômes irréductibles de $\mathbb{R}[X]$)

Les polynômes irréductibles de $\mathbb{R}[X]$ de degré $n \in \mathbb{N}^*$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant strictement négatif.
Autrement dit, pour $P \in \mathbb{R}[X]$ de degré $n \in \mathbb{N}^*$ la factorisation de P s'écrit

$$P = \lambda(X - a_1)^{\alpha_1}(X - a_2)^{\alpha_2}...(X - a_k)^{\alpha_k} Q_1^{\beta_1}...Q_s^{\beta_s}.$$

où a_1, a_2,...a_k sont les racines réelles distinctes de α_1, α_2,...,α_k leur multiplicité respective et les Q_i, $i = 1, ..., s$ sont les polynômes irréductibles de degré 2 de la forme

$$Q_i = X^2 + b_i X + c_i \text{ où } \Delta = b_i^2 - 4c_i.$$

Racines des polynômes

Proposition (Racines complexe de $\mathbb{R}[X]$)

Soient P un polynôme de $\mathbb{R}[X]$ et $a \in \mathbb{C}$ une racine de P alors son conjugué $\bar{a}$ est également une racine de P.

Formule de Taylor

Théorème (Formule de Taylor)

Soient P un polynôme de $\mathbb{C}[X]$ de degré n et $a \in \mathbb{C}$, alors

$$P = P(a) + P'(a)(X-a) + \frac{P''(a)}{2!}(X-a)^2 + \ldots + \frac{P^{(n)}}{n!}(X-a)^n.$$

Remarque

La formule reste valable pour les polynômes de $\mathbb{R}[X]$.

Formule de Taylor

Faisons un bref retour sur les racines multiples d'un polynômes avec la proposition suivante dont la preuve peut se faire en se servant de la formule de Taylor.

Proposition (Racines multiples et dérivée)

Soient P un polynôme de $\mathbb{K}[X]$ (de degré n) et $a \in \mathbb{K}$. L'élément a est une racine exactement d'ordre $k \leq n$ de P si et seulement si a est une racine de P, P', ... et $P^{(k-1)}$ mais pas de $P^{(k)}$.