Chapitre 1

Calculs algébriques

Sommaire

1 Les nombres rationnels

$\mathbb{Z}$ désigne l'ensembles des entiers relatifs. Une *écriture* d'un nombre rationnel est une fraction de la forme

$$\frac{a}{b}$$

avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} - \{0\}$. Exemples : $\frac{2}{3}$, $\frac{3}{4}$, $\frac{-1}{2}$, $\frac{3}{-3}$, $\frac{4}{1}$, $\frac{-12}{21}\dots$ La difficulté est que deux écritures différentes peuvent représenter le même nombre rationnel. Ainsi on décrète que

$$\frac{a}{b} = \frac{c}{d} \;\Leftrightarrow\; ad = bc \in \mathbb{Z}. \tag{1.1}$$

On vient de définir l'ensemble $\mathbb{Q}$ des nombres rationnels. Enfin, pour $a \in \mathbb{Z}$, on pose $a = \frac{a}{1}$ et on obtient $\mathbb{Z} \subset \mathbb{Q}$.

Soit $q = \frac{a}{b}$ un nombre rationnel avec $b > 0$. Pour situer q sur l'axe des abscisses, on procède ainsi

(i) On découpe le segment en $[0; 1]$ en b parts égales. On obtient ainsi $\frac{1}{b}$.

(ii) On reparte a fois cette quantité. (Avec la convention usuelle si a est négatif).

Enfin on a plusieurs opérations sur $\mathbb{Q}$. Un produit

$$\frac{a}{b}.\frac{c}{d} := \frac{ac}{bd},$$

une addition

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + cb}{bd},$$

un ordre

$$\frac{a}{b} \leqslant \frac{c}{d} \;\Leftrightarrow\; ad \leqslant cb,$$

où b et d sont positifs.

2 Nombres réels

2.1 Définition

Pour les grecs de l'antiquité, (VI$^{\text{eme}}$ siècle av. J.C.), les seuls nombres étaient les nombres rationnels. Bien qu'ils aient su que $\sqrt{2}$ n'était pas rationnel, et que cette grandeur est la longueur de la diagonale d'un carré de côté 1, cette grandeur était qualifiée d'incommensurable, montrant bien leur embarras. Il a fallu attendre la fin du XIX^{e} siècle pour que des mathématiciens comme Peano, Dedekind et Cantor notamment aboutissent par une démarche rigoureuse à la première construction du corps des nombres réels. Dans ce cours nous donnons une définition précise de $\mathbb{R}$, mais admettrons l'existence des opérations et leurs propriétés.

Définition I.1: Nombres réels

Un *nombre réel* est une écriture décimale composée de

(i) Une signe $\pm$;

(ii) Une suite finie de chiffres dans $\{0, \cdots, 9\}$ ne commençant pas par 0 ou étant réduite à 0 ;

(iii) Une virgule ;

(iv) Une suite infinies de chiffres (éléments de $\{0, \cdots, 9\}$) après la virgule ne finissant pas par une infinité de 9 successifs.

Le nombre $-0,0\dots0\dots$ n'existe pas ou est égal à $+0,0\dots0\dots$. L'ensemble des nombres réels est noté $\mathbb{R}$.

Remarques. (i) Les éléments de $\mathbb{R}$ se présentent donc ainsi

$$\pm a_p \dots a_0, b_1 \dots b_n \dots$$

avec les $(a_i)_{0 \leqslant i \leqslant p}$ et $(b_j)_{j \in \mathbb{N}}$ éléments de $\{0, \cdots, 9\}$.

(ii) Cette définition n'empêche pas les écritures simplifiées usuelles : $2 = +2,000\dots$ par exemple.

(iii) $0,9\dots9\dots$ est interdit pour la raison suivante. Soit $x < y$ deux nombres réels. On veut que

$$x < \frac{x+y}{2} < y.$$

Avec $x = 0,9\dots9\dots$ et $y = 1$, on a un problème ! E effet, il n'existe pas de z tel que $x < z < y$. On résout ce problème en interdisant $0,9\dots9\dots$. D'autres auteurs autorisent cette écriture mais imposent $0,9\dots9\cdots = 1$.

(iv) Comme tout nombre rationnel a une écriture décimale, l'ensemble $\mathbb{Q}$ des nombres rationnels peut être vu comme une partie de $\mathbb{R}$: $\mathbb{Q} \subset \mathbb{R}$.

On note $\mathbb{R}_+$ l'ensemble des nombres réels avec un signe + et on pose $\mathbb{R}_+^* = \mathbb{R}_+ - \{0\}$ et $\mathbb{R}^* = \mathbb{R} - \{0\}$.

2.2 Interprétation

Un nombre réel peut être pensé comme une suite de nombres rationnels (et même décimaux) qui converge vers, justement, le nombre réel. En effet, soit x un nombre réel. On note x_n le nombre décimal obtenu en ne gardant que les n premiers chiffres après la virgule. Alors x_n est une approximation de x d'autant plus précise que n est grand.

2.3 Opérations

On admettra le résultat suivant pas si facile qu'il n'y parait.

Théorème I.2

Il existe deux lois + et $\times$ et une relation d'ordre $\leqslant$ sur $\mathbb{R}$ telles que :

(i) $+, \times$ et $\leqslant$ prolongent les lois et relations usuelles sur $\mathbb{Q}$.

(ii) $\forall x, y \in \mathbb{R} \quad x + y = y + x$

(iii) $\forall x, y, z \in \mathbb{R} \quad (x + y) + z = x + (y + z)$

(iv) $\forall x \in \mathbb{R} \quad x + 0 = x$

(v) $\forall x \in \mathbb{R} \quad \exists! y \in \mathbb{R} \quad x + y = 0$; on pose $-x := y$

(vi) $\forall x, y \in \mathbb{R} \quad x.y = y.x$

(vii) $\forall x, y, z \in \mathbb{R} \quad (x.y).z = x.(y.z)$

(viii) $\forall x \in \mathbb{R} \quad x.1 = x$

(ix) $\forall x \in \mathbb{R} - \{0\} \quad \exists! y \in \mathbb{R} \quad x.y = 1$; on pose $x^{-1} := y$

(x) $\forall x, y, z \in \mathbb{R} \quad z.(x + y) = z.x + z.y$

(xi) $\forall x, y, z \in \mathbb{R} \quad (x \leqslant y \text{ et } y \leqslant z) \implies x \leqslant z$

(xii) $\forall x, y \in \mathbb{R} \quad x \leqslant y$ ou $y \leqslant x$

(xiii) $\forall x, y, z \in \mathbb{R} \quad x \leqslant y \implies z + x \leqslant z + y$

(xiv) $\forall x \in \mathbb{R}$ et $a \in \mathbb{R}_+ \quad x \leqslant y \implies a.x \leqslant a.y$

(xv) $\forall x \in \mathbb{R}$ et $y \in \mathbb{R}_+^* \quad \exists N \in \mathbb{N} \quad x \leqslant N.y$

Remarque. Par convention . est prioritaire sur +. Cette convention usuelle permet par exemple d'écrire $z.x + z.y$ plutôt que $(z.x) + (z.y)$. On utilisera les conventions usuelles $x/y = x.y^{-1}$, $x - y = x + (-y)\dots$

2.4 Propriété de la borne supérieure

Soit $A \subset \mathbb{R}$ une partie de $\mathbb{R}$. Une nombre réel a est appelé *majorant de* A si

$$\forall x \in A \qquad x \leqslant a.$$

Un majorant est donc un nombre (non nécessairement dans A plus grand que tous les éléments de A. La partie A est dite *majorée* s'il existe un majorant.
Encore un résultat admis :

Théorème I.3. Existence borne supérieure

Toute partie A non vide et majorée de $\mathbb{R}$ possède une borne supérieure, c'est-à-dire un plus petit majorant.

Ce théorème n'est pas vrai pour $\mathbb{Q}$: l'ensemble $A = \{x \in \mathbb{Q} : x^2 \leqslant 2\}$ n'a pas de borne supérieure dans $\mathbb{Q}$.
On note $\sup(A)$ la borne supérieure de A. Si A n'est pas majoré, on pose $\sup(A) = +\infty$. Par ailleurs, $\sup(\emptyset) = -\infty$.
Une caractérisation bien utile de la borne supérieure.

Théorème I.4: Caractérisation du sup

Soit A une partie non vide et majorée de $\mathbb{R}$. Alors $M = \sup(A)$ si et seulement si

(i) M est un majorant de A :

$$\forall x \in A \qquad x \leqslant M$$

(ii) Et, pour tout $\varepsilon > 0$, l'intersection $A \cap]M - \varepsilon; M]$ est non vide.

Remarque. La condition (ii) peut être remplacée par l'existence d'une suite $(U_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers M.

Preuve

Soit M vérifiant les assertions (i) et (ii). Le réel M est un majorant. Il s'agit de montrer que c'est le plus petit. Prenons donc un autre majorant m et montrons que $M \leqslant m$. Par l'absurde supposons que $M > m$ et posons $\varepsilon = M - n$. Par hypothèse, il existe $a \in A \cap]M - \varepsilon; M]$. Mais alors $a > M - \varepsilon = m$. Ce qui contredit le fait que m soit un majorant.

Réciproquement, il est clair que $M = \sup(A)$ vérifie la première assertion. Montrons la seconde. Soit $\varepsilon > 0$. Alors $M - \varepsilon < M$ n'est pas un majorant de A. Donc il existe $a \in A$ tel que $M - \varepsilon < a$. Comme $a \leqslant M$, on a $a \in]M - \varepsilon; M]$. En particulier, l'intersection $A \cap]M - \varepsilon; M]$ est non vide.

Exemple 1. Soit $A = \{-\frac{1}{n} : n \in \mathbb{N}^*\}$. Alors $\sup(A) = 0$. Soit $B = \{x \in \mathbb{Q} : x^2 \leqslant 2\}$. Alors $\sup(B) = \sqrt{2}$.

3 Inégalités

Nous avons déjà rencontré la relation d'ordre $\leqslant$ sur $\mathbb{R}$; on a aussi $\geqslant$, $<$ et $>$.
Voici une liste de propriétés utiles.

Propriété I.5. *Soit a, b, c, d des nombres réels.*

(i) si $a \leqslant b$ alors $a + c \leqslant b + c$;

(ii) *si* $a \leqslant b$ *et* $c \leqslant d$ *alors* $a + c \leqslant b + d$ *; (les 3 inégalités sont dans le même sens !)*

(iii) *si* $a \leqslant b$ *et* $c > 0$ *alors* $ac \leqslant bc$ *;*

(iv) *si* $a \leqslant b$ *et* $c < 0$ *alors* $ac \geqslant bc$ *;*

(v) *si* $a \leqslant b$ *et* a *et* b **ont le même signe** *alors* $\frac{1}{a} \geqslant \frac{1}{b}$.

Remarques. (i) Il y a des propriétés analogues pour $\geqslant$ et $<$. Pour ne pas encombrer vos mémoires, vous pouvez les retrouver facilement.

(ii) Attention à ne pas utiliser d'autres opérations de votre invention. Par exemple, les implications suivantes sont **fausses**

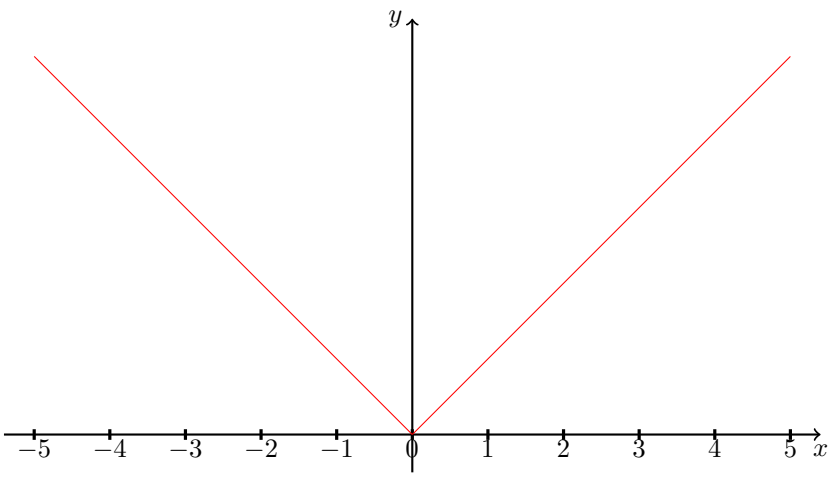
$$a \leqslant b \implies \frac{1}{a} \geqslant \frac{1}{b}$$
$$a \leqslant b \text{ et } c \leqslant d \implies a - c \leqslant c - d$$

4 Valeur absolue

On définit la fonction

$$\begin{array}{rccl} |\cdot| : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \begin{cases} x & \text{si} \quad x \geqslant 0 \\ -x & \text{si} \quad x < 0 \end{cases} \end{array}$$

Son graphe est



Propriété I.6. *Soit* a *et* b *deux nombres réels. Alors*

(i) $|ab| = |a|\,|b|$ *(en particulier* $|-a| = |a|$*) ;*

(ii) $|a + b| \leqslant |a| + |b|$ *avec égalité si et seulment si* a *et* b *ont le même signe.*

(iii) $||a| - |b|| \leqslant |a - b|$.

5 La notation Σ

Soient $m \leqslant n$ deux entiers naturels. On suppose donnés des nombres réels $a_m, a_{m+1}, \ldots, a_n$. On note alors

$$\sum_{k=m}^{n} a_k$$

leur somme. On écrit aussi quelquefois

$$\sum_{m \leqslant k \leqslant n} a_k.$$

Remarques. (i) Il faut prendre conscience que $\sum_{k=m}^{n} a_k$ dépend de m, n et des réels a_k. En revanche, cette somme ne dépend pas de k qui est une variable muette :

$$\sum_{k=m}^{n} a_k = \sum_{i=m}^{n} a_i.$$

(ii) Une autre conséquence du fait que k est une variable muette et que

$$\sum_{k=1}^{n} k$$

a un sens (et vaut $\frac{n(n+1)}{2}$) alors que

$$\sum_{k=1}^{k} k$$

n'a aucun sens.

(iii) Le problème des piquets et des intervalles. Dans la somme $\sum_{k=m}^{n} a_k$ il y a $n-m+1$ termes. Ainsi, par exemple,

$$\sum_{k=0}^{n} 7 = 7(n+1).$$

(iv) Un autre exemple où a_k est indépendant de k :

$$\sum_{k=1}^{n} n = n^2.$$

Changement d'indice. Comme dans les intégrales, on peut faire des changements d'indices. Voici un exemple :

$$\sum_{k=0}^{n} a_k = \sum_{l=1}^{n+1} a_{l-1}$$

obtenu en faisant

$$\left\{ \begin{array}{l} l = k+1 \\ k = l-1 \end{array} \right. \qquad \left\{ \begin{array}{ll} k = 0 & l = 1 \\ k = n & l = n+1 \end{array} \right.$$

Ce qui est important ici est que $k \mapsto l$ est une bijection de $\{0, \ldots, n\}$ sur $\{1, \ldots, n+1\}$.

Règles de calcul. On a

$$\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} (a_k + b_k).$$

Ici, il est important de veiller à ce que **les indices des deux sommes portent sur les mêmes ensembles**.
La distributivité donne

$$\lambda \sum_{k=0}^{n} a_k = \sum_{k=0}^{n} (\lambda a_k).$$

Sommes doubles. La donnée nécessaire pour utiliser un $\sum$ est une série de nombres réels a_k. Imaginons à présent que nous ayons une grille de nombres réels

$$a_{ij} \text{ pour } p \leqslant i \leqslant q \text{ et } r \leqslant j \leqslant s.$$

La somme de ces $(q-p+1)(s-r+1)$ nombres réels est notée

$$\sum_{\substack{p \leqslant i \leqslant q \\ r \leqslant j \leqslant s}} a_{ij}.$$

En faisant, cette addition en ligne ou en colonne, on obtient

$$\sum_{\substack{p \leqslant i \leqslant q \\ r \leqslant j \leqslant s}} a_{ij} = \sum_{p \leqslant i \leqslant q} \left(\sum_{r \leqslant j \leqslant s} a_{ij} \right) = \sum_{r \leqslant j \leqslant s} \left(\sum_{p \leqslant i \leqslant q} a_{ij} \right).$$

Un exemple de somme double vient de la distributivité :

$$\left(\sum_{k=0}^{p} a_k\right)\left(\sum_{k=0}^{q} b_k\right) = \sum_{\substack{0 \leqslant i \leqslant p \\ 0 \leqslant j \leqslant q}} a_i b_j.$$

Pour $p = 2$ et $q = 1$, on obtient

	a_0	a_1	a_2
b_0	a_0b_0	a_1b_0	a_2b_0
b_1	a_0b_1	a_1b_1	a_2b_1

et avec des valeurs numériques :

	1	3	-2
5	5	15	-10
4	4	12	-8

on obtient

$$(1 + 3 - 2)(5 + 4) = 5 + 15 - 10 + 4 + 12 - 8.$$

Sommes télescopiques. Il s'agit d'une simple formule très utile

$$\sum_{k=1}^{n} a_k - a_{k-1} = a_n - a_0.$$

Exemple 2.

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

Quelques sommes à connaitre.

$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$

$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$ si $q \neq 1$

$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

6 Coefficients binomiaux

Pour n entier naturel non nul, on rappelle que $n! = n(n-1)\dots 1$ et se lit « n factorielle ».

Définition I.7: Coefficient binomial

Pour $0 \leqslant k \leqslant n$ deux entiers naturels, on note $\binom{n}{k}$ le nombre de partie à k éléments d'un ensemble à n éléments.

Exemple 3. $\binom{4}{2} = \#\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\} = 6.$

Proposition I.8

Pour $0 \leqslant k \leqslant n$ deux entiers naturels, on a

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

Remarque. Au numérateur de la dernière expression on a un produit de k termes. Pour les calculs pratiques la seconde expression est plus efficace.

Preuve

Les deux expressions du coefficient binomial sont égales par simplification des termes $n-k, \dots, 2$ au numérateur et au dénominateur de la première expression. Pour obtenir une partie à k éléments on peut choisir successivement un premier élément (n choix), un deuxième ($n-1$ choix) et un k-ème ($n-k+1$ choix). Chaque partie est obtenue $k!$ fois par ce procédé correspondant aux façons d'ordonner cette partie.

Quelques formules à connaitre :

Théorème I.9: Egalité de Pascal

Pour $0 \leqslant k \leqslant n$ deux entiers naturels, on a

(i) $\binom{n}{k} = \binom{n}{n-k}$;

(ii) $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$;

(iii) $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Preuve

Par passage au complémentaire on obtient une bijection entre les parties à k éléments et celles à $n-k$ éléments. La deuxième formule s'obtient facilement par le calcul. Pour la dernière formule on distingue deux types de partie de $\{1, \dots, n+1\}$ à k éléments : celles qui contiennent $n+1$ et celles qui ne contiennent pas $n+1$. Il y en a respectivement $\binom{n}{k-1}$ et $\binom{n}{k}$. D'où la formule.

Le nom « coefficients binomiaux » est issu de la formule du binôme de Newton suivante :

Théorème I.10: Binôme de Newton

Soit a et b dans $\mathbb{R}$ et n dans $\mathbb{N}^*$. On a

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

Preuve

On écrit

$$(a+b)^n = (a+b)\dots(a+b)$$

et on imagine que l'on développe cette expression. Chaque terme de la somme obtenue s'obtient en choisissant des a dans certains facteurs et des b dans les autres. Ainsi, il y a $\binom{n}{k}$ façons d'obtenir $a^k b^{n-k}$.

Remarque. Pour la démonstration, on peut aussi faire une récurrence sur n en utilisant la troisième formule de la proposition I.9.

Voici une autre formule bien utile :

Proposition I.11

Soit a et b dans $\mathbb{R}$ et n dans $\mathbb{N}^*$. On a

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k.$$

Preuve

On part du côté le plus compliqué, on développe, sépare les sommes.

$$\begin{aligned}(a-b)\textstyle\sum_{k=0}^{n-1} a^{n-1-k}b^k &= (a\textstyle\sum_{k=0}^{n-1} a^{n-1-k}b^k) - b\textstyle\sum_{k=0}^{n-1} a^{n-1-k}b^k \\ &= \textstyle\sum_{k=0}^{n-1} a^{n-k}b^k - \textstyle\sum_{k=0}^{n-1} a^{n-1-k}b^{k+1}\end{aligned}$$

Dans la seconde somme on fait le changement d'indice

$$\begin{cases} l = k+1 \\ k = l-1 \end{cases}$$

$$\sum_{k=0}^{n-1} a^{n-1-k}b^{k+1} = \sum_{l=1}^{n} a^{n-l}b^l.$$

En réinjectant, on trouve

$$\begin{aligned}(a-b)\textstyle\sum_{k=0}^{n-1} a^{n-1-k}b^k &= \textstyle\sum_{k=0}^{n-1} a^{n-k}b^k - \textstyle\sum_{k=1}^{n} a^{n-k}b^k \\ &= a^n - b^n.\end{aligned}$$

Chapitre 2

Ensembles et applications

Sommaire

1 Ensembles et parties

1.1 Premiers exemples

Un ensemble est un « paquet » sans répétition et sans ordre qui est constitué de ce qu'il est convenu d'appelé ses éléments. Par exemple, les éléments de l'ensemble $\mathbb{N}$ sont les entiers $0, 1, 2, \ldots$. Par ailleurs

$$\{1, 4, 5\} = \{4, 1, 5\} = \{1, 1, 5, 5, 5, 4\}.$$

Lorsque l'on a un ensemble (comme $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{R}^2$) on peut en former d'autres : les parties de cet ensemble. Basiquement, il y a deux façons de définir une partie : paramétriquement (comme l'ensemble des éléments d'une certaines forme) ou implicitement (comme l'ensemble des éléments vérifiant une propriété). Par exemple

$$\{2k : k \in \mathbb{Z}\} = \{n \in \mathbb{Z} : n \in \mathbb{Z} \text{ est divisible par } 2\}.$$

Un autre exemple, emprunté à la géométrie :

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} = \{(\cos(t), \sin(t)) : t \in \mathbb{R}\}.$$

Remarquons que dans la deuxième description chaque point est répété une infinité de fois. Cependant dans l'ensemble on ne tient pas compte de cette répétition. Evidemment, on peut avoir des descriptions plus complexes mélangeant les 2 :

$$\{3k + 1 : k \in \mathbb{Z} \text{ est divisible par } 2\}.$$

1.2 Opérations sur les parties

Si A est une partie d'un ensemble E et x est un élément de E, on écrira $x \in A$ si x appartient à A et $x \notin A$ si x n'appartient pas à A.
Le *complémentaire* de A est défini par

$$E - A := \{x \in E : x \notin A\}.$$

On dit que A *est inclus dans* B si tout élément de A appartient à B. On note $A \subset B$.
La *réunion* de deux parties A et B d'un ensemble E est définie par

$$A \cup B := \{x \in E : x \in A \text{ ou } x \in B\}.$$

L'*intersection* de deux parties A et B d'un ensemble E est définie par

$$A \cap B := \{x \in E : x \in A \text{ et } x \in B\}.$$

Voici une liste de propriétés de ces opérations. Soit A, B et C trois parties d'un ensemble E.

$$\begin{array}{ll} A \cap B = B \cap A & A \cup B = B \cup A \\ A \cap (B \cap C) = (A \cap B) \cap C & A \cup (B \cup C) = (A \cup B) \cup C \\ A \subset B \iff A \cap B = A & A \subset B \iff A \cup B = B \end{array}$$

$$\begin{array}{c} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{array}$$

$$\begin{array}{c} E - (A \cup B) = (E - A) \cap (E - B) \\ E - (A \cap B) = (E - A) \cup (E - B) \end{array}$$

1.3 Produit cartésien

Le produit cartésien $E \times F$ de deux ensembles E et F est l'ensemble des symboles (x, y), appelés *couples* avec $x \in E$ et $y \in F$. Il est important de comprendre que

$$(x, y) = (z, t) \iff x = z \text{ et } y = t.$$

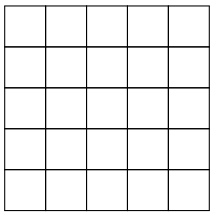
Par exemple,

$$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\},$$

et

$$\{0, 1\} \times \{a, b, c\} = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}.$$

L'ensemble $\{0, 1, \dots 5\} \times \{0, 1, \dots 5\}$ s'identifie à l'ensemble des points du quadrillage suivant :



Enfin, $(2, 2)$ est permis, $(2, 3) \neq (3, 2)\dots$ Remarquons aussi que « $(2, 2) = 2$ » n'a pas de sens car de part et d'autre d'un signe égal on doit avoir deux éléments d'un même ensemble.

2 Applications

2.1 Premiers exemples

Une *application* f est la donnée de deux ensembles E et F et d'une flèche $f : E \longrightarrow F$ qui associe à chaque élément x de E un élément noté $f(x)$ de F. Le *graphe de* f est la partie suivante de $E \times F$:

$$\Gamma(f) := \{(x, f(x)) : x \in E\}.$$

Il est important de comprendre que E et F font parties de la donnée. Ainsi, sin n'est pas une application.

(i) Certaines applications sont données par une formule :

$$\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 2x + 3 \end{array} \qquad \begin{array}{rccc} f : & \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \frac{2}{x} + 3 \end{array} \qquad \begin{array}{rccc} f : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & -2x + 7 \end{array}$$

(ii) ou par plusieurs formules :

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} 2x + 5 \text{ si } x \leqslant 0 \\ 7x + 5 \text{ si } x > 0 \end{cases} \end{array}$$

(iii) ou par une propriété caractéristique :

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \text{l'unique entier } n \text{ tel que } n \leqslant x < n + 1 \end{array}$$

(iv) ou par une liste exhaustive :

$$\begin{array}{c} \{1, 2, 3\} \longrightarrow \{1, 2, 3\} \\ 1 \mapsto 2 \quad 2 \mapsto 2 \quad 3 \mapsto 1 \end{array}$$

(v) ou que sais-je encore...

Il est important de comprendre que pour tout $x \in E$ il y a un unique $f(x)$ dans F. Exercice. Illustrer cette propriété sur le « modèle » des patates, des étiquettes, des graphes.

2.2 Injectivité, surjectivité, bijectivité

Définition II.12: Injective, surjective, bijective

(i) Une application $f : E \longrightarrow F$ est *injective* si

$$\forall x, y \in E \qquad f(x) = f(y) \implies x = y.$$

(ii) Une application $f : E \longrightarrow F$ est *surjective* si

$$\forall y \in F \qquad \exists x \in E \quad f(x) = y.$$

(iii) Une application $f : E \longrightarrow F$ est *bijective* si elle est injective et surjective.

Exercice 1. *Illustrer l'injectivité, la surjectivité et la bijectivité sur les « modèles » des patates, des étiquettes, des graphes.*

Exercice 2. *Traduire par une phrase avec $\forall$ and $\exists$ le fait d'être une bijection.*

Une application $f : E \longrightarrow F$ est bijective si

$$\forall y \in F \quad \exists! x \in E \quad f(x) = y.$$

L'affirmation précédente permet d'associer un unique élément x à chaque élément y de E. Ainsi, on définit une application

$$f^{-1} : F \longrightarrow E, \, y \longmapsto x.$$

L'application f^{-1} ainsi définie est appelée réciproque de f et est caractérisée parmi les applications de F dans E par les deux propriétés suivantes

$$f^{-1} \circ f = \mathrm{Id}_E \qquad f \circ f^{-1} = \mathrm{Id}_F.$$

Exemple 4. Considérons $f : \mathbb{R}^+ \longrightarrow \mathbb{R}^+, x \longmapsto x^2$. Cette application est bijective et $f^{-1} : \mathbb{R}^+ \longrightarrow \mathbb{R}^+, x \longmapsto \sqrt{x}$.

2.3 Composition

Soit $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. On définit alors

$$\begin{array}{rccc} g \circ f \ : & E & \longrightarrow & G \\ & x & \longmapsto & g(f(x)) \end{array}$$

L'application $g \circ f$ est appelé la composée de f et g.

Remarques. (i) Pour pouvoir définir $g \circ f$, il faut que l'ensemble d'arrivée de f soit égal à (ou inclus dans) l'ensemble de départ de g.

(ii) Dans la représentation graphique avec des patates, la flèche de f est à gauche de la flèche de g dans $g \circ f$. Cela correspond au fait que pour calculer $g \circ f(2)$ il faut d'abord calculer $f(2)$ puis g de la valeur obtenue.

Exercice 3. *(i) Soit $f : \mathbb{R} \longrightarrow \mathbb{R}, x \mapsto \sin(x)$, $g : \mathbb{R} \longrightarrow \mathbb{R}, x \mapsto x + 2$ et $h : \mathbb{R} \longrightarrow \mathbb{R}, x \mapsto 3x$. Calculer les 6 fonctions $f \circ g$, $g \circ f$, $f \circ h$, $h \circ f$, $g \circ h$ et $h \circ g$.*

(ii) On revient à la situation de la définition. Montrer que si $g \circ f$ est injective alors f l'est. Interpréter ce résultat sur le « modèle des patates ». La réciproque est-elle vraie ?

(iii) On revient à la situation de la définition. Montrer que si $g \circ f$ est surjective alors g l'est. Interpréter ce résultat sur le « modèle des patates ». La réciproque est-elle vraie ?

2.4 Image directe, image réciproque

Soit $f : E \longrightarrow F$ une application. Si $A \subset E$ est une partie de E, on appelle *image directe de* A la partie de F suivante :

$$f(A) := \{f(x) \,:\, x \in A\}.$$

Si $B \subset F$ est une partie de F, on appelle *image réciproque* la partie de E suivante :

$$f^{-1}(B) := \{x \in E \,:\, f(x) \in B\}.$$

L'image réciproque jouie de propriétés agréables :

Proposition II.13

Soit A et B deux parties de F. Alors

(i) $f^{-1}(F - A) = E - f^{-1}(A)$;

(ii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;

(iii) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

La preuve est laissée en exercice.

Attention. Ces trois propriétés ne sont pas toutes vraies pour l'image directe. Comme exercice, justifier cette dernière affirmation en montrant celles qui sont vraies et trouvant des contre-exemples pour les autres.

Chapitre 3

Logique

Sommaire

1 Prédicats

1.1 Définitions

Une *assertion* est une affirmation mathématique qui peut être vraie ou fausse. Exemples : 8 est un entier pair ; tous les entiers sont des nombres rationnels ; tout nombre réel est le carré d'un nombre réel ; pour tout entier n, l'entier $6n+1$ est impair...
Un *prédicat* est une « assertion » dépendant d'une ou plusieurs variables. Sa valeur de vérité dépend de la valeur de la variable. Exemples : l'entier n est pair ; le réel x est un nombre rationnel ; le réel x est le carré d'un nombre réel...

1.2 Opérations

Sur les prédicats, on a plusieurs opérations : le *et*, le *ou*, la négation *non* et l'implication définies par le tableau de vérité suivant :

P	Q	P *et* Q	P *ou* Q	non(P)	$P \implies Q$
V	V	V	V	F	V
V	F	F	V	F	F
F	V	F	V	V	V
F	F	F	F	V	V

La plus difficile à comprendre et peut-être la plus importante en mathématique est l'implication : $P \implies Q$. Elle est équivalente à l'affirmation suivante « si P est vraie alors Q est vraie ». En particulier, lorsque P est fausse cette affirmation est vraie. Le seul cas où elle est fausse est si P est vraie et Q est faux.
Il ne faut pas non plus confondre le si alors mathématique avec celui du langage courant. En effet, il n'y a pas de notion de cause et conséquence enn mathématiques. Dans la vie courante on pourrait dire s'il y a des nuages alors il pleut pour dire que les nuages sont la cause de pluie. En math, on dirait le contraire, s'il pleut alors il y a des nuages. Ceci signifie si je constate qu'il pleut c'est nécessairement qu'il y a des nuages car ceux-ci sont la seule cause de pluie.

1.3 Composé d'opération

Théorème III.14: Négation

Soit P et Q deux prédicats.

(i) $P \implies Q$ est équivalent à non(P) *ou* Q ;

(ii) non$(P$ *ou* $Q)$ est équivalent à non(P) *et* non(Q) ;

(iii) non$(P$ *et* $Q)$ est équivalent à non(P) *ou* non(Q) ;

Preuve

Il suffit de vérifier que les prédicats équivalents ont la même table de vérité. Pour la première équivalence cela donne :

P	Q	non(P)	non(P) *ou* Q	$P \implies Q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

2 Les quantificateurs pour tout et il existe

La notation $\forall x \in E$ se lit pour tout x dans E. La notation $\exists x \in E$ se lit il existe x dans E. Enfin, La notation $\exists! x \in E$ se lit il existe un unique x dans E. Une règle d'or :

Pour montrer un $\forall$ on écrit « soit ».

Plusieurs choses importantes à comprendre :

(i) Pour contredire le fait que tous les éléments de E ont une propriété il faut et il suffit de trouver un contre-exemple. Ceci s'écrit : les deux prédicats

$$\text{non}(\forall x \in E \qquad P(x))$$

et

$$\exists x \in E \qquad \text{non}(P(x)))$$

sont équivalents.

(ii) Dit autrement, pour contredire, qu'il existe un élément de E vérifiant une propriété il faut montrer que tous les éléments de E la contredisent. Ainsi

$$\text{non}(\exists x \in E \qquad P(x))$$

et

$$\forall x \in E \qquad \text{non}(P(x)))$$

sont équivalents.

(iii) Une affirmation du type

$$\exists! x \in E \qquad P(x)$$

est équivalente à

$$\begin{cases} \exists x \in E \qquad P(x) \\ \text{Si } P(x) \text{ et } P(y) \text{ sont vraies alors } x = y. \end{cases}$$

Voici quelques exemples de négation.
Les deux lignes suivantes sont une proposition P et sa négation non(P)

$$\begin{array}{llll} \forall x \in \mathbb{R}^+, & \exists \alpha \in \mathbb{R}^+ & \alpha < x \\ \exists x \in \mathbb{R}^+, & \forall \alpha \in \mathbb{R}^+ & \alpha \geqslant x \end{array}$$

Les deux lignes suivantes sont une proposition Q et sa négation non(Q)

$$\begin{array}{llllll} \exists x \in \mathbb{R}, & \forall n \in \mathbb{N}, & \exists y \in \mathbb{R}, & x = ny \\ \forall x \in \mathbb{R}, & \exists n \in \mathbb{N}, & \forall y \in \mathbb{R}, & x \neq ny \end{array}$$

Un dernier exemple :

$$\begin{array}{ll} \forall x \in \mathbb{R}, & [(\exists x \in \mathbb{N},\ n \leqslant x) \implies (\forall p \in \mathbb{N},\ p \geqslant x)] \\ \exists x \in \mathbb{R}, & (\exists x \in \mathbb{N},\ n \leqslant x) \textit{ et } (\exists p \in \mathbb{N},\ p < x) \end{array}$$

3 Quelques techniques de preuves

3.1 Disjonction de cas

Un exemple vaut mieux qu'un long discours. Montrer que

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R} : x < y^2.$$

Preuve

Soit $x \in \mathbb{R}$.

(i) Si $x < 0$, alors $y = 0$ convient car $x < 0 = y^2$.

(ii) Si $0 \leqslant x < 1$, alors $y = 1$ convient car $x < 1 = y^2$.

(iii) Si $x = 1$ alors $y = 2$ convient car $x = 1 < 4 = y^2$.

(iv) Si $x > 1$ alors $y = x$ convient.

Il est important que les cas étudiés recouvrent toutes les possibilités. Ici, tout $x \in \mathbb{R}$ vérifie l'une des 4 assertions $x < 0$, $0 \leqslant x < 1$, $x = 1$ ou $x > 1$.

3.2 Ensembliste

Pour montrer une inclusion $A \subset B$ entre deux parties A et B d'un ensemble E, on prend un élément de A et on montre qu'il est dans B.

> Soit $x \in A$.
> ...
> alors $x \in B$.
> On vient de montrer que $A \subset B$.

On a encore un avatar de la démonstration par l'absurde. Pour montrer $A \subset B$, on peut montrer que $(E - B) \subset (E - A)$:

> Soit $x \in E$ tel que $x \notin B$.
> ...
> alors $x \notin A$.
> On vient de montrer que $(E - B) \subset (E - A)$, c'est-à-dire que $A \subset B$.

Pour montrer une égalité $A = B$ entre deux parties A et B d'un ensemble E, le plus souvent on montre séparément $A \subset B$ et $B \subset A$.

Pour montrer qu'un élément x de E appartient à $A \cap B$, on montre séparément que $x \in A$ et $x \in B$.

Pour montrer qu'un élément x de E appartient à $A \cup B$, on suppose que $x \notin B$ et on montre $x \in A$ (ou de manière symétrique on suppose que $x \notin A$ et on montre $x \in B$.

> Soit $x \in E$.
> Supposons que $x \notin B$.
> ...
> alors $x \in A$.
> On vient de montrer que $x \in A \cup B$.

Exercice 4. *Soit A, B et C trois parties de E.*

(i) Montrer que
$$(A \cup B \subset A \cup C \text{ et } A \cap B \subset A \cap C) \implies (B \subset C).$$

(ii) Montrer que
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

(iii) Montrer que
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

3.3 Et, ou, et implication

Pour montrer un « et » P *et* Q, il faut montrer séparément, successivement P puis Q.

Plus difficile, pour montrer un « ou » P *ou* Q, il faut supposer que l'une des deux assertions est fausse et, fort de cette hypothèse, montrer l'autre.

Pour montrer une implication $P \implies Q$ on a basiquement deux manières de démarrer :

(i) *Raisonnement direct* : on suppose que P est vrai et on montre Q. Ici, P devient une hypothèse et Q une conclusion.

(ii) *Raisonnement par contraposé* : on suppose que non(Q) est vraie et on montre non(P). Ici, non(Q) devient une hypothèse et non(P) une conclusion. La validité de cette approche résulte de la proposition III.14.

Exemples 5. (i) Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction. Montrer que

$$(f \text{ impaire}) \implies (f(0) = 0).$$

(ii) Soit x un réel positif. Montrer que

$$(\forall \varepsilon > 0, \quad x < \varepsilon) \implies (x = 0).$$

3.4 Prouver qu'une assertion est fausse

Pour montre qu'une assertion de la forme

$$\forall x \in E \quad P(x)$$

est FAUSSE, il suffit de trouver un élément $x \in E$ tel que $P(x)$ est fausse. Ainsi, on montre la négation :

$$\exists x \in E \quad \text{non}(P(x)).$$

Exercice 5. *Montrer que l'assertion*

$$\forall x \in \mathbb{R} \quad \forall \varepsilon > 0 \quad (|x| < \varepsilon \implies x = 0)$$

est fausse.

3.5 Raisonnement par récurrence

Le raisonnement par récurrence permet de montrer des propriétés du type :

$$\forall n \in \mathbb{N} \quad P(n) \text{ est vraie}$$

On montre pour cela successivement les deux assertions suivantes :

$$\begin{array}{l} P(0) \text{ est vraie} \\ \forall n \in \mathbb{N} \qquad (P(n) \implies P(n+1)) \end{array}$$

Il y a une variante appelée récurrence forte :

$$\begin{array}{l} P(0) \text{ est vraie} \\ \forall n \in \mathbb{N} \qquad ((\forall k \in \{0, \ldots, n\} \quad P(k) \text{ est vraie}) \implies P(n+1) \text{ est vraie}) \end{array}$$

Une preuve par récurrence prend la forme suivante :

Initialisation. Soit $n = 0$.
[...].
Alors $P(0)$ est vraie.

Hérédité. Soit $n \in \mathbb{N}$. Supposons que $P(n)$ est vraie.
(ou supposons que pour tout $k \leqslant n$, $P(k)$ est vraie).
[...] « par hypothèse de récurrence » [...]
Alors $P(n+1)$ est vraie.

Chapitre 4

Fonctions usuelles

Sommaire

1 Polynômes

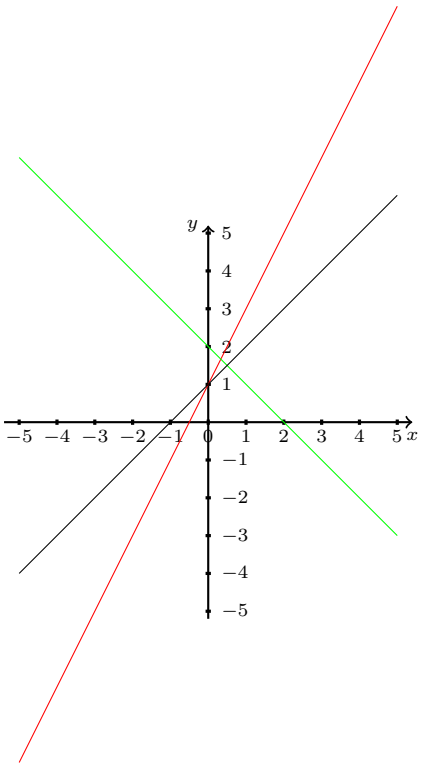
1.1 Fonctions affines

Une fonction affine est une fonction

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & ax+b \end{array}$$

où a et b sont des constantes réelles données. Cette fonction est dérivable et sa dérivée est $f' = a$. On peut retrouver a et b à partir de f comme suit

$$b = f(0) \qquad a = \frac{f(x_1) - f(x_2)}{x_1 - x_2} \quad \forall x_1 \neq x_2 \in \mathbb{R}.$$



Exercice 6. *Reconnaitre sur le dessin ci-dessus les graphes de* $x \mapsto 2x+1$, $x \mapsto -x+2$ *et* $x \mapsto x+1$.

1.2 Polynômes de degré 2

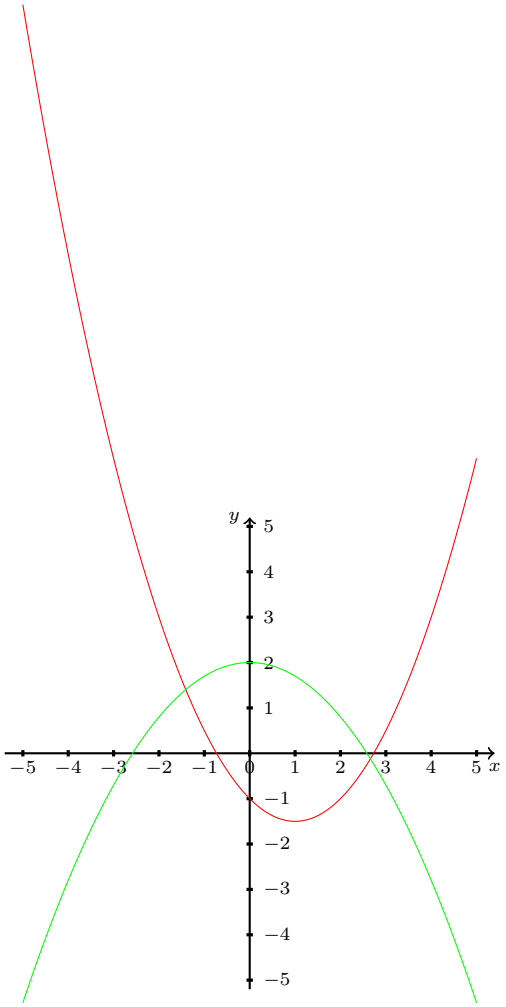
Une fonction polynomiale de degré 2 est une fonction

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & ax^2+bx+c \end{array}$$

où a, b et c sont des constantes réelles données telles que $a \neq 0$. Cette fonction est dérivable et sa dérivée est $f'(x) = 2ax + b$. Les limites sont

$$\lim_{x\to+\infty} f(x) = \lim_{x\to-\infty} f(x) = \begin{cases} +\infty & \text{si } a > 0 \\ -\infty & \text{si } a < 0 \end{cases}$$

La fonction a un minimum (resp. maximum) en $-b/2a$ si $a > 0$ (resp. $a < 0$).



Exercice 7. *Lire sur les graphes ci-dessus, le signe de a et les valeurs de $\frac{-b}{2a}$ et b/a.*

2 Partie Entière

Définition IV.15: Partie Entière

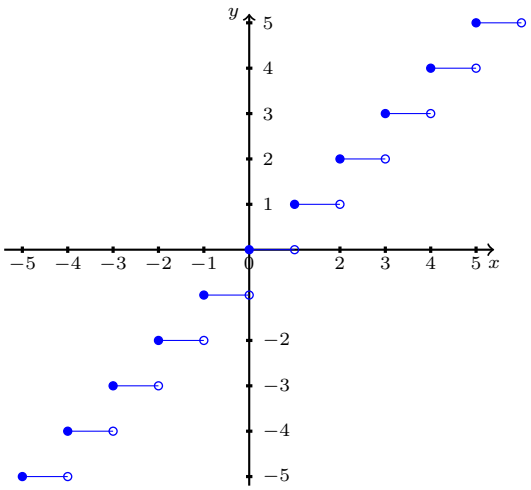
Pour tout $x \in \mathbb{R}$, il existe un unique entier relatif, noté $E(x)$ et appelé *partie entière de x*, tel que

$$E(x) \leqslant x < E(x) + 1.$$

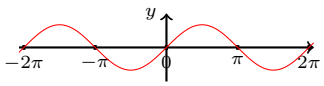
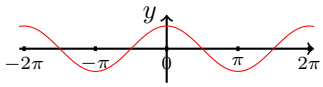
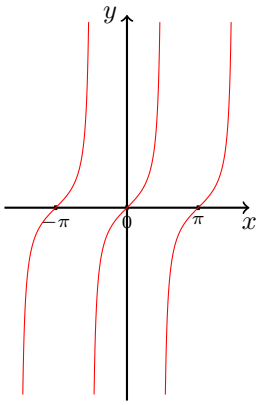
Il s'avère que cette définition est pratique pour les démonstrations. Il convient de remarquer que $E(\pi) = 3$, $E(7) = 7$, $E(-2,28) = -3$ et $E(-4) = -4$.
On obtient ainsi la fonction partie entière

$$\begin{array}{rccc} E: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & E(x) \end{array}$$

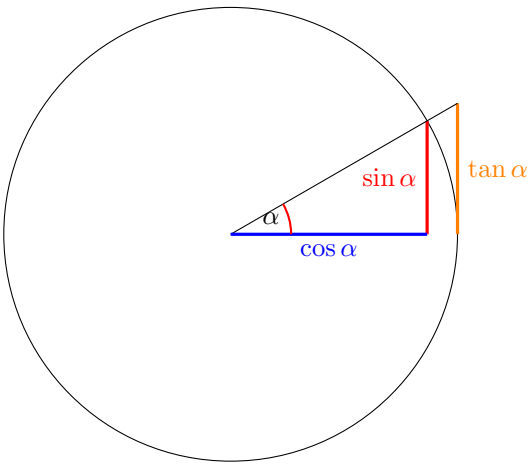
La fonction E est 1-périodique, dérivable sur $\mathbb{R} - \mathbb{Z}$ (de dérivée nulle) et non continue en tout point de $\mathbb{Z}$.



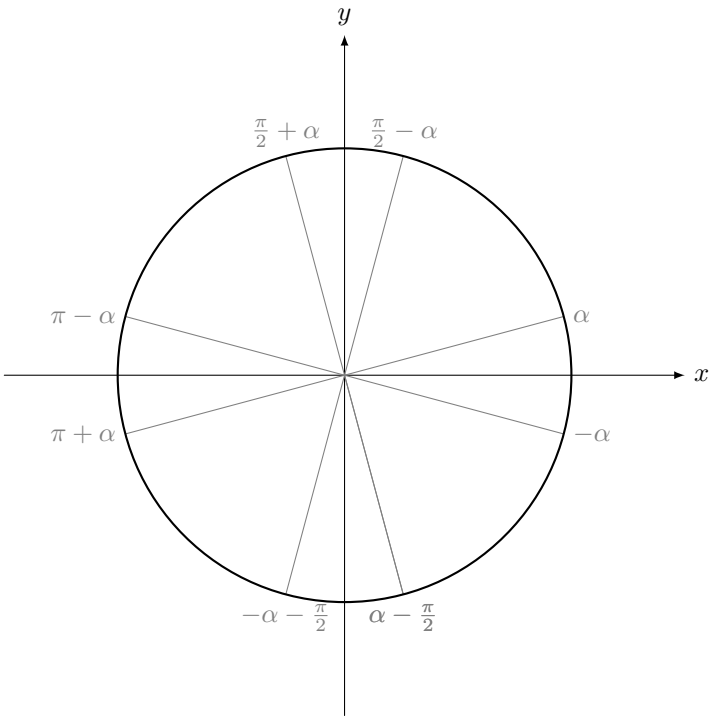
3 Fonctions trigonométriques

	$\sin(x)$	$\cos(x)$	$\tan(x)$
domaine	$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R} - \frac{\pi}{2}(2\mathbb{Z}+1)$
parité	impaire	paire	impaire
période	2π	2π	π
f'	$\cos(x)$	$-\sin(x)$	$1+\tan^2(x)$
primitive	$-\cos(x)$	$\sin(x)$	$-\ln(\lvert\cos(x)\rvert)$
graphe			

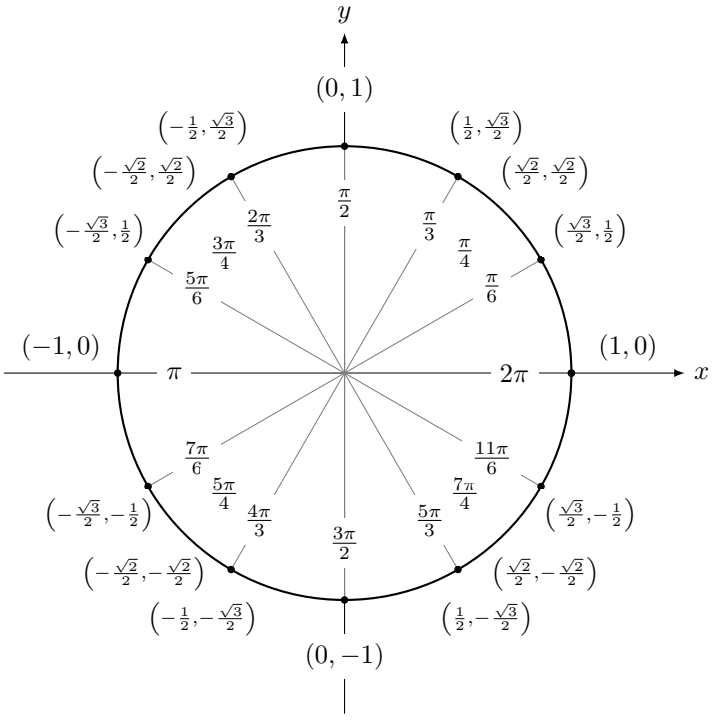
Le cercle trigonométrique :



Angles associés :



Quelques valeurs de sin et cos :



Formulaire

S'il n'y en avait qu'une...

$$\sin^2(x) + \cos^2(x) = 1$$

Angles associés

$$\begin{array}{lll} \sin(-x) = -\sin(x) & \sin(\pi - x) = \sin(x) & \sin(\pi + x) = -\sin(x) \\ \cos(-x) = \cos(x) & \cos(\pi - x) = -\cos(x) & \cos(\pi + x) = -\cos(x) \end{array}$$

$$\begin{array}{ll} \sin(\frac{\pi}{2} - x) = \cos(x) & \sin(\frac{\pi}{2} + x) = \cos(x) \\ \cos(\frac{\pi}{2} - x) = \sin(x) & \cos(\frac{\pi}{2} + x) = -\sin(x) \end{array}$$

Formules d'addition

$$\sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b) \quad \cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$$

Formules de linéarisation

$$\sin^2(a) = \frac{1-\cos(2a)}{2} \quad \cos^2(a) = \frac{1+\cos(2a)}{2} \quad \tan^2(a) = \frac{1-\cos(2a)}{1+\cos(2a)}$$

Passage d'un produit à une somme

$$\begin{array}{l} \sin(a)\sin(b) = \frac{1}{2}(\cos(a-b) - \cos(a+b)) \\ \cos(a)\cos(b) = \frac{1}{2}(\cos(a-b) + \cos(a+b)) \\ \cos(a)\sin(b) = \frac{1}{2}(\sin(a+b) - \sin(a-b)) \end{array}$$

Passage d'une somme à un produit

$$\sin(p) + \sin(q) = 2\sin(\tfrac{p+q}{2})\cos(\tfrac{p-q}{2})) \quad \cos(p) + \cos(q) = 2\cos(\tfrac{p+q}{2})\cos(\tfrac{p-q}{2}))$$

En fonction de $t = \tan(\frac{a}{2})$

$$\cos(a) = \frac{1-t^2}{1+t^2} \quad \sin(a) = \frac{2t}{1+t^2} \quad \tan(a) = \frac{2t}{1-t^2}$$

Quelques valeurs

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\cos(\theta)$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\sin(\theta)$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1

4 Logarithme et exponentielle

4.1 Exponentielle

On admet (provisoirement) le théorème suivant.

Théorème IV.16. Caractérisation de l'exponentielle

Il existe une unique fonction dérivable $f : \mathbb{R} \longrightarrow \mathbb{R}$ telle que

$$\begin{cases} f'(x) = f(x) & \forall x \in \mathbb{R} \\ f(0) = 1 \end{cases}$$

Cette fonction est notée $\exp : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \exp(x)$.

L'exponentielle transforme addition en multiplication :

Théorème IV.17: Exponentielle d'une somme

Pour tout x et y dans $\mathbb{R}$, on a

$$\exp(x+y) = \exp(x)\exp(y).$$

Par ailleurs,

$$\exp(x-y) = \frac{\exp(x)}{\exp(y)}.$$

Preuve

Fixons $y \in \mathbb{R}$. Considérons la fonction $g : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto \frac{\exp(x+y)}{\exp(x)\exp(y)}$. On vérifie que g est dérivable, que sa dérivée vaut 0 et que g vaut 1 en 0. On en déduit que g est la fonction constante égale à 1.
Pour fonctionner cette preuve nécessite d'avoir montré que exp ne s'annule pas. En effet, on a divisé par $\exp x.\exp y$. On peut procéder ainsi. Posons $h : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto \exp(x)\exp(-x)$. On vérifie que h est dérivable, que sa dérivée vaut 0 et que h vaut 1 en 0. On en déduit que h est la fonction constante égale à 1. Donc exp ne s'annule pas.

La démonstration implique que exp ne s'annule jamais ($\exp(x).\exp(-x) = 1$). Mais alors par le théorème des valeurs intermédiaires

$$\forall x \in \mathbb{R} \qquad \exp(x) > 0.$$

On pose $e = \exp(1) \simeq 2,718\ldots$. On note parfois $e^x := \exp(x)$. Les formules se mettent alors à ressembler aux formules connues pour les puissances entières :

$$e^1 = e \quad e^{x+y} = e^x e^y \quad e^{-x} = \frac{1}{e^x}.$$

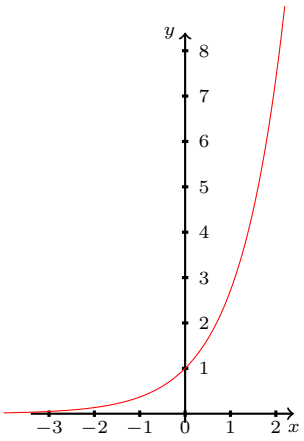
Proposition IV.18

La fonction exp est strictement croissante et

$$\lim_{x\to+\infty} \exp(x) = +\infty$$
$$\lim_{x\to-\infty} \exp(x) = 0$$

Preuve

Comme exp est croissante la limite en $+\infty$ existe dans $\mathbb{R} \cup \{+\infty\}$. Elle ne peut être finie car $\lim_{x\to+\infty} \exp(2x) = \exp(2) \lim_{x\to+\infty} \exp(x)$.
Comme $\exp(x) = \frac{1}{\exp(-x)}$ la limite en $-\infty$ en découle.



4.2 Logarithme

Théorème IV.19: Définition du logarithme

L'application $\exp : \mathbb{R} \longrightarrow]0, +\infty[$ est une bijection. Sa fonction réciproque est notée $\ln :]0, +\infty[\longrightarrow \mathbb{R}$. Autrement dit la fonction ln est définie par la relation

$$\exp(\ln(x)) = x \qquad \forall x \in]0, +\infty[.$$

Preuve

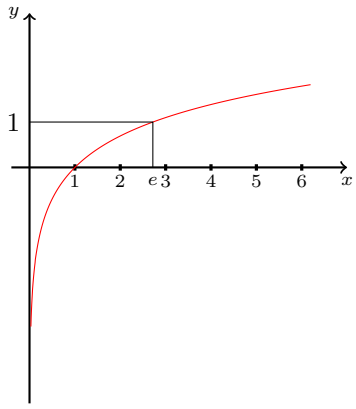
Ceci est une conséquence du tableau de variation de exp et du théorème des valeurs intermédiaires (que nous démontrerons plus tard).

Les principales propriétés de ln sont résumées ici :

Théorème IV.20: Propriétés de ln

(i) La fonction $\ln :]0, +\infty[\longrightarrow \mathbb{R}$ est bijective.
(ii) $\ln(1) = 0$, $\ln(e) = 1$.
(iii) Pour tout $x, y \in]0, +\infty[$, on a $\ln(xy) = \ln(y) + \ln(y)$ et $\ln(\frac{x}{y}) = \ln(y) - \ln(y)$.
(iv) La fonction ln est croissante.
(v) Ses limites sont $\lim_{x\to0, x>0} \ln(x) = -\infty$ et $\lim_{x\to+\infty} \ln(x) = +\infty$.

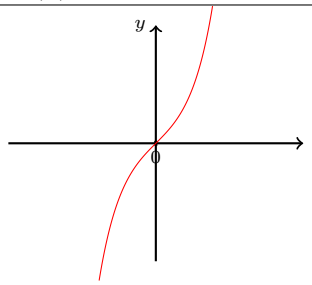
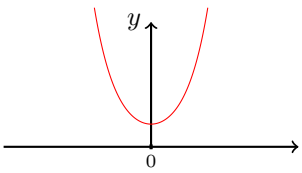
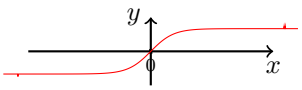
(vi) La fonction ln est dérivable et sa dérivée est $]0,+\infty[\longrightarrow \mathbb{R}, x \longmapsto \frac{1}{x}$.



4.3 Les fonctions hyperboliques

On définit 3 fonctions sur $\mathbb{R}$ par les formules suivantes

$$\begin{array}{rccc} \text{sh}: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \frac{e^x-e^{-x}}{2} \end{array} \qquad \begin{array}{rccc} \text{ch}: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \frac{e^x+e^{-x}}{2} \end{array} \qquad \begin{array}{rccc} \tanh: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \frac{\text{sh}(x)}{\text{ch}(x)} = \frac{e^x-e^{-x}}{e^x+e^{-x}} \end{array}$$

	$\text{sh}(x)$	$\text{ch}(x)$	$\tanh(x)$
domaine	$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R}$
parité	impaire	paire	impaire
$\lim_{x\to+\infty}$	$+\infty$	$+\infty$	1
$\lim_{x\to-\infty}$	$-\infty$	$+\infty$	-1
f'	$\text{ch}(x)$	$\text{sh}(x)$	$1-\tanh^2(x)$
graphe			

Formulaire

$$\mathrm{ch}^2(x) - \mathrm{sh}^2(x) = 1$$

Exponentielle

$$\exp(x) = \mathrm{ch}(x) + \mathrm{sh}(x) \qquad \exp(-x) = \mathrm{ch}(x) - \mathrm{sh}(x)$$

Formule de puissance

$$(\mathrm{sh}(x) + \mathrm{ch}(x))^n = \mathrm{sh}(nx) + \mathrm{ch}(nx) \quad \forall n \in \mathbb{N}$$

Formules d'addition

$$\mathrm{sh}(a+b) = \mathrm{sh}(a)\,\mathrm{ch}(b) + \mathrm{ch}(a)\,\mathrm{sh}(b) \qquad \mathrm{ch}(a+b) = \mathrm{ch}(a)\,\mathrm{ch}(b) + \mathrm{sh}(a)\,\mathrm{sh}(b)$$

Pour $a = b$, on obtient

$$\mathrm{sh}(2a) = 2\,\mathrm{sh}(a)\,\mathrm{ch}(b) \qquad \mathrm{ch}(2a) = \mathrm{ch}(a)^2 - \mathrm{sh}(a)^2 \qquad \tanh(2a) = \frac{2\tanh(a)}{1+\tanh^2(a)}$$

Formules de linéarisation

$$\mathrm{sh}^2(a) = \frac{\mathrm{ch}(2a)-1}{2} \qquad \mathrm{ch}^2(a) = \frac{\mathrm{ch}(2a)+1}{2} \qquad \tanh^2(a) = \frac{\mathrm{ch}(2a)-1}{\mathrm{ch}(2a)+1}$$

Passage d'une somme à un produit

$$\mathrm{sh}(p) + \mathrm{sh}(q) = 2\,\mathrm{sh}(\frac{p+q}{2})\,\mathrm{ch}(\frac{p-q}{2}) \qquad \mathrm{ch}(p) - \mathrm{ch}(q) = 2\,\mathrm{sh}(\frac{p+q}{2})\,\mathrm{sh}(\frac{p-q}{2})$$

Valeurs à l'origine

$$\mathrm{sh}(0) = 0 \qquad \mathrm{ch}(0) = 1 \qquad \tanh(0) = 0$$

4.4 Fonctions puissances

Dans cette section, nous étudions les fonctions puissances a^α. La définition est un peu délicate car le domaine de définition de $a \mapsto a^\alpha$ dépend de α. Avant de rentrer dans le détail, on donne le formulaire :

$$\boxed{\begin{array}{lll} 1^\alpha = 1 & a^\alpha a^\beta = a^{\alpha+\beta} & (a^\alpha)^\beta = a^{\alpha\beta} \\ & (ab)^\alpha = a^\alpha b^\alpha & a^{-\alpha} = \frac{1}{a^\alpha} \end{array}}$$

Détaillons à présent la définition de a^α en fonction de la valeur de α.

Le cas α entier naturel : $\alpha = n \in \mathbb{N}$.
Dans ce cas, $a^n = a \times \cdots \times a$, n fois est défini pour tout $a \in \mathbb{R}$. Remarquons que $a \mapsto a^n$ de $\mathbb{R}$ dans lui-même a la même parité que n.

Le cas α entier négatif : $\alpha = n \in -\mathbb{N}^*$.
Dans ce cas,

$$a^n = \frac{1}{a} \times \cdots \times \frac{1}{a} \qquad (-n) \text{ fois}$$

est défini pour tout $a \in \mathbb{R}^*$.

Le cas où α l'inverse d'un entier naturel : $\frac{1}{\alpha} \in \mathbb{N}^*$.
Dans ce cas, $a^{\frac{1}{n}}$ est la racine n^{ieme} de a, elle est définie pour

$$\begin{array}{ll} a \in [0; +\infty[& \text{si } \frac{1}{\alpha} \text{ est pair} \\ a \in \mathbb{R} & \text{si } \frac{1}{\alpha} \text{ est impair} \end{array}$$

Le cas où α réel. $\alpha \in \mathbb{R}$.
Ici, a^α est défini pour tout $a \in]0; +\infty[$ par la formule

$$\boxed{a^\alpha := \exp(\alpha \ln(a))}$$

Quelques limites comparées. Pour $\alpha, \beta > 0$, on a

$$\boxed{\lim_{x\to+\infty} \frac{\exp(x)}{x^\alpha} = +\infty \qquad \lim_{x\to+\infty} \frac{x^\alpha}{\ln(x)^\beta} = +\infty \qquad \lim_{x\to 0^+} x^\alpha \ln(x)^\beta = 0}$$

5 Convexité

Une fonction f définie sur un intervalle de $\mathbb{R}$ est *convexe* si son graphe est au-dessous de ses cordes. Voici une définition plus formelle.

Définition IV.21: Fonction convexe

Soit f une fonction définie sur un intervalle I de $\mathbb{R}$. Alors f est *convexe* si

$$\forall x, y \in I \quad \forall t \in [0,1] \quad f(tx + (1-t)y) \leqslant tf(x) + (1-t)f(y).$$

Elle est dite *concave* si $-f$ est convexe.

Pour $x < y$ fixés, $tx + (1-t)y$ parcourt le segment $[x; y]$ lorsque t parcourt $[0; 1]$. Les fonctions convexes peuvent être caractérisées par une propriété de monotonie des pentes.

Théorème IV.22. Pentes des fonctions convexes

Soit f une fonction définie sur un intervalle I de $\mathbb{R}$. Alors f est *convexe* si et seulement si pour tout $a < b < c$ dans I, on a

$$\frac{f(b)-f(a)}{b-a} \leqslant \frac{f(c)-f(a)}{c-a} \leqslant \frac{f(c)-f(b)}{c-b}$$

Si f est dérivable, on a d'autres caractérisations :

Théorème IV.23. Dérivée d'une fonction convexe

Soit f une fonction définie sur un intervalle I de $\mathbb{R}$ et dérivable. Alors, les conditions suivantes sont équivalentes

(i) f est convexe ;

(ii) f' est croissante sur I ;

(iii) le graphe de f est au-dessus de ses tangentes.

Grâce à ce critère, on peut facilement montrer que exp est convexe. De même, si $\alpha \geqslant 1$ la fonction $\mathbb{R}^{+*} \longrightarrow \mathbb{R}, x \longmapsto x^\alpha$ est convexe.
La fonction ln est concave. Si $\alpha \leqslant 1$ la fonction $\mathbb{R}^{+*} \longrightarrow \mathbb{R}, x \longmapsto x^\alpha$ est concave.

Si f est deux fois dérivable, on a une autre caractérisation :

Théorème IV.24. Dérivée seconde d'une fonction convexe

Soit f une fonction définie sur un intervalle I de $\mathbb{R}$ et deux fois dérivable.
Alors, f est convexe si et seulement si f'' est positive ou nulle sur I.

Chapitre 5

Suites réelles

Sommaire

Nous allons définir dans ce chapitre et le suivant une notion fondamental en analyse, celle de limite. Qu'ont en commun les objets suivants :

(i) Une dérivée ?

(ii) Une intégrale ?

(iii) Une somme infinie ?

(iv) La longueur d'une courbe ?

Ce sont toutes des **limites**. Bien que les mathématiciens utilisent ces différents objets depuis la renaissance, ce n'est que vers la fin du 18^e siècle et le début du 19^e siècle que la notion de limite, grâce à D'Alembert et à Cauchy, commence à être formalisée. Le cours d'analyse de Cauchy, alors qu'il professait à l'école Polytechnique, allait d'ailleurs devenir une référence pour tout travail en analyse au 19^e siècle. Malgré la grande rigueur de son contenu, il subsistait des lacunes, comme une preuve, fausse, que la limite d'une série de fonctions continues est continue. Le mathématicien allemand Karl Weierstrass vers 1860 et ses élèves formalisèrent définitivement la notion de limite et parachevèrent l'œuvre de Cauchy. La forme actuelle de la définition d'une limite est exactement celle donnée par Weierstrass.
Il vous faudra prendre le temps dans ce chapitre de bien comprendre les nouvelles notions, de faire et refaire les démonstrations. Il a fallu plusieurs siècles pour que les mathématiciens formalisent ces concepts correctement. Il est alors naturel que ceux-ci vous demandent un travail approfondi. Vous êtes en train de préparer les fondations sur lesquelles seront construites toute votre connaissance en analyse.

1 Définitions et exemples

Définition V.25: Suite réelle

Une *suite réelle* est une application de $\mathbb{N}$ dans $\mathbb{R}$. On note souvent la suite $(U_n)_{n\in\mathbb{N}}$ comme une liste de valeurs indexées par $\mathbb{N}$.

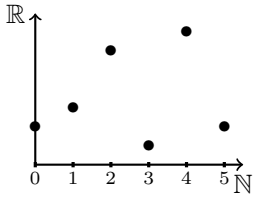
Voici deux exemples simples

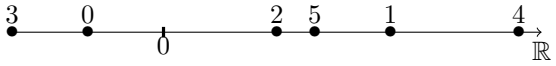
$$U_n = 3n + 7 \qquad V_n = (1 + \frac{1}{n})^n.$$

On peut se représenter une suite comme un tableau infini à deux lignes dont la première ligne est la suite des entiers :

0	1	2	3	4	5	...
e	π	-7	$\frac{1}{\pi}$	4	$\ln 2$	...

On peut aussi se représenter une suite comme un graphe, ou une famille de nombres réels numérotés sur la droite réelle :





Définition V.26: Monotonie

La suite $(U_n)_{n\in\mathbb{N}}$ est *croissante* si

$$\forall n \in \mathbb{N} \qquad U_{n+1} \geqslant U_n.$$

La suite $(U_n)_{n\in\mathbb{N}}$ est *décroissante* si

$$\forall n \in \mathbb{N} \qquad U_{n+1} \leqslant U_n.$$

On dit qu'une suite est *monotone* si elle est croissante ou décroissante.
La suite $(U_n)_{n\in\mathbb{N}}$ est *majorée* si

$$\exists M \in \mathbb{R} \qquad \forall n \in \mathbb{N} \qquad U_n \leqslant M.$$

La suite $(U_n)_{n\in\mathbb{N}}$ est *minorée* si

$$\exists m \in \mathbb{R} \qquad \forall n \in \mathbb{N} \qquad U_n \geqslant m.$$

La suite $(U_n)_{n\in\mathbb{N}}$ est *bornée* si

$$\exists M \in \mathbb{R} \qquad \forall n \in \mathbb{N} \qquad |U_n| \leqslant M.$$

Exercice 8. *(i) Illustrer par des exemples et contre-exemples chacune de ces définitions.*
(ii) Montrer que la suite $(U_n)_{n\in\mathbb{N}}$ est croissante si et seulement si

$$\forall m \geqslant n \qquad U_m \geqslant U_n.$$

(iii) Montrer qu'une suite $(U_n)_{n\in\mathbb{N}}$ est bornée si et seulement si elle est majorée et minorée.

On trouve aussi souvent des *suites définies par une relation de récurrence*. Le terme $n+1$ dépend alors du terme n (voire même d'autres termes précédents). Il faut alors donner une (ou plusieurs) valeur initiale. Voici deux exemples célèbres

$$\begin{cases} U_0 = 1 \\ U_{n+1} = \frac{1}{2}(U_n + \frac{2}{U_n}) \end{cases}$$

Soit N un entier naturel. On pose alors

$$\begin{cases} V_0 = N \\ V_{n+1} = \begin{cases} \frac{V_n}{2} & \text{si } V_n \text{ est pair} \\ 3V_n + 1 & \text{si } V_n \text{ est impair} \end{cases} \end{cases}$$

Remarques. (i) La suite U_n ci-dessus permet de calculer les décimales de $\sqrt{2}$. Elle peut s'obtenir par une méthode générale d'approximation des racines d'une équation appelée méthode de Newton.

(ii) La suite V_n est la suite de Syracuse. Elle est l'objet d'une conjecture complètement ouverte malgré un énoncé simple. Remarquons que si $N = 1$, alors la suite est

$$1, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$$

La conjecture dit que quelquesoit le premier terme la suite finira par boucler sur le motif ci-dessus. Plus formellement

$$\forall N \qquad \exists n_0 \quad V_{n_0} = 1.$$

1.1 Un exemple historique

A l'origine, les suites sont apparues comme des moyens d'approcher des nombres qui n'étaient pas accessibles par des calculs explicites. Il faut d'abord se souvenir que dans l'antiquité, les mathématiques étaient principalement utilisées pour mesurer, c'est-à-dire calculer des longueurs et des aires.
Par exemple, au premier siècle après JC, Héron d'Alexandrie se demanda comment calculer l'aire d'un triangle. La donnée la plus facile à mesurer est sans doute les longueurs a, b et c de ses côtés. Il trouva que la surface S d'un tel triangle était donnée par la formule

$$S = \sqrt{p(p-a)(p-b)(p-c)},$$

où $p = \frac{a+b+c}{2}$ est le demi-périmètre.

Héron d'Alexandrie examina l'exemple où $a = 7$, $b = 8$ et $c = 9$. Il obtient alors $S = \sqrt{720}$. Devant une telle expression, notre réflexe est de se jeter sur notre calculatrice, mais il n'en avait pas ! ! Voici ce qu'il écrivit :
« Puisque alors les 720 n'ont pas le côté exprimable, nous prendrons le côté avec une très petite différence ainsi. Puisque le carré le plus voisin de 720 est 729 et il a 27 comme côté, divise les 720 par le 27 : il en résulte 26 et deux tiers. Ajoute les 27 : il en résulte 53 et deux tiers. De ceux-ci la moitié : il en résulte 26 2' 3'. Le côté approché de 720 sera donc 26 2' 3'. En effet 26 2' 3' par eux-mêmes : il en résulte 720 36', de sorte que la différence est une 36e part d'unité. Et si nous voulons que la différence se produise par une part plus petite que le 36', au lieu de 729, nous placerons les 720 et 36' maintenant trouvés et, en faisant les mêmes choses, nous trouverons la différence qui en résulte inférieure, de beaucoup, au 36' »
La première chose qui saute aux yeux est le langage utilisé. On voit que la notion de racine carré est évoquée de manière géométrique : « on ne peut pas trouver le côté du carré d'aire 720 ». Ensuite la représentation décimale des nombres est absentes. Mais ces remarques ne sont pas l'essentiel pour notre cours.
Il souligne le fait que $\sqrt{720}$ n'est pas un nombre rationnel et ressent donc le besoin de calculer des approximations rationnelles de ce nombre réel. Pour cela il remarque que $27^2 = 729$ est voisin de 720. Donc

$$\sqrt{720} \simeq 27.$$

Ainsi une première approximation d'un carré d'aire 720 est un rectangle de côté

$$27 \times 720/27.$$

Ensuite, pour obtenir un rectangle plus proche d'un carré il impose qu'un de ses côté b est la moyenne des deux côtés précédents et l'aire toujours 720. Il obtient un rectangle

$$\frac{27 + \frac{720}{27}}{2} \times \frac{2 * 720}{27 + \frac{720}{27}}.$$

Et

$$\sqrt{720} \simeq \frac{27 + \frac{720}{27}}{2} = \frac{161}{6} = 26,833333\ldots$$

Au fait, aujourd'hui notre calculatrice nous dit

$$\sqrt{720} = 26,832815729997476\ldots$$

Mais d'ailleurs, comment fait-elle ?
Il a donc drôlement gagné en précision par rapport à la première approximation de 27. Mais pourquoi s'arrêter en si bon chemin. On peut remplacer le dernier rectangle obtenu par

$$\frac{\frac{161}{6} + \frac{720*2}{161}}{2} \times \frac{2 * 720}{\frac{161}{6} + \frac{720*2}{161}}.$$

On obtient alors l'approximation :

$$\sqrt{720} \simeq \frac{51841}{1932} = 26,832815734989\ldots$$

Pas mal, n'est-ce pas ! Et de plus, comme le dit Héron d'Alexandrie, nous pourrions continuer...

Aujourd'hui, nous dirions que la suite de Héron est définie par

$$\begin{cases} U_0 = 27 \\ U_{n+1} = \frac{U_n + \frac{720}{U_n}}{2} \end{cases}$$

et converge vers $\sqrt{720}$.

Mais aujourd'hui, les choses sont-elles si différentes que dans l'antiquité. Et bien pas tant que ça. En effet, notre calculatrice, pour obtenir $\sqrt{720}$ utilise aussi une suite de nombres calculables grâce aux opérations de base et convergeant vers $\sqrt{720}$, peut-être même la suite de Héron ! !

Lorsque l'on applique cette méthode pour calculer $\sqrt{2}$, on obtient :

$$\begin{cases} U_0 = 1 \\ U_{n+1} = \frac{U_n + \frac{2}{U_n}}{2} \end{cases}$$

On a alors :

$$\begin{aligned} U_0 &= 1 \\ U_1 &= 1,5 \\ U_2 &= 1,4166\ldots \\ U_3 &= 1,4142156\ldots \\ U_4 &= 1,4142135623745\ldots \\ U_5 &= 1,41421356237309504880168 96\ldots \end{aligned}$$

Et notre calculatrice nous dit

$$\sqrt{2} = 1,414213562373095\ldots$$

C'est fou, non ?

1.2 Opérations

Etant donnés deux suites $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ et un scalaire λ, on peut former

- La somme $(U_n + V_n)_{n\in\mathbb{N}}$ dont le terme n est $U_n + V_n$;
- Le produit $(U_n.V_n)_{n\in\mathbb{N}}$ dont le terme n est $U_n.V_n$;
- La multiplication par le scalaire λ : $(\lambda U_n)_{n\in\mathbb{N}}$ dont le terme n est λU_n.

Souvent on s'intéresse aux propriétés asymptotiques des suites, c'est-à-dire valables pour les grandes valeurs de n. Un vocable très utilisé pour cela est « à partir d'un certain rang ». Ainsi, une suite $(U_n)_{n\in\mathbb{N}}$ a une propriété P à partir d'un certain rang si et seulement si

$$\exists N \in \mathbb{N} \qquad \text{t.q. la suite } (U_{N+n})_{n\in\mathbb{N}} \text{ a la proprit } P.$$

1.3 Des suites classiques

Soit $r \in \mathbb{R}$. Une *suite arithmétique de progression r* est une suite $(u_n)_{n\in\mathbb{N}}$ vérifiant

$$\forall n \in \mathbb{N} \qquad u_{n+1} = u_n + r.$$

Son terme général est donné par

$$\forall n \in \mathbb{N} \qquad u_n = u_0 + nr.$$

La somme des premiers termes est donnée par

$$\boxed{\sum_{k=0}^{n} u_k = (n+1)u_0 + r\frac{n(n+1)}{2}.}$$

Soit $q \in \mathbb{R}^*$. Une *suite géométrique de raison q* est une suite $(u_n)_{n\in\mathbb{N}}$ vérifiant

$$\forall n \in \mathbb{N} \qquad u_{n+1} = qu_n.$$

Son terme général est donné par

$$\forall n \in \mathbb{N} \qquad u_n = u_0 q^n.$$

La somme des premiers termes est donnée par

$$\boxed{\sum_{k=0}^{n} u_k = \begin{cases} u_0 \frac{q^{n+1}-1}{q-1} \text{ si } q \neq 1 \\ u_0(n+1) \text{ si } q = 1. \end{cases}}$$

On mélange maintenant ces deux types de suites. Soit $r \in \mathbb{R}$ et $q \in \mathbb{R}^*$. Une *suite arithmético-géométrique* est une suite $(u_n)_{n\in\mathbb{N}}$ vérifiant

$$\forall n \in \mathbb{N} \qquad u_{n+1} = qu_n + r.$$

On suppose $q \neq 1$, sinon on a une suite arithmétique. On pose alors

$$a = \frac{r}{1-q}.$$

Son terme général est donné par

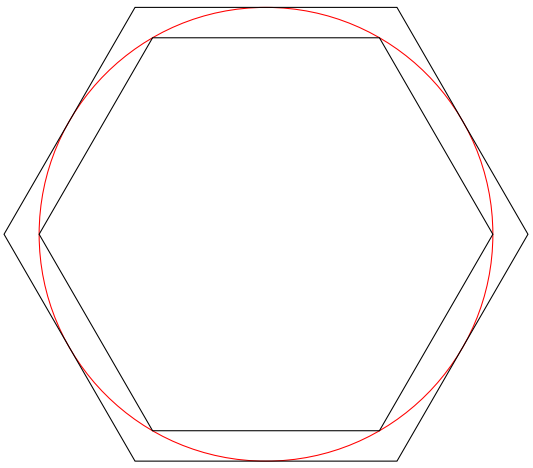
$$\boxed{\forall n \in \mathbb{N} \qquad u_n = (u_0 - a)q^n + a.}$$

La somme des premiers termes est donnée par

$$\boxed{\sum_{k=0}^{n} u_k = (u_0 - a)\frac{q^{n+1}-1}{q-1} + (n+1)a.}$$

1.4 Un exemple géométrique : π

Nous présentons ici la méthode d'Archimède d'approximation de π. Il s'agit d'interpréter π comme le demi-périmètre du cercle unité et d'approcher celui-ci avec des polygones ayant de plus en plus de côtés. Ce qui fait fonctionner la méthode, et introduit des suites est que la périmètre d'un polygône obtenu à une étape donnée est une fonction simple (enfin pas très compliquée) d'un périmètre du polygône d'avant.
Précisons les choses. Soit $\mathcal{C}$ le cercle de centre O et de rayon 1. Fixons un entier $N \geqslant 3$. Soit $\mathcal{P}$ un polygone régulier à N côtés inscrit dans le cercle et $\mathcal{Q}$ un polygone régulier à N côtés circonscrit au cercle.
Pour $N = 6$, on obtient



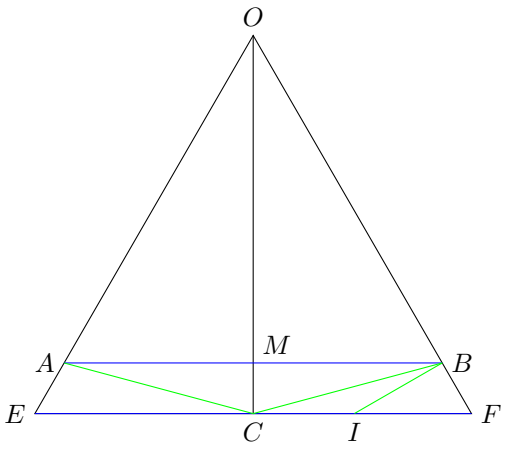
Soit a et b les longeurs des côtés de $\mathcal{P}$ et $\mathcal{Q}$ respectivement. On a l'encadrement

$$Na \leqslant 2\pi \leqslant Nb. \tag{1.1}$$

L'idée est alors de doubler le nombre de côtés : considérons les polygones $\mathcal{P}'$ et $\mathcal{Q}'$ inscrits et circonscrits avec $2N$ côtés. Notons a et b les longeurs des côtés de $\mathcal{P}'$ et $\mathcal{Q}'$. L'idée est double. D'un côté

$$2Na' \leqslant 2\pi \leqslant 2Nb' \tag{1.2}$$

est un meilleur encadrement de 2π et de l'autre a' et b' s'expriment simplement en fonction de a et b.
Pour montrer cela considérons la figure suivante



où

(i) A, B et C sont des points du cercle ;

(ii) AB est un côté de p ;

(iii) CB est un côté de p' ;

(iv) EF est un côté de P ;

(v) M est l'intersection de (AB) et (OC) ;

(vi) I est un sommet de P'.

En bleu nous avons des côtés de $\mathcal{P}$ et $\mathcal{Q}$ et en vert des côtés et demi-côtés de $\mathcal{P}'$ et $\mathcal{Q}'$. Ainsi, on a

$$a = AB \qquad a' = CB \qquad b = EF \qquad b' = 2BI.$$

Nous allons à présent montrer des relations entre ces quantités. Comme $\mathcal{P}$ et $\mathcal{Q}$ ont le même nombre de côtés ils sont homothétiques donc

$$b.OM = a.$$

La droite (IB) est un côté de $\mathcal{Q}'$ donc tangente au cercle. Mais alors (IB) est orthogonale à (OB). Mais alors les triangles (OCF) et (CBF) ont deux ablges égaux : ils sont donc semblables. En particulier

$$\frac{IB}{IF} = \frac{OC}{OF}.$$

Or I est un sommet de $\mathcal{Q}'$ sur le côté inclus dans la droite (EF) et C est le milieu de ce côté. Donc $2CI = b'$. Enfin $IB = b'/2$, $IF = (b - b')/2$.
Par ailleurs, par le théorème de Thales, $\frac{OC}{OF} = \frac{OM}{OB} = OM$. On obtient donc

$$\frac{b'}{b - b'} = \frac{a}{b},$$

qui peut se réécrire

$$b' = \frac{ab}{a + b}. \tag{1.3}$$

Les sommets du triangle (ACB) sont trois sommets consécutifs de $\mathcal{P}'$. Les sommets du triangle (CIB) sont un sommet de $\mathcal{Q}'$ et les milieux des deux côtés adjacents. On en déduit que ceux sont deux triangles isocèles partageant un angle : ils sont semblables. Mais alors

$$\frac{a'}{a/2} = \frac{b'}{a'},$$

qui peut se réécrire

$$2(a')^2 = ab'. \tag{1.4}$$

En réitérant ce procédé, on obtient deux suites U_n (égale à $(Na)/2$) et $V_n = (Nb)/2$) telles ques

$$\begin{cases} V_{n+1} = & \frac{2U_nV_n}{U_n+V_n} \\ U_{n+1} = & \sqrt{U_nV_{n+1}} \end{cases}$$

On a alors

$$\forall n \in \mathbb{N} \qquad U_n \leqslant 2\pi \leqslant V_n$$

et la longueur de l'intervalle $V_n - U_n$ tend vers 0 quand n tend vers l'infini.

2 Convergence d'une suite

2.1 Définitions

Vient ici, la définition la plus importante de ce cours.

Définition V.27: Limite d'une suite

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle et l un nombre réel. On dit que *la suite* $(U_n)_{n\in\mathbb{N}}$ *tend vers* l si

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad (n \geqslant N \implies |U_n - l| \leqslant \varepsilon).$$

On note alors

$$U_n \xrightarrow[n\to\infty]{} l.$$

On dit aussi que *la limite de la suite* $(U_n)_{n\in\mathbb{N}}$ *vaut* l et on écrit

$$\lim_{n\to\infty} U_n = l.$$

Pour comprendre la définition, on remarquera que

(i) La condition $|U_n - l| < \varepsilon$ est équivalente à $l - \varepsilon < U_n < l + \varepsilon$ ou encore à $U_n \in]l - \varepsilon; l + \varepsilon[$ ou encore que l'écart entre U_n et l est inférieur à ε.

(ii) Le bout de phrase « $\forall n \in \mathbb{N} \quad (n \geqslant N \implies$ » signifie « à partir du rang N on a ».

(iii) Le bout de phrase « $\exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad (n \geqslant N \implies$ » signifie « à partir d'un certain rang N on a ».

(iv) Plus ε est petit, plus la condition $|U_n - l| < \varepsilon$ est contraignante pour U_n.

Ainsi, on peut traduire cette définition par la phrase : aussi petit que soit un intervalle fixé autour de l, les éléments de la suite U_n appartiennent à cet intervalle à partir d'un certain rang.

Exercice 9. *Montrer que la suite* $(\frac{1}{n+1})_{n\in\mathbb{N}}$ *tend vers* 0.

On traduit souvent intuitivement $(U_n)_{n\in\mathbb{N}}$ tend vers l par « U_n se rapproche de l lorsque n est grand ». S'il y a du vrai dans cette phrase, elle est trompeuse. En effet, on peut comprendre U_n est de plus en plus proche de l. Or cela est faux, comme le montre l'exemple suivant

Exercice 10. *Considérons la suite suivante*

$$U_n = \begin{cases} \frac{1}{n} \text{ si } n \textit{ est impair} \\ 0 \text{ si } n \textit{ est pair} \end{cases}$$

Montrer que U_n *tend vers* 0. *Expliquer en quoi* U_n *ne se rapproche pas de* 0, *lorsque* n *augmente.*

Ainsi, il vaut mieux dire « U_n est proche de l lorsque n est grand ». Comme, en math, nous n'avons pas d'ordres de grandeur (celles-ci dépendent du contexte d'application), on traduit « proche » par aussi proche que l'on veut. Ainsi, on arrive à la phrase suivante qui est très proche de la définition

U_n est aussi proche que l'on veut l pourvu que n soit grand.

Remarque. L'auteur de ce cours préfère l'expression « tend vers » à « la limite est égale » (idem pour les notations). En effet, l'expression *la limite de la suite* $(U_n)_{n\in\mathbb{N}}$ *vaut* l peut laisser croire que la limite de la suite $(U_n)_{n\in\mathbb{N}}$ est une quantité bien définie et qu'elle vaut l. Or il n'en est rien comme nous allons le voir.

Définition V.28: Divergence

S'il existe une limite $l \in \mathbb{R}$, on dit que la suite *converge*. Sinon, on dit qu'elle *diverge*.

ATTENTION. La limite n'existe pas toujours.

Exercice 11. *Considérons la suite* $U_n = (-1)^n$. *Montrer que cette suite diverge.*

Une manière de comprendre une assertion mathématique est de comprendre sa négation.

Exercice 12. *Traduire par une phrase mathématique, l'affirmation* U_n *ne tend pas vers* l.

2.2 Propriétés fondamentales des suites convergentes

Théorème V.29. Unicité de la limite

La limite d'une suite, si elle existe est unique.

Preuve

Soit U_n une suite qui tend vers l_1 et l_2. Montrons par l'absurde que $l_1 = l_2$. Supposons donc que $l_1 \neq l_2$. Posons

$$\varepsilon = \frac{|l_1 - l_2|}{3}.$$

Par définition de la convergence, il existe N_1 et N_2 dans $\mathbb{N}$ tels que

$$\forall n \geqslant N_1 \qquad |U_n - l_1| \leqslant \varepsilon$$

et

$$\forall n \geqslant N_2 \qquad |U_n - l_2| \leqslant \varepsilon.$$

Posons $N = \max(N_1, N_2)$. Alors

$$U_N \in [l_1 - \varepsilon; l_1 + \varepsilon] \cap [l_2 - \varepsilon; l_2 + \varepsilon].$$

Or, vu la valeur de ε, cette intersection est vide. Contradiction.

Théorème V.30

Toute suite convergente est bornée.

Preuve

Soit U_n une suite qui converge vers une limite l. Appliquons la définition de la limite avec $\varepsilon = 1$:

$$\exists N \in \mathbb{N} \qquad \forall n \geqslant N \qquad l - 1 \leqslant U_n \leqslant l + 1.$$

Considérons

$$M = \max\{U_0, U_1, \ldots, U_{N-1}, l+1\}$$

et

$$m = \min\{U_0, U_1, \ldots, U_{N-1}, l-1\}.$$

Ces réels sont bien définis car les ensembles sont finis. Soit $n \in \mathbb{N}$. Si $n < N$, alors $U_n \leqslant M$. Si $n \geqslant N$ alors $U_n \leqslant l+1 \leqslant M$. Ainsi dans tous les cas on a $U_n \leqslant M$. De même, on montre que $U_n \geqslant m$. Ainsi

$$\forall n \in \mathbb{N} \qquad m \leqslant U_n \leqslant M.$$

2.3 Opérations

Théorème V.31. Combinaison linéaire

Soit $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ deux suites réelles. Soit α et β deux nombres réels. On suppose que $(U_n)_{n\in\mathbb{N}}$ tend vers une limite l_1 et $(V_n)_{n\in\mathbb{N}}$ vers l_2.
Alors, la suite $(\alpha U_n + \beta V_n)_{n\in\mathbb{N}}$ tend vers $\alpha l_1 + \beta l_2$.

Preuve

Soit $\varepsilon > 0$. Posons

$$\varepsilon_1 = \frac{\varepsilon}{|\alpha| + |\beta|}.$$

Remarquons que si α et β sont nuls l'énoncé est trivial. Sinon ε_1 est bien défini et strictement positif. Par définition de la convergence, il existe N_1 et N_2 dans $\mathbb{N}$ tels que

$$\forall n \geqslant N_1 \qquad |U_n - l_1| \leqslant \varepsilon_1$$

et

$$\forall n \geqslant N_2 \qquad |V_n - l_2| \leqslant \varepsilon_1.$$

Posons $N = \max(N_1, N_2)$. Alors, pour tout $n \geqslant N$

$$\begin{array}{rcll} |\alpha U_n + \beta V_n - \alpha l_1 - \beta l_2| & = & |\alpha(U_n - l_1) + \beta(V_n - l_2)| & \\ & \leqslant & |\alpha(U_n - l_1)| + |\beta(V_n - l_2)| & \text{parI.T.} \\ & \leqslant & |\alpha|\,|U_n - l_1)| + |\beta|\,|(V_n - l_2)| & \\ & \leqslant & (|\alpha| + |\beta|)\varepsilon_1 & \\ & \leqslant & \varepsilon & \end{array}$$

Ainsi, $(\alpha U_n + \beta V_n)_{n\in\mathbb{N}}$ tend vers $\alpha l_1 + \beta l_2$.

Théorème V.32. Produit

Soit $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ deux suites réelles. On suppose que $(U_n)_{n\in\mathbb{N}}$ tend vers une limite l_1 et $(V_n)_{n\in\mathbb{N}}$ vers l_2.
Alors, la suite $(U_n.V_n)_{n\in\mathbb{N}}$ tend vers $l_1.l_2$.

Preuve

Soit $\varepsilon > 0$. La suite U_n est convergente, donc elle est bornée :

$$\exists M > 0 \quad \forall n \in \mathbb{N} \quad |U_n| \leqslant M. \tag{2.1}$$

Posons

$$\varepsilon_1 = \frac{\varepsilon}{M + |l_2|}.$$

Par définition de la convergence, il existe N_1 et N_2 dans $\mathbb{N}$ tels que

$$\forall n \geqslant N_1 \qquad |U_n - l_1| \leqslant \varepsilon_1 \tag{2.2}$$

et

$$\forall n \geqslant N_2 \qquad |V_n - l_2| \leqslant \varepsilon_1. \tag{2.3}$$

Posons $N = \max(N_1, N_2)$. Alors, pour tout $n \geqslant N$

$$\begin{array}{rcll} |U_nV_n - l_1l_2| & = & |U_n(V_n - l_2) + l_2(U_n - l_1)| & \\ & \leqslant & |U_n(V_n - l_2)| + |l_2(U_n - l_1)| & \text{par l'I.T.} \\ & \leqslant & |U_n|.|V_n - l_2| + |l_2|.|U_n - l_1| & \\ & \leqslant & |U_n|\varepsilon_1 + |l_2|\varepsilon_1 & \text{par (2.2) et (2.3)} \\ & & & \text{car } n \geqslant N_1 \text{ et } n \geqslant N_2 \\ & \leqslant & (M + |l_2|)\varepsilon_1 & \text{par (2.1)} \\ & \leqslant & \varepsilon & \end{array}$$

Ainsi, $(U_nV_n)_{n\in\mathbb{N}}$ tend vers l_1l_2.

Théorème V.33. Inverse

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle qui ne s'annule pas. On suppose que $(U_n)_{n\in\mathbb{N}}$ tend vers une limite **non nulle** l.
Alors, la suite $(\frac{1}{U_n})_{n\in\mathbb{N}}$ tend vers $\frac{1}{l}$.

Preuve

Commençons par écrire l'inégalité que nous finirons par utiliser

$$|\frac{1}{U_n} - \frac{1}{l}| = \frac{|U_n - l|}{|l|.|U_n|} \leqslant \frac{\varepsilon_1}{|l|.|U_n|} \tag{2.4}$$

En particulier, il nous faut majorer $\frac{1}{|U_n|}$! Commence maintenant la preuve formelle.
Comme U_n tend vers $l \neq 0$,

$$\exists N_1 \in \mathbb{N} \quad \forall n \geqslant N_1 \quad |U_n| \geqslant \frac{|l|}{2}.$$

Soit $\varepsilon > 0$. Posons

$$\varepsilon_1 = \frac{1}{2}\varepsilon|l|^2.$$

Par définition de la convergence, il existe N_2 dans $\mathbb{N}$ tel que

$$\forall n \geqslant N_2 \qquad |U_n - l_1| \leqslant \varepsilon_1. \tag{2.5}$$

Posons $N = \max(N_1, N_2)$. Alors, pour tout $n \geqslant N$

$$|\frac{1}{U_n} - \frac{1}{l}| = \frac{|U_n - l|}{|l|.|U_n|} \leqslant \frac{\varepsilon_1}{|l|.|U_n|} \leqslant \frac{2\varepsilon_1}{|l|^2} \leqslant \varepsilon.$$

Ainsi, la suite $(\frac{1}{U_n})_{n\in\mathbb{N}}$ tend vers $\frac{1}{l}$.

Remarque. En combinant les deux théorèmes précédents on obtient que $\frac{V_n}{U_n}$ tend vers $\frac{l_2}{l_1}$.

2.4 Suites et inégalités

On peut passer à la limite dans les inégalités **larges** :

Théorème V.34. Limite dans inégalités larges

Soit $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ deux suites réelles qui tendent respectivement vers des limites l_1 et l_2.
Si

$$\forall n \in \mathbb{N} \qquad U_n \leqslant V_n$$

alors $l_1 \leqslant l_2$.

Preuve

Montrons le résultat par l'absurde. Supposons donc que $l_1 > l_2$. Posons

$$\varepsilon = \frac{l_1 - l_2}{3} > 0.$$

Par définition de la convergence, il existe N_1 et N_2 dans $\mathbb{N}$ tels que

$$\forall n \geqslant N_1 \qquad U_n \geqslant l_1 - \varepsilon$$

et

$$\forall n \geqslant N_2 \qquad V_n \leqslant l_2 + \varepsilon.$$

Posons $N = \max(N_1, N_2)$. Alors

$$U_N \geqslant l_1 - \varepsilon = l_2 + 2\varepsilon > l_2 + \varepsilon \geqslant V_N.$$

En particulier $U_N > V_N$; ce qui constitue une contradiction.

Corollaire V.35

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle qui converge vers une limite l.
On a

(i) si M est un nombre réel tel que

$$\forall n \in \mathbb{N} \qquad U_n \leqslant M$$

alors $l \leqslant M$;

(ii) si m est un nombre réel tel que

$$\forall n \in \mathbb{N} \qquad U_n \geqslant m$$

alors $l \geqslant m$.

Preuve

Il suffit d'appliquer le théorème V.34 avec une suite constante.

Théorème V.36. Théorème des gendarmes

Soit $(U_n)_{n\in\mathbb{N}}$, $(V_n)_{n\in\mathbb{N}}$ et $(W_n)_{n\in\mathbb{N}}$ trois suites réelles telles que

$$\forall n \in \mathbb{N} \qquad U_n \leqslant W_n \leqslant V_n.$$

On suppose en outre que U_n et V_n tendent vers **la même** limite l.
Alors, la suite $(W_n)_{n\in\mathbb{N}}$ tend vers l.

Preuve

Soit $\varepsilon > 0$. Par définition de la convergence, il existe N_1 et N_2 dans $\mathbb{N}$ tels que

$$\forall n \geqslant N_1 \qquad U_n \in [l-\varepsilon; l+\varepsilon]$$

et

$$\forall n \geqslant N_2 \qquad V_n \in [l-\varepsilon; l+\varepsilon].$$

Posons $N = \max(N_1, N_2)$. Alors,

$$\forall n \geqslant N \qquad V_n \text{ et } U_n \text{ appartiennent à } [l-\varepsilon; l+\varepsilon].$$

Fixons $n \geqslant N$. Alors, l'intervalle $[U_n, V_n]$ est inclus dans $[l-\varepsilon; l+\varepsilon]$. Or W_n appartient à cet intervalle. Donc $W_n \in [l-\varepsilon; l+\varepsilon]$.

Remarque. Pour appliquer le théorème des gendarmes, il convient de vérifier les 3 hypothèses :

(i) encadrement ;
(ii) convergence des bornes ;
(iii) égalité des limites de ces bornes.

2.5 Suites monotones

Théorème V.37: Limites de suites monotones

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle.

(i) Si $(U_n)_{n\in\mathbb{N}}$ est croissante et majorée alors U_n converge.
(ii) Si $(U_n)_{n\in\mathbb{N}}$ est décroissante et minorée alors U_n converge.

Preuve

Soit $(U_n)_{n\in\mathbb{N}}$ une suite croissante et majorée. Posons

$$l := \sup\{U_n \,:\, n \in \mathbb{N}\}.$$

Puisque U_n est majorée cette borne supérieure est un nombre réel. Montrons que $(U_n)_{n\in\mathbb{N}}$ tend vers l.
Soit $\varepsilon > 0$. Par définition du sup, $l-\varepsilon$ n'est pas majorant de la suite U_n. Donc il existe $N \in \mathbb{N}$ tel que $U_N > l-\varepsilon$. Puisque la suite est croissante on a

$$\forall n \geqslant N \qquad U_n \geqslant U_N > l-\varepsilon$$

Or l est un majorant, donc

$$\forall n \geqslant N \qquad l \geqslant U_n.$$

Ainsi,

$$\forall n \geqslant N \qquad l+\varepsilon > l \geqslant U_n > l-\varepsilon$$

et U_n tend vers l.

Pour la seconde assertion, considérons suite $(V_n)_{n\in\mathbb{N}}$ définie par $V_n = -U_n$. On vérifie aisément que V_n est croissante et majorée. D'après la première assertion, il existe $l \in \mathbb{R}$ tel que $V_n \xrightarrow[n\to\infty]{} l$. En appliquant le théorème V.31, on obtient : $U_n \xrightarrow[n\to\infty]{} -l$.

Exercice 13. *Soit $(U_n)_{n\in\mathbb{N}}$ une suite croissante et majorée. Notons l sa limite. Montrer que pour tout $N \in \mathbb{N}$,*

$$l := \sup\{U_n \,:\, n \in \mathbb{N} \text{ t.q. } n \geqslant N\}.$$

2.6 Suites adjacentes

Le théorème suivant est un moyen de montrer la convergence de suites.

Théorème V.38. Suites adjacentes

Soit $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ deux suites réelles telles que

(i) U_n est croissante ;

(ii) V_n est décroissante ;

(iii) $V_n - U_n$ tend vers 0.

Alors, les suites $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ convergent vers la même limite l. De plus, pour tout m et n dans $\mathbb{N}$, on a $U_m \leqslant l \leqslant V_n$.

Preuve

Posons $W_n = V_n - U_n$, pour tout $n \in \mathbb{N}$. On étudie la monotonie de W_n. Pour tout n, on a

$$W_{n+1} - W_n = V_{n+1} - U_{n+1} - V_n + U_n = (V_{n+1} - V_n) - (U_{n+1} - U_n) \leqslant 0.$$

La dernière inégalité utilise les monotonies des suites U_n et V_n. Donc $(W_n)_{n\in\mathbb{N}}$ est décroissante. Comme W_n tend vers 0, on en déduit que W_n est positive :

$$\forall n \in \mathbb{N} \qquad W_n \geqslant 0.$$

Ainsi

$$\forall n \in \mathbb{N} \qquad V_0 \geqslant V_n \geqslant U_n \geqslant U_0.$$

En particulier, les suites $(U_n)_{n\in\mathbb{N}}$ et $(V_n)_{n\in\mathbb{N}}$ sont bornées. Comme elles sont monotones, la proposition V.37 montre que ces suites convergent vers des limites finies l_1 et l_2.
Par le théorème V.31, la suite $(V_n - U_n)_{n\in\mathbb{N}}$ tend vers $l_2 - l_1$. Or elle tend vers 0. Donc, par unicité de la limite (théorème V.29), on a $l_2 - l_1 = 0$ et $l_1 = l_2$.

Voici un premier exemple de suites adjacentes.

Exemple 6. Soit x un nombre réel. On pose, pour tout $n \in \mathbb{N}$

$$U_n = \frac{E(x10^n)}{10^n} \qquad V_n = \frac{E(x10^n)+1}{10^n}.$$

On peut montrer que les deux suites sont adjacentes. Ainsi, elles convergent vers la même limite qui se trouve être x.
On peut remarquer que les deux suites sont constituées de nombres rationnels : cette construction peut être utilisée pour définir le produit et la somme de deux nombres réels...

3 Suites extraites

3.1 Définition

La définition formelle de suite extraite est ainsi.

Définition V.39: Suite extraite

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle. Une *suite extraite* de $(U_n)_{n\in\mathbb{N}}$ est une suite $(V_n)_{n\in\mathbb{N}}$ où $V_n = U_{\varphi(n)}$ pour une fonction $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante.

Les éléments de la suite V_n sont certains éléments de la suite U_n. Le fait que φ soit strictement croissante dit que l'on garde dans V_n les éléments de U_n dans l'ordre où ils étaient et sans répétition.
Si U_n est représentée par un tableau infini, une suite extraite s'obtient en deux étapes

(i) On efface certaines colonnes tout en veillant à ce qu'il en reste une infinité.

(ii) On renumérote la première ligne pour obtenir la liste des entiers naturels.

Proposition V.40

Une suite extraite d'une suite croissante, décroissante, majorée ou minorée l'est.

Preuve

Ceci est évident.

Exercice 14. *Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle. Soit φ et ψ deux applications strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$. Soit $(V_n)_{n\in\mathbb{N}}$ la suite extraite de $(U_n)_{n\in\mathbb{N}}$ associée à φ. Soit $(W_n)_{n\in\mathbb{N}}$ la suite extraite de $(V_n)_{n\in\mathbb{N}}$ associée à ψ.*
Montrer que $(W_n)_{n\in\mathbb{N}}$ est la suite extraite de $(U_n)_{n\in\mathbb{N}}$ associée à $\varphi \circ \psi$.

Remarque. Une suite extraite d'une suite extraite est une suite extraite.

3.2 Suites extraites complémentaires

Deux exemples courants de suites extraites soit les suites des termes pairs et impairs :

$$U_{2n} \qquad U_{2n+1}.$$

Ces deux suites extraites recouvrent toutes les valeurs de la suite. Cette remarque permet d'obtenir le résultat suivant.

Proposition V.41

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle. Alors, se valent :

(i) la suite $(U_n)_{n\in\mathbb{N}}$ converge ;

(ii) les deux suites extraites $(U_{2n})_{n\in\mathbb{N}}$ et $(U_{2n+1})_{n\in\mathbb{N}}$ convergent vers **la même limite**.

Preuve

La démonstration est laissée en exercice.

3.3 Suites extraites monotones

Théorème V.42. Ramsey

De toute suite de nombres réels, on peut extraire une suite monotone.

Preuve

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle. Considérons l'ensemble suivant :

$$E := \{n \in \mathbb{N} : \forall m > n \quad U_m \geqslant U_n\}.$$

Deux situations se présentent :

Cas 1 : l'ensemble E est fini.
En particulier, l'ensemble E est borné. Donc

$$\exists N \in \mathbb{N} \quad \forall n \geqslant N \quad n \notin E,$$

c'est-à-dire

$$\exists N \in \mathbb{N} \quad \forall n \geqslant N \quad \exists m > n \quad U_m < U_n \tag{3.1}$$

On construit alors, une suite n_k par récurrence telle que
- $n_{k+1} > n_k$ pour tout k ;
- $U_{n_{k+1}} < U_{n_k}$ pour tout k.

Posons $n_0 = N$. Soit $k \in \mathbb{N}$. Supposons $N = n_0 < \cdots < n_k$ construits. Comme $n_k \geqslant N$, il existe $m > n_k$ tel que $U_m < U_{n_k}$. Il suffit de poser $n_{k+1} = m$.

Cas 2 : l'ensemble E est infini.
Dans ce cas, on note n_k le $(k+1)^{ieme}$ élément de E, pour tout $k \in \mathbb{N}$. En particulier, on a :
- $n_k \in E$, pour tout k dans $\mathbb{N}$;
- $n_{k+1} > n_k$, pour tout k dans $\mathbb{N}$.

On montre alors que la suite extraite $(U_{n_k})_{k\in\mathbb{N}}$ est croissante : Soit $k \in \mathbb{N}$. Comme $n_k \in E$ et $n_{k+1} > n_k$, on a

$$U_{n_{k+1}} \geqslant U_{n_k}.$$

3.4 Le cas des suites bornées

Théorème V.43. Bolzano-Weierstrass

Toute suite bornée admet une suite extraite convergente.

Preuve

Soit $(U_n)_{n\in\mathbb{N}}$ une suite réelle. D'après le théorème V.42, il existe $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que la suite $(U_{\varphi(n)})_{n\in\mathbb{N}}$ est monotone.
Or la suite $(U_n)_{n\in\mathbb{N}}$ étant bornée, la suite $(U_{\varphi(n)})_{n\in\mathbb{N}}$ l'est aussi. Mais alors, la proposition V.37 montre que $(U_n)_{n\in\mathbb{N}}$ converge.

Ce théorème est important comme nous le verrons dans le chapitre consacré aux fonctions continues. La preuve présentée ici a le mérite d'être courte et l'inconvénient de sembler un peu miraculeuse. Une autre preuve, par dicotomie est possible. Cette dernière est assez difficile à écrire formellement mais se comprend bien...

Exemple 7. Regardons notre suite bornée, non convergent préférée : $U_n = (-1)^n$. Alors la suite extraite des nombres pairs tend vers 1 et celle des nombres impairs tend vers -1. On a construit deux suites extraites convergentes.

4 Limites infinies

4.1 Définition

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On dit que u_n tend vers $+\infty$, si u_n est aussi grand que l'on veut pourvu que n soit grand. Plus formellement :

Définition V.44: Limites infinies

La suite $(u_n)_{n\in\mathbb{N}}$ *tend vers plus l'infini* si

$$\forall M \in \mathbb{R} \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \quad u_n \geqslant M.$$

On note alors

$$u_n \xrightarrow[n\to\infty]{} +\infty.$$

La suite $(u_n)_{n\in\mathbb{N}}$ *tend vers moins l'infini* si $-u_n$ tend vers $+\infty$. On note alors

$$u_n \xrightarrow[n\to\infty]{} -\infty.$$

4.2 Suites monotones, comparaisons

Théorème V.45. Convergence des suites monotones

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle **croissante**. On a l'alternative suivante :

(i) soit $(u_n)_{n\in\mathbb{N}}$ converge ;

(ii) soit $(u_n)_{n\in\mathbb{N}}$ tend vers $+\infty$.

Preuve

La suite est majorée ou pas. Si elle est majorée, la proposition V.37 montre qu'elle converge. Supposons que u_n n'est pas majorée et montrons qu'elle tend vers $+\infty$. Soit $M \in \mathbb{R}$. Comme la suite n'est pas majorée par M, il existe N tel que $U_N > M$. Mais alors, pour tout $n \geqslant N$, $U_n \geqslant U_N > M$. Donc la suite tend vers $+\infty$.

Exercice 15. *(i) Construire une suite non majorée qui ne tend pas vers $+\infty$.*

(ii) Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle non majorée. Montrer qu'elle admet une suite extraite qui tend vers $+\infty$.

Théorème V.46. Comparaison

Soit $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles telles que

$$\forall n \in \mathbb{N} \quad u_n \geqslant v_n.$$

Si $(v_n)_{n\in\mathbb{N}}$ tend vers $+\infty$ il en va de même de la suite $(u_n)_{n\in\mathbb{N}}$.

Preuve

Soit $M \in \mathbb{R}$. Comme v_n tend vers $+\infty$, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N \qquad v_n \geqslant M.$$

Mais alors,

$$\forall n \geqslant N \qquad u_n \geqslant v_n \geqslant M.$$

Donc la suite u_n tend vers $+\infty$.

4.3 Opérations

On résume sans démonstration le comportement des limites infinies par le tableau ci-dessous. Ici, l_1 et l_2 sont des nombres réel (finis).

$\lim u_n$	$\lim v_n$	$\lim u_n + v_n$	$\lim u_n v_n$	$\lim \frac{u_n}{v_n}$	$\lim \frac{v_n}{u_n}$
l_1	$+\infty$	$+\infty$	$+\infty$ si $l_1 > 0$ $-\infty$ si $l_1 < 0$ FI si $l_1 = 0$	0	$+\infty$ si $l_1 > 0$ $-\infty$ si $l_1 < 0$ FI si $l_1 = 0$
$+\infty$	$+\infty$	$+\infty$	$+\infty$	FI	FI
$-\infty$	$+\infty$	FI	$-\infty$	FI	FI

Ici FI signifie forme indéterminée.

5 Suites de Cauchy

Le critère de Cauchy est un critère équivalent à la convergence de la suite. La beauté de la chose et qu'il ne mentionne pas de limite. De manière relâchée, une suite de Cauchy est une suite dont les termes sont aussi proches que l'on veut les uns des autres, pourvu que leurs indices soient grands. De manière plus formelle :

Définition V.47: Suite de Cauchy

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. La suite est dite *de Cauchy* si

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall p, q \geqslant N \quad |u_p - u_q| \leqslant \varepsilon.$$

Le théorème fondamental (on dit que $\mathbb{R}$ est *complet*) est :

Théorème V.48. Cauchy et convergence

Les conditions suivantes sont équivalentes :

(i) la suite $(u_n)_{n\in\mathbb{N}}$ converge ;

(ii) la suite $(u_n)_{n\in\mathbb{N}}$ est de Cauchy.

Preuve

Supposons que la suite converge disons vers l. Montrons qu'elle est de Cauchy. Soit $\varepsilon > 0$. Puisque $(u_n)_{n\in\mathbb{N}}$ converge, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N \qquad |u_n - l| \leqslant \frac{\varepsilon}{2}.$$

Soit p et q supérieurs à N. Alors

$$|u_p - u_q| = |u_p - l - (u_q - l)| \leqslant |u_p - l| + |u_q - l| \leqslant 2\frac{\varepsilon}{2} = \varepsilon.$$

Donc la suite est de Cauchy.

Supposons réciproquement que la suite est de Cauchy et montrons qu'elle converge. La difficulté est de construire la limite. La démonstration se décompose en 4 étapes.
Etape 1 : Montrons que la suite est bornée.
Pour cela on écrit la définition d'être de Cauchy pour $\varepsilon = 1$ et $q = N$. On obtient : Pour tout $p \geqslant N$, $|u_p - u_N| \leqslant 1$. Donc $u_p \in [u_N - 1; u_N + 1]$. Par ailleurs, l'ensemble fini, $u_0, \ldots, u_{N-1}$ est borné car fini. Donc la suite est bornée.

Etape 2 : Bolzano-Weierstrass
Grâce à l'étape 1, on appliquer le théorème de Bolzano-Weierstrass (théorème V.43) : il existe une suite extraite $u_{\varphi(n)}$ convergente vers l.

Etape 3 : $\varphi(m) \geqslant m$ pour tout m.
La restriction de φ est injective de $\{0, \ldots, m\}$ dans $\{\varphi(0), \varphi(1), \ldots, \varphi(m)\}$ par stricte monotonie. L'étape 3 en découle.

Etape 4 : Convergence de la suite vers l.
Soit $\varepsilon > 0$. Puisque $(u_{\varphi(n)})_{n\in\mathbb{N}}$ converge, il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1 \qquad |u_{\varphi(n)} - l| \leqslant \frac{\varepsilon}{2}.$$

Par ailleurs, la suite est de Cauchy. Donc, il existe $N_2 \in \mathbb{N}$ tel que

$$\forall p, q \geqslant N_2 \quad |u_p - u_q| \leqslant \frac{\varepsilon}{2}.$$

Soit $n \geqslant N_2$. Soit $m \geqslant \max(N_1, N_2)$. Alors,

$$|u_n - l| \leqslant |u_n - u_{\varphi(m)}| + |u_{\varphi(m)} - l| \leqslant 2\frac{\varepsilon}{2}.$$

Donc u_n converge vers l.

Chapitre 6

A propos de l'exponentielle

Sommaire

1 Rappel

Le but de ce chapitre est de démontrer le théorème suivant que nous avions admis.

Théorème VI.49. Définition Exponentielle

Il existe une unique fonction dérivable $f : \mathbb{R} \longrightarrow \mathbb{R}$ telle que

$$\begin{cases} f'(x) = f(x) & \forall x \in \mathbb{R} \\ f(0) = 1 \end{cases}$$

Cette fonction est notée $\exp : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \exp(x)$.

Cette démonstration permettra d'illustrer l'utilisation des suites et de leurs propriétés.
Pour $x \in \mathbb{R}$, considérons la suite

$$U_n(x) = (1 + \frac{x}{n})^n.$$

On va montrer que la suite $U_n(x)$ converge et que $f(x) = \lim_{n\to\infty} U_n(x)$ convient.

2 Suites adjacentes

Pour $n \neq x$, on pose

$$V_n(x) = (1 + \frac{-x}{n})^{-n},$$

pour $n > |x|$.

Proposition VI.50

Les suites $U_n(x)$ et $V_n(x)$ sont adjacentes.

Preuve

Nous utiliserons l'inégalité suivante

$$(1+y)^n \geqslant 1 + ny \qquad \forall n \in \mathbb{N} \quad \forall y > -1. \tag{2.1}$$

Celle-ci peut se démontrer par récurrence sur n.
Pour $n > |x|$, on montre que

$$\begin{array}{ll} (i) & \frac{U_{n+1}(x)}{U_n(x)} \geqslant 0 \\ (ii) & V_n(x) = \frac{1}{U_n(-x)} \\ (iii) & 1 - \frac{x^2}{n} \leqslant \frac{U_n(x)}{V_n(x)} \leqslant 1. \end{array}$$

******** TO DO ****

Grâce à la proposition VI.50, on peut poser, pour tout $x \in \mathbb{R}$,

$$f(x) = \lim_{n\to\infty} (1 + \frac{x}{n})^n.$$

*** Mq Ca marche ****

3 Le cas complexe

Dans le cas complexe, on peut aussi définir

$$\exp(z) = \lim_{n\to\infty} (1 + \frac{z}{n})^n.$$

Cela dit le preuve de la convergence est plus délicate.

Chapitre 7

Nombres complexes

Sommaire

1 Définition des nombres complexes, addition et multiplication

1.1 Définition

On introduit un nouveau nombre, noté i et on impose

$$\boxed{i^2 = -1}$$

Définition VII.51: Nombres complexes

Un *nombre complexe* est une écriture de la forme

$$a + ib$$

avec a et b dans $\mathbb{R}$. On note $\mathbb{C}$ l'ensemble des nombres complexes.

Des exemples sont $0 + 2i = 2i$, $\sqrt{2} - i\sqrt{3}$, $\pi + i\ln(2)$...Traditionellement, on note $z = a + ib$ un nombre complexe plutôt que x.
Une première chose à comprendre est que cette écriture est formelle dans le sens où

$$\forall a, b, c, d \in \mathbb{R} \qquad a + ib = c + id \iff a = c \text{ et } b = d.$$

Ainsi, l'application

$$\begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ \begin{pmatrix} a \\ b \end{pmatrix} & \longmapsto & a + ib \end{array}$$

est une bijection.
On définit ensuite l'addition (pour tout $a, b, c, d \in \mathbb{R}$)

$$\boxed{(a + ib) + (c + id) = (a + c) + i(b + d),}$$

comme l'addition des vecteurs dans $\mathbb{R}^2$.
Enfin, on définit la multiplication en utilisant la distributivité et la règle $i^2 = -1$:

$$\boxed{(a + ib).(c + id) = (ac - bd) + i(bc + ad).}$$

Les règles de calcul pour ces opérations $+$ et $\times$ sont semblables à celles sur les nombres réels (on dit que $\mathbb{R}$ et $\mathbb{C}$ sont des corps). On plonge $\mathbb{R}$ dans $\mathbb{C}$ par $a \mapsto a + i0$.

Théorème VII.52. Règles de calcul dans $\mathbb{C}$

Les deux lois $+$ et $\times$ sur $\mathbb{C}$ vérifient :

(i) $+$ et $\times$ prolongent les lois usuelles sur $\mathbb{R}$.
(ii) $\forall z_1, z_2 \in \mathbb{C} \qquad z_1 + z_2 = z_2 + z_1$
(iii) $\forall z_1, z_2, z_3 \in \mathbb{C} \qquad (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$
(iv) $\forall z_1 \in \mathbb{C} \qquad z_1 + 0 = z_1$
(v) $\forall z_1 \in \mathbb{C} \quad \exists! z_2 \in \mathbb{C} \qquad z_1 + z_2 = 0$; on pose $-z_1 := z_2$
(vi) $\forall z_1, z_2 \in \mathbb{C} \qquad z_1.z_2 = z_2.z_1$
(vii) $\forall z_1, z_2, z_3 \in \mathbb{C} \qquad (z_1.z_2).z_3 = z_1.(z_2.z_3)$
(viii) $\forall z_1 \in \mathbb{C} \qquad z_1.1 = z_1$
(ix) $\forall z_1 \in \mathbb{C} - \{0\} \quad \exists! z_2 \in \mathbb{C} \qquad z_1.z_2 = 1$; on pose ${z_1}^{-1} := z_2$

(x) $\forall z_1, z_2, z_3 \in \mathbb{C} \qquad z_3.(z_1 + z_2) = z_3.z_1 + z_3.z_2$

Le théorème VII.52 est facile à établir mais fastidieux. Il existe des preuves sans calcul mais plus sophistiquées à l'aide de matrices ou d'algèbre des polynômes...
On revient tout de même sur une assertion : l'existence d'un inverse. Soit $z = a + ib$ non nul. Alors

$$\boxed{z^{-1} = \frac{a-ib}{a^2+b^2}.}$$

Exemple 8. Calculer $(1 + i\sqrt{3})^{-1}$.

L'ensemble des nombres réels se plonge dans celui des nombres complexes par :

$$\begin{array}{rccc} \iota : & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & a & \longmapsto & a + i0 \end{array}$$

Cette application respecte la somme et le produit :

$$\iota(a + b) = \iota(a) + \iota(b) \qquad \iota(a.b) = \iota(a).\iota(b)$$

pour tout $a, b \in \mathbb{R}$.

1.2 Conjugaison, parties réelles et imaginaires

On définit la conjugaison par

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z = a + ib & \longmapsto & \bar{z} = a - ib \end{array} \qquad \text{pour } a \text{ et } b \text{ dans } \mathbb{R}$$

On définit les parties réelles et imaginaires par

$$\begin{array}{rccc} \mathrm{Re} : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z = a + ib & \longmapsto & a = \frac{z+\bar{z}}{2} \end{array} \qquad \begin{array}{rccc} \mathrm{Im} : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z = a + ib & \longmapsto & b = \frac{z-\bar{z}}{2i} \end{array}$$

Les propriétés importantes de la conjugaison sont :

Théorème VII.53: Calculs dans $\mathbb{C}$

Soit z, z_1 et z_2 des nombres complexes. On a :

(i) $\bar{\bar{z}} = z$;
(ii) $z = \bar{z}$ si et seulement si z est réel (cad appartient à l'image de ι) ;
(iii) $z = -\bar{z}$ si et seulement si $z \in i\mathbb{R}$ (on dit que z est *imaginaire pur*) ;
(iv) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
(v) $\overline{z_1.z_2} = \bar{z}_1.\bar{z}_2$;
(vi) $\overline{\frac{1}{z}} = \frac{1}{\bar{z}}$.

Preuve

Laissée en exercice.

1.3 Module

Le module d'un nombre complexe $z = a + ib$ avec a et b dans $\mathbb{R}$ est défini par

$$\boxed{|z| = \sqrt{a^2 + b^2} = \sqrt{z\bar{z}} \in \mathbb{R}^+}$$

On a :

Théorème VII.54: Propriétés du module

Soit z, z_1 et z_2 des nombres complexes. On a :

(i) si $z \in \mathbb{R}$, $|z|$ est la valeur absolue de z.

(ii) si $z \neq 0$, alors $|\frac{1}{z}| = \frac{1}{|z|}$.

(iii) $|z_1 z_2| = |z_1|.|z_2|$.

Preuve

Laissée en exercice.

Plus délicat est le comportement du module relativement à la somme.

Théorème VII.55: Inégalité triangulaire

Soit z_1 et z_2 des nombres complexes. On a :

$$|z_1 + z_2| \leqslant |z_1| + |z_2|.$$

De plus, on a égalité si et seulement si il existe $\tau \in \mathbb{R}^+$ tel que $z_1 = \tau z_2$ ou $z_2 = \tau z_1$.

Preuve

Commençons par montrer l'inégalité. On a :

$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2)(\bar{z}_1 + \bar{z}_2) \\ &= z_1\bar{z}_1 + z_2\bar{z}_2 + z_1\bar{z}_2 + \bar{z}_1 z_2 \\ &= |z_1|^2 + |z_2|^2 + z_1\bar{z}_2 + \overline{z_1\bar{z}_2} \\ &= |z_1|^2 + |z_2|^2 + 2\mathrm{Re}(z_1\bar{z}_2). \end{aligned}$$

Or

$$\mathrm{Re}(z_1\bar{z}_2) \leqslant |z_1\bar{z}_2| = |z_1 z_2|. \tag{1.1}$$

Donc

$$|z_1 + z_2|^2 \leqslant |z_1|^2 + |z_2|^2 + 2|z_1 z_2| = (|z_1| + |z_2|)^2$$

Comme $\sqrt{\ }$ est croissante et $|z_1 + z_2|$ et $|z_1| + |z_2|$ appartiennent à $\mathbb{R}^+$, on en déduit que

$$|z_1 + z_2| \leqslant |z_1| + |z_2|.$$

La preuve précédente implique que $|z_1 + z_2| = |z_1| + |z_2|$ si et seulement si $\mathrm{Re}(z_1\bar{z}_2) = |z_1\bar{z}_2|$; ce qui est encore équivalent à $z_1\bar{z}_2 \in \mathbb{R}^+$.
Deux cas se présentent. Si z_2 est nul, d'une part on a l'égalité et d'autre part $z_1\bar{z}_2 \in \mathbb{R}^+$ et il existe $\tau \in \mathbb{R}^+$ tel que $z_2 = \tau z_1$.

Supposons maintenant z_2 non nul. Posons $t = z_1\bar{z}_2 \in \mathbb{R}^+$. Alors

$$z_1 = \frac{t}{\bar{z}_2} = \frac{t}{z_2\bar{z}_2}z_2 = \frac{t}{|z_2|^2}z_2 \in \mathbb{R}^+ z_1.$$

Réciproquement, si $z_1 \in \mathbb{R}^+ z_2$ alors $z_1\bar{z}_2 \in \mathbb{R}^+$.

1.4 Calculs avec les nombres complexes

Comme nous l'avons vu les nombres complexes, leur addition et leur multiplication partagent beaucoup des propriétés de ces opérations sur les nombres réels. En conséquence, beaucoup des formules sur les nombres réels sont aussi valables pour les complexes (avec des preuves identiques). Par exemple

$$(z_1 + z_2)^n = \sum_{k=0}^{n} \binom{n}{k} z_1^k z_2^{n-k},$$

ou

$$1 + z + \cdots + z^n = \frac{z^{n+1} - 1}{z - 1} \quad \text{si } z \neq 1.$$

2 Nombres complexes et plan euclidien

Nous travaillons dans le plan muni d'un repère orthonormé $(O, \overrightarrow{e}_1, \overrightarrow{e}_2)$. Ainsi tout élément (a, b) de $\mathbb{R}^2$ correspond à un point $M(a, b)$ et au vecteur $a\overrightarrow{e}_1 + b\overrightarrow{e}_2$.
En identifiant $\mathbb{R}^2$ à $\mathbb{C}$, on obtient une identification $z \mapsto M(z)$ entre $\mathbb{C}$ et le plan. Le nombre complexe z est appelé *l'affixe* du point $M(z)$ et le point $M(z)$ est appelé le *point d'affixe* z.
Fort de cette identification, on peut interpréter géométriquement certains calculs dans $\mathbb{C}$. Pour tout z, z_1 et z_2 dans $\mathbb{C}$, on a :

(i) $\overrightarrow{OM(z_1 + z_2)} = \overrightarrow{OM(z_1)} + \overrightarrow{OM(z_2)}$.

(ii) $\|\overrightarrow{OM(z)}\| = |z|$.

(iii) $(\mathrm{Re}(z), Im(z))$ sont les coordonnées de $M(z)$ dans le repère $(O, \overrightarrow{e}_1, \overrightarrow{e}_2)$.

(iv) Le point $M(\bar{z})$ est l'image du point $M(z)$ par la symétrie orthogonale par rapport à l'axe des abscisses.

(v) Le point $M(iz)$ est l'image du point $M(z)$ par rotation d'angle $\pi/2$ et de centre O.

(vi) L'inégalité $|z_1 - z_2| \leqslant |z_1| + |z_2|$ s'interprète comme l'inégalité triangulaire dans le triangle $OM(z_1)M(z_2)$.

3 Exponentielle complexe

3.1 Définition et premières propriétés

Pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}$ on pose

$$z_n = (1 + \frac{z}{n})^n.$$

On admettra que la suite $(z_n)_{n\in\mathbb{N}}$ converge vers une limite que l'on netera $\exp(z)$ ou e^z. Par définition, dire que la suite z_n converge signifie que $\mathrm{Re}(z_n)$ et $\mathrm{Im}(z_n)$ convergent. Pour information, on peut montrer cela en utilisant le critère de Cauchy, théorème V.48. On obtient ainsi, la fonction exponentielle complexe

$$\begin{array}{rccc} \exp : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \exp(z). \end{array}$$

Remarque. Dans la pluspart des ouvrages, le rôle de la suite z_n est joué par la suite $s_n = \sum_{k=0}^{n} \frac{z^n}{n!}$.
On admettra aussi le théorème suivant

Théorème VII.56. Exponentielle complexe

(i) Pour tout z et z' dans $\mathbb{C}$, on a

$$\exp(z+z') = \exp(z)\exp(z').$$

(ii) La restriction de l'exponentielle complexe à $\mathbb{R}$ est l'exponentielle réelle.

(iii) L'image de la fonction exp est $\mathbb{C}^*$.

(iv) Pour tout z dans $\mathbb{C}$,

$$\exp(\bar{z}) = \overline{\exp(z)}.$$

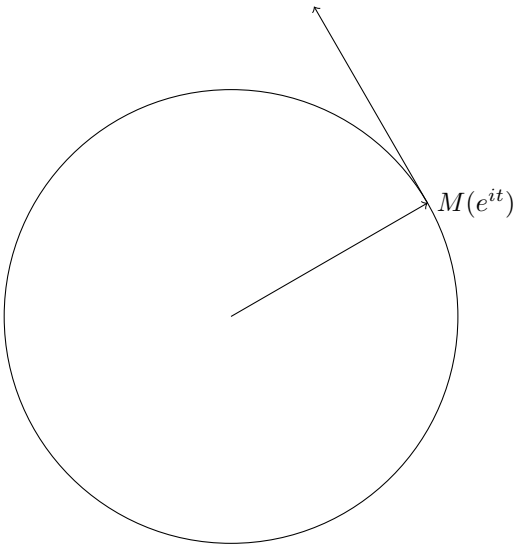
(v) Pour tout z dans $\mathbb{C}$,

$$|\exp(z)| = 1 \iff z \in i\mathbb{R}.$$

On admettra que

$$\forall t \in \mathbb{R} \qquad \frac{e^{i(t+h)} - e^{it}}{h} \xrightarrow[h\to 0]{} ie^{it}.$$

On interprète ce calcul de manière cinétique



$M(e^{it})$ est la position. Son vecteur unitaire tangent est son image par la rotation d'angle $\frac{\pi}{2}$ c'est-à-dire ie^{it}.

Proposition VII.57

L'application $\mathbb{R} \longrightarrow \mathbb{C}$, $t \longmapsto e^{it}$ est un paramétrage 2π-périodique à vitesse constante égale à 1 du cercle unité.

Ainsi, lorsque t parcourt $\mathbb{R}$, e^{it} parcours le cercle unité à vitesse 1. Pour tout $t \in \mathbb{R}$, on pose

$$\boxed{\sin(t) := \mathrm{Im}(e^{it}) = \frac{e^{it} - e^{-it}}{2i} \qquad \cos(t) := \mathrm{Re}(e^{it}) = \frac{e^{it} + e^{-it}}{2}.}$$

Donc

$$\boxed{e^{it} = \cos(t) + i\sin(t).}$$

On peut maintenant montrer les formules à l'aide du théorème VII.56 :

$$\sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b) \qquad \cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b).$$

De même, on obtient la formule de Moivre

$$\boxed{(\cos(t) + i\sin(t))^n = \cos(nt) + i\sin(nt),}$$

pour tout entier n et nombre réel t.

3.2 Décomposition polaire

Théorème VII.58: Décomposition polaire

Tout nombre complexe non nul z s'écrit de manière unique sous la forme

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

avec $\rho \in \mathbb{R}^{+*}$ et $\varphi \in [0; 2\pi[$.

Preuve

Notons $\mathcal{C}(O,1)$ le cercle de centre O et de rayon 1. Toute demi-droite d'origine 0 rencontre le cercle $\mathcal{C}(O,1)$ en un unique point. Par ailleurs,

$$\varphi \in [0; 2\pi[\longrightarrow \mathcal{C}(0,1),\ t \longmapsto e^{it}$$

est une bijection.

Remarque. Il convient de remarquer que $\rho = |z|$. De plus, φ est l'angle **en radian** formé par $\overrightarrow{OM(z)}$ et l'axe des abscisses.

Il convient de connaitre, ou retrouver facilement, les exemples simples suivants :

$e^{i0} = 1$	$e^{i\pi} = -1$
$e^{i\frac{\pi}{2}} = i$	$e^{-i\frac{\pi}{2}} = -i$
$e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$	$\sqrt{2}e^{i\frac{\pi}{4}} = 1 + i$

En particulier, on a la superbe identité d'Euler :

$$\boxed{e^{i\pi} + 1 = 0}$$

L'esthétique de cette formule tient au fait qu'elle melle les constantes les plus fondamentales des math $0, 1, e, i$ et π et les opération de base $+, \times$ et puissance.

Changements de coordonnées.
Supposons $z = \rho e^{i\theta}$ donné. Les coordonnées cartésiennes de $z = a + ib$ (avec a et b dans $\mathbb{R}$) sont données par

$$\boxed{a = \rho\cos(\theta) \qquad b = \rho\sin(\theta)}$$

Réciproquement supposons que $z = a + ib$ avec a et b dans $\mathbb{R}$. Pour obtenir l'écriture polaire $z = \rho e^{i\theta}$ on fait

$$\boxed{\rho = \sqrt{a^2 + b^2}.}$$

L'obtention de θ est plus délicate. Si $a \neq 0$, on constate que $\tan(\theta) = \frac{b}{a}$. Regardons alors

$$\alpha = \arctan(\frac{b}{a}) \in]-\frac{\pi}{2}; \frac{\pi}{2}[.$$

Comme $\tan(\alpha) = \tan(\theta)$, on sait qu'il existe $k \in \mathbb{Z}$ tel que $\theta = \alpha + k\pi$. Comme $\theta \in [0; 2\pi[$, on en déduit que θ vaut α, $\alpha + \pi$ ou $\alpha + 2\pi$. Pour décider entre ces 4 cas on regarde dans quel cadran se trouve z :

$\theta = \alpha + \pi$	$\theta = \alpha$
$\theta = \alpha + \pi$	$\theta = \alpha + 2\pi$

Si $a = 0$, alors

$$\theta = \begin{cases} \frac{\pi}{2} & \text{si } b > 0 \\ \frac{3\pi}{2} & \text{si } b < 0 \end{cases}$$

Application. En utilisant la décomposition polaire on peut résoudre l'équation $z^n = 1$:

Théorème VII.59: Racines de l'unité

Pour $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$, on a $z^n = 1$ si et seulement s'il existe $k \in \{0, \ldots, n-1\}$ tel que

$$z = e^{\frac{2ik\pi}{n}}.$$

3.3 Racines carrés

Théorème VII.60: Racine carrée

Soit z un nombre complexe fixé. On s'intéresse à l'équation

$$\omega^2 = z \tag{3.1}$$

d'inconnue ω.

(i) Si $z = 0$, l'équation (3.1) a une unique solution $\omega = 0$.

(ii) Si $z \neq 0$, l'équation (3.1) a exactement deux solutions opposées $\omega = \pm\omega_0$.

Preuve

L'expression polaire de ω_0 est bien plus facile que son expression cartésienne. Si $z = \rho e^{i\varphi}$, alors $\omega_0 = \rho e^{i\frac{\varphi}{2}}$.

Corollaire VII.61

Toute équation polynomiale de degré 2,

$$az^2 + bz + c = 0$$

avec $a \neq 0, b$ et c dans $\mathbb{C}$ admet une ou deux solutions.

Preuve

Posons $\Delta = b^2 - 4ac$. Soit $\delta \in \mathbb{C}$ tel que $\delta^2 = \Delta$. Posons

$$z_\pm = \frac{\pm\delta - b}{2a},$$

et développons

$$\begin{aligned} a(z - z_1)(z - z_2) &= az^2 - az(z_- + z_+) + az_-z_+ \\ &= az^2 + bz + c. \end{aligned}$$

Le résultat en découle.

Remarque. Dans le cas où les coefficients de l'équation de degré 2 sont réels, les couples de solution ne peuvent pas être quelconque. En effet, dans ce cas Δ est réel et

(i) Si $\Delta > 0$, l'équation a deux solutions réelles.

(ii) Si $\Delta = 0$, l'équation a une solution réelle.

(iii) Si $\Delta < 0$, l'équation a deux solutions complexes conjuguées $\{z_0, \bar{z}_0\}$.

Cela est une conséquence facile du fait que si Δ est un réel strictement négatif alors δ est imaginaire pur.

4 Transformations du plan

Plusieurs transformations du plan ont des formules analytiques simples en utilisant les nombres complexes. Par exemple, on a déjà vu que la réflection orthogonale d'axe $(O, \overrightarrow{e_1})$ est l'application

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \bar{z} \end{array}$$

4.1 Homothéties

Soit $\lambda \in \mathbb{R}$. L'homothétie de centre O et de rapport λ s'écrit

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \lambda z. \end{array}$$

Corollaire VII.62

Soit $z_0 \in \mathbb{C}^*$ et $\lambda \in \mathbb{R}^*$. Alors,

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \lambda(z - z_0) + z_0. \end{array}$$

est l'homothétie de centre z_0 et de rapport λ.

4.2 Translation

Théorème VII.63: Translation

Soit $\overrightarrow{v}$ un vecteur de $\mathbb{R}^2$ et z_1 son affixe. Alors l'application

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & z + z_1 \end{array}$$

est la translation de vecteur $\overrightarrow{v}$.

Preuve

C'est une conséquence directe de la formule $\overrightarrow{OM(z_1+z_2)} = \overrightarrow{OM(z_1)} + \overrightarrow{OM(z_2)}$.

4.3 Rotations de centre O

Théorème VII.64: Rotation

Soit θ un nombre réel. Alors l'application

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & e^{i\theta}z \end{array}$$

est la rotation de centre O et d'angle θ.

Preuve

C'est une conséquence directe de la formule $e^{i\theta}\rho e^{i\varphi} = \rho e^{i(\theta+\varphi)}$.

Exercice 16. *Soit $z_0 \in \mathbb{C}$ et $\theta \in \mathbb{R}$. Soit $z \in \mathbb{C}$. Montrer que l'image de $M(z)$ par la rotation d'angle θ et de centre $M(z_0)$ vaut*

$$e^{i\theta}(z - z_0) + z_0.$$

4.4 Retour sur la suite $(1 + z/n)^n$

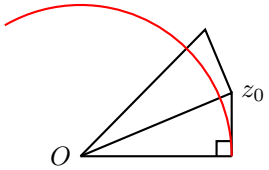
Dans cette section, nous allons interpréter géométriquement la suite $(1+\frac{z}{n})^n$, lorsque $z = it$ avec $t \in \mathbb{R}$. Fixons n tel que $|t/n| < 1$. Ecrivons $z_0 := 1 + \frac{t}{n} = \rho e^{i\theta}$. Regardons la transformation

$$\begin{array}{rccc} \varphi : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & z_0 z = e^{i\theta}\rho z. \end{array}$$

L'application φ est la composé d'une homothétie de rapport ρ et d'une rotation d'angle θ et de centre O.
Regardons le triangle $(OM(1)M(z_0))$. C'est un triangle rectangle. Son image par φ est un triangle rectangle T tel que

(i) O est un sommet de T ;
(ii) z_0 est un sommet de T et T est rectangle en z_0 ;
(iii) l'hypoténuse de T est de longueur ρ^2.

On obtient :



De même on obtient une suite de triangles semblables (pour $\theta = \frac{2\pi}{3}$ et $n = 10$ et 20) :

On peut à présent interpréter géométriquement la formule :

$$(1+\frac{it}{n})^n \longrightarrow_{n\to\infty} e^{it}.$$

5 Théorème fondamental de l'algèbre

Théorème VII.65. d'Alembert-Gauss

Soit P un polynôme non constant à coefficients complexes :

$$P(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_0,$$

avec $a_0, \ldots, a_d$ dans $\mathbb{C}$ et $a_d \neq 0$.
Alors, il existe z_0 dans $\mathbb{C}$ tel que $P(z_0) = 0$.

Les anglo-saxons appelle ce théorème « the Fundamental theorem of algebra » soulignant ainsi son importance. Nous n'en verrons pas de démonstration dans ce cours.

Chapitre 8

Limites et continuité

Sommaire

1 Intervalles de $\mathbb{R}$

Un intervalle I de $\mathbb{R}$ est une partie de $\mathbb{R}$ de la forme $[a;b]$, $]a;b[$, $[a;b[$ ou $]a;b]$, avec $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{\infty\}$. Les quantités a et b sont appelées les bornes de l'intervalle. On dit que I est *d'interieur non vide* si $a \neq b$. *L'interieur* de l'intervalle I est $]a;b[$.

2 Limites

2.1 Définitions et Opérations

Définition VIII.66: Limite continue

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle de $\mathbb{R}$. Soit a dans I, ou une borne de I. Soit $l \in \mathbb{R} \cup \{\pm\infty\}$.
On dit que f *tend vers* l *en* a si pour toute suite u_n d'éléments de I qui tend vers a, la suite $f(u_n)$ tend vers l.
On note alors $\lim_{x\to a} f(x) = l$ ou $f(x) \xrightarrow[x\to a]{} l$.

Les théorèmes sur les suites et les opérations s'appliquent directement.

Théorème VIII.67. Limites et opérations

Soient f et g deux fonctions d'un intervalle I dans $\mathbb{R}$. Soit a dans I ou une borne de I. Soit λ et μ dans $\mathbb{R}$.

(i) Si f tend vers l_1 en a et g tend vers l_2 en a alors $\lambda f + \mu g$ tend vers $\lambda l_1 + \mu l_2$ en a.
(ii) Si f tend vers l_1 en a et g tend vers l_2 en a alors fg tend vers $l_1 l_2$ en a.
(iii) Si f tend vers l_1 en a et g tend vers $l_2 \neq 0$ en a alors $\frac{f}{g}$ tend vers $\frac{l_1}{l_2}$ en a.
(iv) Supposons que f tend vers l_1 en a et g tend vers l_2 en a. Si pour tout $x \in I$, $f(x) \leqslant g(x)$ alors $l_1 \leqslant l_2$.

De même le théorème des gendarmes donne :

Théorème VIII.68. Gendarmes

Soient f, g et h trois fonctions d'un intervalle I dans $\mathbb{R}$. Soit a dans I ou une borne de I. On suppose que

$$\forall x \in I \qquad f(x) \leqslant h(x) \leqslant g(x).$$

Si f et g tendent vers la même limite l en a alors h tend vers l en a.

2.2 Composée

Une nouveauté par rapport aux suites : la composé de fonctions.

Théorème VIII.69. Composée de Limites

Soient I et J deux intervalles de $\mathbb{R}$. Soient $f : I \longrightarrow J$ et $g : J \longrightarrow \mathbb{R}$ deux fonctions. Soit $a \in I$. On suppose que

(i) f tend vers y en a ;

(ii) $y \in J$ ou est une borne de J ;

(iii) g tend vers l en y.

Alors, $g \circ f$ tend vers l en a.

Preuve

Soit u_n une suite qui tend vers a. Alors $f(u_n)$ tend vers y car f tend vers y en a. Mais alors, $g(f(u_n)) = (g \circ f)(u_n)$ tend vers l car g tend vers l en y. Ainsi, $g \circ f$ tend vers l en a.

2.3 Cas des limites à gauche et à droite

Nous traitons ici d'un exemple. Soit $I = [a; b]$ un intervalle et $f : I \longrightarrow \mathbb{R}$ une fonction. Soit c dans l'intérieur de I et $l \in \mathbb{R}$. On dit que f tend vers l à droite de c si $f_{|[c,b]}$ tend vers l en c.
Remarquons que dans la définition de limite en un point, on ne regarde que des suites dont les éléments appartiennent à l'intervalle de définition de f. Ainsi, lorsque l'on dit que f tend vers l à droite de c, on ne considère que le comportement des suites d'éléments supérieurs à c.

Théorème VIII.70. Limite de fonctions monotones

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle de $\mathbb{R}$. Soit a dans I ou une borne de I.
Si f est monotone alors f admet des limites finies ou pas à gauche et à droite de a.

2.4 Avec des epsilons

Nous avons défini la convergence des suites à l'aide de quantificateurs et d'ε. On peut faire de même pour les fonctions. Considérons ici le cas de limite fini en un point de $\mathbb{R}$.

Théorème VIII.71. Limite et ε

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle de $\mathbb{R}$. Soit a dans I, ou une borne réelle de I. Soit $l \in \mathbb{R}$.
Alors f tend vers l en a si et seulement si

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - a| \leqslant \delta \implies |f(x) - l| \leqslant \varepsilon. \tag{2.1}$$

Ce théorème dit que f tend vers l en a signifie que $f(x)$ est aussi proche que l'on veut de l pourvu que x soit proche de a.

Preuve

Supposons que la condition (2.1) est satisfaite. Montrons que f tend vers l en a. Soit u_n une suite d'éléments de I telle que u_n tend vers a. Montrons que $f(u_n)$ tend vers l.
Soit $\varepsilon > 0$. Fixons $\delta > 0$ tel que

$$\forall x \in I \quad |x - a| \leqslant \delta \implies |f(x) - l| \leqslant \varepsilon.$$

Comme u_n tend vers a, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N \quad |u_n - a| \leqslant \delta.$$

Mais alors,

$$\forall n \geqslant N \quad |f(u_n) - l| \leqslant \varepsilon.$$

Donc $f(u_n)$ tend vers l. CQFD.

Réciproquement, supposons que f tend vers l en a. Montrons que la condition (2.1) est satisfaite. Pour cela on raisonne par l'absurde en supposant que la condition (2.1) n'est pas satisfaite.

$$\exists \varepsilon > 0 \quad \forall \delta > 0 \quad \exists x \in I \quad |x - a| \leqslant \delta \text{ et } |f(x) - l| > \varepsilon. \tag{2.2}$$

Fixons un ε satisfaisant la condition (2.2). Alors, pour $\delta = \frac{1}{n}$, il existe $x_n \in I$ tel que

(i) $|x_n - a| \leqslant \frac{1}{n}$; et

(ii) $|f(x_n) - l| > \varepsilon$.

La suite x_n ainsi construite tend vers a d'après la première condition. Mais la seconde condition implique que $f(x_n)$ ne tend pas vers l. Contradiction.

On peut obtenir le même type de description pour des limites infinies ou finies en l'infini ou en un point de $\mathbb{R}$. A titre d'exemple, f tend vers $+\infty$ en $+\infty$ si et seulement si

$$\forall M > 0 \quad \exists B > 0 \quad \forall x \in I \quad x \geqslant B \implies f(x) \geqslant M.$$

3 Continuité

Définition VIII.72: Continuité

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle de $\mathbb{R}$. Soit a dans I.
On dit que f *est continue en* a si f tend vers $f(a)$ en a.

Remarque. Puisque $a \in I$, la limite de $f(x)$ ne peut être que $f(a)$. Ainsi, f est continue en a si et seulement si $f(x)$ a une limite lorsque x tend vers a.

Définition VIII.73: Continuité sur Intervalle

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle de $\mathbb{R}$. La fonction f est dite *continue sur* I si elle est continue en tout point de I.

Les théorèmes VIII.67, VIII.69 impliquent facilement le résultat suivant.

Théorème VIII.74. Opérations sur les fonctions continues

La somme, les combinaisons linéaires, le produit, le quotient, la composé de fonctions continues sont continus.

Le théorème VIII.74 permet de démontrer des continuités si on en connait. Mise à part la partie entière, toutes les fonctions usuelles vues dans le chapitre du même titre sont continues sur leur intervale de définition.

Exemple 9. Le théorème VIII.74 permet par exemple de démontrer que $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \sqrt{|\sin(x^2 + 4x)|}\exp(2x - 3)$ est continue sachant que $|\ |$, $\sqrt{\ }$, sin et $x \mapsto x$, $x \mapsto 1$ et exp le sont toutes.

Voyons maintenant un exemple de fonction non continue.

Exemple 10. La fonction partie entière $\mathbb{R} \longrightarrow \mathbb{Z}$, $x \longmapsto E(x)$ est continue en $a \in \mathbb{R}$ si et seulement si $a \notin \mathbb{Z}$.

4 Théorème des valeurs intermédiaires

Le théorème suivant est la principale propriété des fonctions continues. Il dit que le graphe d'une fonction continue ne peut passer de dessous à dessus une droite sans la couper.

Théorème VIII.75. TVI

Soit $f : I \longrightarrow \mathbb{R}$ une fonction continue définie sur un intervalle I. Soit $a < b$ dans I. Soit $y \in \mathbb{R}$ tel que

$$f(a) \leqslant y \leqslant f(b)$$

ou

$$f(b) \leqslant y \leqslant f(a).$$

Alors, il existe $c \in [a, b]$ tel que $f(c) = y$.

Avant d'écrire la démonstration, nous remarquons que l'énoncé est faux sur les nombres rationnels. En effet, la fonction $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, $x \longmapsto x^2$ est continue, vaut 0 en 0, 4 en 2. Pour autant il n'existe pas de nombre rationnel $x \in [0; 2]$ tel que $f(x) = 2$.
Cette remarque nous montre en particulier qu'il faut utiliser dans la démonstration une propriété de $\mathbb{R}$ qui n'est pas satisfaite par $\mathbb{Q}$: cette propriété sera la propriété de la borne supérieure.

Preuve

On suppose que $f(a) \leqslant y \leqslant f(b)$. On peut toujours se ramener à ce cas quitte à considérer $-f$. Considérons l'ensemble

$$E = \{x \in [a; b] \ : \ f(x) \leqslant y\}.$$

L'ensemble E est non vide car il contient a. Il est majoré car inclus dans $[a; b]$. Posons

$$c := \sup(E).$$

Alors $c \in [a; b]$. Il existe une suite $(U_n)_{n\in\mathbb{N}}$ d'éléments de E qui tend vers c. Comme f est continue en c, on en déduit que $f(U_n)$ tend vers $f(c)$. Or, $f(U_n) \leqslant y$ pour tout n. Donc, par passage à la limite dans l'inégalité, on obtient $f(c) \leqslant y$.

Si $c = b$, on a $f(c) = f(b) \geqslant y$. Donc $f(c) = y$. CQFD.

Supposons à présent que $c < b$. Il existe N tel que $(c+\frac{1}{n}) \in]c, b]$ pour tout $n \geqslant N$. Alors, $(c+\frac{1}{n}) \notin E$ car c est le sup ! En particulier, $f(c + \frac{1}{n}) > y$. En passant à la limite lorsque n tend vers l'infini dans cette inégalité, on obtient $f(c) \geqslant y$. Finalement, $f(c) = y$. CQFD.

Remarque. Il est important que la fonction soit définie sur un intervalle. En effet, la fonction $f : \mathbb{R}^* \longrightarrow \mathbb{R}$, $x \longmapsto \frac{1}{x}$ est continue, change de signe mais ne s'annule pas ! !

Corollaire VIII.76

L'image d'un intervalle par une fonction continue est un intervalle.

Preuve

Soit I un intervalle contenu dans l'ensemble de définition de f. Posons $a = \inf f(I)$ et $b = \sup f(I)$. Le théorème des valeurs intermédiaires permet de montrer aisément que $]a; b[\subset f(I) \subset [a; b]$. Le corollaire en découle.

5 Continuité, monotonie et injectivité

Théorème VIII.77

Soit f une fonction définie sur un intervalle. Si f est continue et injective alors f est strictement monotone.

Preuve

C'est une conséquence du théorème des valeurs intermédiaires. On laisse la démonstration en exercice.

Théorème VIII.78. Continuité de la réciproque

Soit f une fonction définie sur un intervalle I, continue et injective. On pose $J = f(I)$.
Alors, la fonction réciproque $f^{-1} : J \longrightarrow I$ est continue.

Preuve

D'après le théorème VIII.77, f est monotone. Quitte à remplacer f par $-f$, on suppose que f est strictement croissante. Notons g la fonction réciproque de f.
Montrons que g est strictement croissante. Soit $y_1 < y_2$ dans J. Soit x_1 et x_2 tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. Comme f est strictement croissante $x_1 < x_2$. Or $x_1 = g(y_1)$ et $x_2 = g(y_2)$. Donc g est strictement croissante.

Comme $g(J) = I$ est un intervalle, on peut conclure en appliquant le lemme VIII.79 ci-dessous.

Lemme VIII.79

Soit $f : I \longrightarrow \mathbb{R}$ une fonction monotone définie sur un intervalle I. Alors se valent :

(i) f est continue ;

(ii) l'image de f est un intervalle.

Preuve

Si f est continue, le corollaire VIII.76 montre que l'image de f est un intervalle.
Réciproquement, supposons que l'image de f est un intervalle. Quitte à remplacer f par $-f$, on suppose que f est croissante. Soit a un élément de I. Par le théorème VIII.70, les limites à gauche et à droite de f en a existent. Puisque l'image de I est un intervalle, ces deux limites sont nécessairement égales. On en déduit que f est continue.

6 Fonctions continues sur un intervalle fermé borné

Théorème VIII.80. Continue sur fermé borné

Soit $a < b$ dans $\mathbb{R}$ et $I = [a; b]$. Soit $f : I \longrightarrow \mathbb{R}$ une fonction continue.
Alors, f est bornée et atteint ses bornes.

Remarque. Attention, la forme de l'intervalle est importante ici. L'énoncé est en effet faux sur les intervalles $[a; b[$ ou $[a, +\infty[$ par exemple. Vous pourrez chercher des contre-exemples.

Preuve

Posons

$$M = \sup f([a; b]) \in \mathbb{R} \cup \{+\infty\}.$$

Il s'agit de montrer que M est fini et appartient à l'image de f.
Il existe une suite $(U_n)_{n\in\mathbb{N}} \in [a; b]^{\mathbb{N}}$ telle que $f(U_n)$ tend vers M. D'après le théorème de Bolzano-Weierstrass, il existe une suite extraite $U_{\varphi(n)}$ de U_n qui converge dans $[a; b]$. Notons x la limite de $U_{\varphi(n)}$. La suite $f(U_{\varphi(n)})$ tend vers M. Puisque f est continue en x, $f(U_{\varphi(n)})$ tend vers $f(x)$. Par unicité de la limite, $f(x) = M$. En particulier, M est fini et dans l'image de f.
On raisonne de même avec l'inf. On peut aussi remarquer que $\inf f([a; b]) = -\sup -f([a; b])$.

7 Prolongement par continuité

Proposition VIII.81

Soit $a \in \mathbb{R}$ et $b \in]a; +\infty[\cup \{+\infty\}$. Soit $f :]a; b[\longrightarrow \mathbb{R}$ une fonction. On suppose qu'il existe $l \in \mathbb{R}$ tel que

$$\lim_{x\to a^+} f(x) = l.$$

On définit la fonction

$$\begin{array}{rccl} g : & [a; b[& \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \begin{cases} f(x) & \text{si } x > a \\ l & \text{si } x = a \end{cases} \end{array}$$

Alors, la fonction g est continue en a.

La preuve est évidente. On dit que g est obtenue à partir de f par prolongement par continuité. Dans le même ordre d'idée, on a l'énoncé suivant.

Proposition VIII.82

Soit $f : I \longrightarrow \mathbb{R}$ une fonction et a un point dans l'intérieur de I. On suppose que

(i) la fonction $f_{|I\cap]-\infty;a[}$ tend vers $f(a)$ en a ;

(ii) la fonction $f_{|I\cap]a;+\infty[}$ tend vers $f(a)$ en a.

Alors f est continue en a.

Cette proposition est particulièrement utile lorsque f est définie par deux formules différentes à gauche et à droite de a. Par exemple, la fonction

$$\begin{array}{rccl} f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longrightarrow & \begin{cases} 0 & \text{si } x < a \\ x & \text{si } x \geqslant 0 \end{cases} \end{array}$$

est continue en 0 (et même sur $\mathbb{R}$).

Chapitre 9

Arithmétiques de $\mathbb{Z}$ et des polynômes

Sommaire

1 Nombres premiers et décomposition

L'arithmétique est l'étude des relations de divisibilité. Les entiers « indivisibles » ou premiers y jouent un rôle central.
Commençons par quelques définitions.

Définition IX.83: Multiple, Premier

(i) Soient a et b deux entiers dans $\mathbb{Z}$ avec $b \neq 0$. On dit que a est un *multiple* de b (ou que b est une *diviseur* a) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$.

(ii) Un entier naturel supérieur à 2, est dit *premier* si ses seuls diviseurs sont 1 et lui-même.

Les premiers nombres premiers sont

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47 \ldots$$

Un algorithme pour énumérer tous les nombres premiers inférieurs à un entier donné est le **crible d'Eratosthène**.
Le premier résultat fondamental est dû à Euclide :

Théorème IX.84. Euclide

Il existe une infinité de nombres premiers.

Preuve

Supposons qu'il existe k nombre premiers (avec k dans $\mathbb{N}^*$) et montrons qu'il en existe un autre.
Soit donc $p_1, \ldots, p_k$, k nombres premiers 2 à 2 distincts. Considérons l'entier

$$N = p_1 \ldots p_k + 1.$$

Soit p le plus petit diviseur de N supérieur ou égal à 2. D'après le lemme IX.85 ci-dessous, p est un nombre premier.
Remarquons que chaque p_i (pour $i \in \{1, \ldots, k\}$) divise $p_1 \ldots p_k$ et pas 1. Donc il ne divise pas N.
En particulier $p_i \neq p$.
Ainsi p est un nombre premier qui n'est pas dans la liste $p_1, \ldots, p_k$.

Lemme IX.85

Soit n un entier supérieur à deux. Soit p son plus petit diviseur supérieur à 2.
Alors p est un nombre premier.

Preuve

Si p n'était pas premier il aurait un diviseur d tel que $2 \leqslant d < p$. Alors d serait un diviseur de n supérieur à 2 et strictement inférieur à p. Ceci contredit la minimalité de p.

Le résultat le plus important de cette section permet de parler de décomposition en facteurs premiers.

Théorème IX.86. Décomposition en facteurs premiers

Soit n un entier naturel supérieur à deux. Il existe une unique écriture de n sous la forme

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s},$$

où

(i) les entiers p_i sont premiers ;
(ii) les exposant α_i sont des entiers naturels non nuls : $\alpha_i \geqslant 1$;
(iii) $p_1 < \dots < p_s$.

Nous démontrons maintenant l'existence et nous montrerons l'unicité plus tard.

Preuve

On prouve l'existence par récurrence forte.
Pour $n = 2$, l'énoncé est clair.
Fixons $n \geqslant 3$. Supposons l'existence connue pour tout entier $2 \leqslant m < n$. Soit p le plus petit diviseur de n supérieur à 2.
Alors, d'après le lemme IX.85, p est un nombre premier. D'après l'hypothèse de récurrence $\frac{n}{p}$ admet une décomposition. On en déduit que n admet une telle décomposition.

1.1 Division Euclidienne

Il s'agit de la division avec quotient et reste que l'on apprend à l'école primaire.

Théorème IX.87. Division Euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Alors il existe un unique couple d'entiers (q, r) tel que

(i) $a = bq + r$;
(ii) $0 \leqslant r < |b|$.

Preuve

Regardons l'ensemble

$$\mathcal{D} = \{mb \,:\, m \in \mathbb{Z}\}$$

des multiples de b. Soit $q \in \mathbb{Z}$ tel que bq soit le plus grand élément de $\mathcal{D} \cap]-\infty; a]$. Alors $bq + |b| \in \mathcal{D}$ et $bq + |b| \notin \mathcal{D} \cap]-\infty; a]$. Ainsi

$$bq \leqslant a < bq + |b|.$$

En posant $r = a - bq$, on obtient l'existence.

Montrons l'unicité. Soit (q_1, r_1) et (q_2, r_2) deux couples qui conviennent. On a alors

$$b(q_1 - q_2) = r_2 - r_1.$$

En particulier, b divise $|r_2 - r_1|$. Or, $r_1, r_2 \in [0, |b| - 1]$. Donc $0 \leqslant |r_2 - r_1| \leqslant |b| - 1$. On en déduit que $r_2 - r_1 = 0$ puis $r_2 = r_1$. Mais alors, puisque $bq_1 + r_1 = bq_2 + r_2$, on a $q_1 = q_2$.

1.2 PGCD

Définition IX.88

Soit a et b deux entiers, non tous les deux nuls. L'ensemble des diviseurs dans $\mathbb{N}^*$ communs à a et b contient 1 et est fini. Donc il a un plus grand élément noté $\text{pgcd}(a,b)$ et appelé *plus grand commun diviseur de a et b*.

Exemples 11. Soit a et b deux entiers non nuls.

(i) $\text{pgcd}(a,b) = \text{pgcd}(b,a)$;
(ii) $\text{pgcd}(a,0) = a$;
(iii) $\text{pgcd}(a,1) = 1$;
(iv) $\text{pgcd}(a,b) = \text{pgcd}(a,b-a)$;

Théorème IX.89. PGCD

Soit a et b deux entiers, non tous les deux nuls. Soit d un entier non nul. Alors, se valent

(i) d divise a et b ;
(ii) d divise $\text{pgcd}(a,b)$.

Par définition, tout diviseur commun de a et b est inférieur à $\text{pgcd}(a,b)$. Le théorème précédent montre plus : tout diviseur commun de a et b est un diviseur de $\text{pgcd}(a,b)$.

Preuve

Si d divise $\text{pgcd}(a,b)$ alors d divise a et b. On démontre la réciproque par récurrence sur $\max(a,b)$. Posons $D = \text{pgcd}(a,b)$. Si ce maximum vaut 1, on regarde $\text{pgcd}(1,1)$ ou $\text{pgcd}(1,0)$ et l'énoncé est évident. Réciproquement, supposons que d divise a et b.
Si $a = b$, alors $D = a$ et l'énoncé est évident. Supposons à présent $a \neq b$. Quitte à échanger a et b, supposons que $a < b$. On remarque que d divise a et $b-a$, or $D = \text{pgcd}(b-a,a)$. Comme $\max(b-a,a) < \max(a,b)$, on peut appliquer l'hypothèse de récurrence et on obtient d divise D.

Lorsque les entiers sont décomposés en produits de facteurs premiers, il est facile de calculer leur pgcd :

Théorème IX.90. PGCD et premiers

Soit a et b deux entiers naturels non nuls. Soit $p_1, \ldots, p_s$ des nombres premiers 2 à 2 distincts tels qu'il existe des entiers naturels $\alpha_1, \ldots, \alpha_s$ et $\beta_1, \ldots, \beta_s$ tels que

$$a = p_1^{\alpha_1} \ldots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} \ldots p_s^{\beta_s}.$$

Alors

$$\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \ldots p_s^{\min(\alpha_s,\beta_s)}.$$

Preuve

Nous prouverons ce résultat plus tard.

Algorithme d'Euclide. Cet algorithme très efficace permet de calculer le pgcd de deux entiers a et b. Le principe de l'algorithme est le suivant :

Quitte à échanger a et b on suppose que $a \geqslant b$.
Si $b = 0$, $\text{pgcd}(a, b) = a$.
Si $b \neq 0$ on fait la division euclidienne de a par b : $a = bq + r$
On écrit que $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Voici un exemple : calcul de $\text{pgcd}(1222, 449)$.

a	b	q	r
1222	449	2	324
449	324	1	125
324	125	2	74
125	74	1	51
74	51	1	23
51	23	2	5
23	5	4	3
5	3	1	2
3	2	1	1
2	1	2	0
1	0		

1.3 Entiers premiers entre eux

Définition IX.91: Premiers entre eux

On dit que a et b sont premiers entre eux, si $\text{pgcd}(a, b) = 1$.

Théorème IX.92. Bezout

Soit a et b deux entiers non nuls. Alors a et b sont premiers entre eux si et seulement si il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.

Preuve

S'il existe u et v comme dans l'énoncé, tout diviseur commun de a et b divise 1. Donc $\text{pgcd}(a, b) = 1$.
Supposons à présent que $\text{pgcd}(a, b) = 1$. On fait encore une preuve par récurrence sur $\max(a, b)$.
Le point clé, pour passer de (a, b) à $(b - a, a)$ est que :

$$au + (b - a)v = 1$$

équivaut à

$$a(u - v) + bv = 1.$$

Exercice 17. *Soit a et b deux entiers non nuls. Alors il existe u et v dans $\mathbb{Z}$ tels que $au+bv = \text{pgcd}(a, b)$.*

Preuve

Il suffit de diviser a et b par leur pgcd, puis d'appliquer Bezout.

Théorème IX.93. Gauss

Soit a, b et c trois entiers non nuls. On suppose que a et b sont premiers entre eux et que a divise bc. Alors a divise c.

Exercice 18. *Trouver 3 entiers tels que a divise bc mais a ne divise ni b ni c. Quel est le pgcd des entiers a et b que vous avez trouvés ?*

Preuve

D'après le théorème de Bezout IX.92, il existe u et v dans $\mathbb{Z}$ tels que

$$au + bv = 1.$$

Multiplions par c :

$$auc + bvc = c.$$

Alors a divise auc mais aussi bvc, donc a divise c.

Corollaire IX.94

Soit p un nombre premier et a et b deux entiers quelconques. Si p divise ab alors il divise a ou b.

Preuve

Supposons que p ne divise pas a. Alors le pgcd de a et p est un diviseur strict de p : c'est donc 1 puisque p est premier. Mais alors, le théorème de Gauss montre que p divise b.

On peut maintenant démonter l'unicité de la décomposition en produit de facteurs premiers.

Preuve de l'unicité du théorème IX.86

On fait une démonstration par récurrence forte. Pour $n = 2$, l'unicité est claire.
Fixons $n \in \mathbb{N}$, $n \geqslant 3$. Supposons l'unicité acquise pour tout $2 \leqslant k < n$. Soit

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s} \quad \text{et} \quad n = q_1^{\beta_1} \dots q_t^{\beta_t}$$

deux décompositions comme dans le théorème IX.86. Remarquons que q_1 divise n. Comme q_1 est premier, il divise l'un de p_i, d'après le corollaire IX.94. Comme p_i est premier et $q_1 \neq 1$, on obtient $q_1 = p_i$. Quitte à renuméroter les p_i, on peut supposer que $i = 1$. En divisant par q_1 on obtient

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = q_1^{\beta_1 - 1} \dots q_t^{\beta_t}$$

Comme $\frac{n}{p_1} < n$, on peut appliquer l'hypothèse de récurrence et déduire le résultat.

De même, on peut maintenant démonter le théorème IX.90.

Preuve du théorème IX.90

Il est facile de voir qu'il suffit de montrer le résultat suivant.

Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ et $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ deux entiers.
Alors n divise m si et seulement si pour tout i, $\alpha_i \leqslant \beta_i$.

Posons $\gamma_i = \min(\alpha_i, \beta_i)$ et

$$k = p_1^{\gamma_1} \dots p_s^{\gamma_s}.$$

En divisant n et m par k, il suffit de montrer que p divise $p_1^{\beta_1-\gamma_1} \dots p_s^{\beta_s-\gamma_s}$ si et seulement si p est un des p_i tels que $\beta_i - \gamma_i \neq 0$. Cela découle du corollaire IX.94.

1.4 PPCM

Cette notion est complémentaire de la notion de PGCD. Nous ne montrerons pas les résultats qui s'obtiennent de manière analogue au cas du PGCD.

Définition IX.95: PPCM

Soit a et b deux entiers, non tous les deux nuls. L'ensemble des multiples dans $\mathbb{N}^*$ communs à a et b contient ab et est infini. Il a un plus petit élément noté $\text{ppcm}(a, b)$ et appelé *plus petit commun multiple de a et b*.

Exemples 12. Soit a et b deux entiers non nuls.

(i) $\text{ppcm}(a, b) = \text{ppcm}(b, a)$;

(ii) $\text{ppcm}(a, 1) = a$.

Théorème IX.96. PPCM

Soit a et b deux entiers, non tous les deux nuls. Soit d un entier non nul. Alors, se valent

(i) d est un multiple de a et b ;

(ii) d est un multiple de $\text{ppcm}(a, b)$.

Par définition, tout multiple commun de a et b est supérieur à $\text{ppcm}(a, b)$. Le théorème précédent montre plus.
Lorsque les entiers sont décomposés en produits de facteurs premiers, il est facile de calculer leur ppcm :

Théorème IX.97. PPCM et premiers

Soit a et b deux entiers naturels non nuls. Soit $p_1, \dots, p_s$ des nombres premiers 2 à 2 distincts tels qu'il existe des entiers naturels $\alpha_1, \dots, \alpha_s$ et $\beta_1, \dots, \beta_s$ tels que

$$a = p_1^{\alpha_1} \dots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} \dots p_s^{\beta_s}.$$

Alors

$$\text{ppcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \dots p_s^{\max(\alpha_s,\beta_s)}.$$

Le corollaire suivant précise le fait que pgcd et ppcm sont des notions complémentaires.

Corollaire IX.98

Soit a et b deux entiers naturels non nuls. Alors

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

Avec ce résultat l'algorithme d'Euclide permet de calculer le ppcm de deux entiers.

1.5 Une équation diophantienne

Théorème IX.99: Points entiers sur une droite

Soit a, b et c des entiers relatifs. On s'intéresse, dans $\mathbb{Z}^2$ à l'équation

$$ax + by = c \tag{1.1}$$

(i) Cette équation a des solution $(x, y) \in \mathbb{Z}^2$ si et seulement si $\text{pgcd}(a, b)$ divise c.

(ii) Si le $\text{pgcd}(a, b)$ divise c alors il existe x_0, y_0, α et β dans $\mathbb{Z}$ tels que l'ensemble des solutions de l'équation (1.1) est

$$\{(x_0 + k\alpha, y_0 + k\beta) \ : \ k \in \mathbb{Z}\}.$$

Preuve

Supposons que le $\text{pgcd}(a, b)$ divise c. Disons $c = d \times \text{pgcd}(a, b)$, avec $d \in \mathbb{Z}$. D'après le théorème de Bezout, il existe u et v tels que $au + bv = \text{pgcd}(a, b)$. Alors $a(ud) + b(vd) = c$. Donc l'équation a une solution.

Supposons qu'il existe $(x, y) \in \mathbb{Z}^2$ vérifiant (1.1). Remarquons que $\text{pgcd}(a, b)$ divise ax et by. Il divise alors $c = ax + by$.

Supposons que le $\text{pgcd}(a, b)$ divise c. Ecrivons $a = a'\text{pgcd}(a, b)$, $b = b'\text{pgcd}(a, b)$ et $c = c'\text{pgcd}(a, b)$. L'équation (1.1) est équivalente à

$$a'x + b'y = c',$$

et a' et b' sont premiers entre eux. On peut donc supposer que a et b sont premiers entre eux.

Soit $(x, y) \in \mathbb{Z}^2$ et $(x', y') \in \mathbb{Z}^2$ deux solutions de (1.1). Alors $ax + by = ax' + by'$ et $a(x - x') = b(y' - y)$. On en déduit que b divise $a(x - x')$. D'après le théorème de Gauss, b divise $x - x'$. De même a divise $y - y'$. Soient k et l dans $\mathbb{Z}$ tels que $x - x' = bk$ et $y - y' = al$. On obtient

$$x' = x - bk, \qquad y' = y - al.$$

Réciproquement, (x', y') est solution si et seulement si

$$a(x - bk) + b(y - al) = c - ab(k + l) = c,$$

si et seulement si $k = -l$. Donc

$$S = (x, y) + \mathbb{Z}(-b, a).$$

1.6 Congruence

Définition IX.100: Congruence

Soit n un entier naturel non nul. Soit a et b deux entiers relatifs. On dit que a *et* b *sont congrus modulo* n et on note $a \equiv b\ [n]$ si n divise $a - b$.

Remarque. $a \equiv b\ [n]$ si et seulement si les restes des divisions euclidiennes de a et b par n sont égaux. Ces congruences ont le bon goût de bien se comporter par rapport à la somme et au produit :

Théorème IX.101: Opérations et modulo

Soit n un entier naturel non nul. Soit a, b, c et d quatre entiers relatifs tels que

$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases}$$

Alors

(i) $a + c \equiv b + d\ [n]$; et

(ii) $ac \equiv bd\ [n]$.

Preuve

La preuve est laissée en exercice.

Théorème IX.102. Théorème chinois

Soient m et n deux entiers naturels non nuls et premiers entre eux. Soient a et b deux entiers relatifs. Notons S l'ensemble des entiers $k \in \mathbb{Z}$ tels que

$$\begin{cases} k \equiv a\ [n] \\ k \equiv b\ [m] \end{cases}$$

Alors, il existe un unique k_0 tel que

(i) $S = k_0 + nm\mathbb{Z}$;

(ii) $k_0 \in \{0, 1, \ldots, nm - 1\}$.

Preuve

Commençons par montrer que S est non vide. D'après le théorème de Bezout, il existe u et v dans $\mathbb{Z}$ tels que

$$un + vm = 1.$$

Posons

$$s_0 = bun + avm.$$

En remarquant que $un \equiv 1\ [m]$, la proposition IX.101 montre que $bun \equiv b\ [m]$. Mais alors, $s_0 \equiv b\ [m]$.
De même, on montre que $s_0 \equiv a\ [n]$. Ainsi $s_0 \in S$.

Montrons que si $t \in S$ et $k \in \mathbb{Z}$ alors $t + kmn \in S$.
En remarquant que $kmn \equiv 0\ [m]$, la proposition IX.101 montre que $t + kmn \equiv b\ [m]$. De même, $t + kmn \equiv a\ [n]$.

Soit t_1 et t_2 deux élément de S. Montrons que mn divise $t_1 - t_2$.
La proposition IX.101 implique que $t_1 - t_2 \equiv 0\ [m]$ et $t_1 - t_2 \equiv 0\ [n]$. Ainsi, m et n divisent $t_1 - t_2$.
Comme m et n sont premiers entre eux, le théorème de Gauss montre que mn divise $t_1 - t_2$.

Soit k_0 le reste de la division euclidienne de s_0 par mn. Alors $k_0 \in S$. On vient de démontrer que

$$S = k_0 + mn\mathbb{Z}.$$

Mais alors, $(k_0 + mn\mathbb{Z}) \cap \{0, 1, \ldots, nm - 1\} = \{k_0\}$ montrant l'unicité de k_0.

2 Polynômes

2.1 Un peu de vocabulaire

Définition IX.103: Polynôme

Etant donnée une suite fini $(a_0, \dots, a_n)$ de nombres réels ou complexes, on associe la formule suivante

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

où X est une indéterminée. Une telle formule est appelée un *polynôme*.
Si x est dans $\mathbb{R}$ ou $\mathbb{C}$, on peut substituer x à X. On obtient ainsi un nombre complexe $P(x)$. Ainsi, on a une application associée, encore notée P

$$P : \mathbb{C} \longrightarrow \mathbb{C},\ x \longmapsto P(x).$$

Le *degré de* P est le plus grand entier d tel que $a_d \neq 0$. Par convention le degré du polynôme nul est $-\infty$. Le coefficient a_d d'un polynôme de degré d est appelé le *coefficient dominant*. Un polynôme est dit *unitaire* si son coefficient dominant vaut 1.
L'ensemble des polynômes à coefficients complexes (respectivement réels) est noté $\mathbb{C}[X]$ (resp. $\mathbb{R}[X]$).

2.2 Cinq opérations

Les polynômes s'ajoutent, se multiplient, se conjuguent, se dérivent et se substituent.
Soit $P = a_0 + a_1 X + \cdots + a_p X^p$ et $Q = b_0 + b_1 X + \cdots + b_q X^q$ deux polynômes à coefficients complexes (qui peut le plus peut le moins !). Par convention, $a_k = 0$ pour tout $k > p$ et $b_k = 0$ pour tout $k > q$.
La *somme* $P + Q$ des deux polynômes est le polynôme $c_0 + c_1 X + \cdots + c_{\max(p,q)} X^{\max(p,q)}$ tel que

$$c_k = a_k + b_k \qquad \forall k \geqslant 0.$$

Le *produit* PQ des deux polynômes est le polynôme $c_0 + c_1 X + \cdots + c_{p+q} X^{p+q}$ tel que

$$c_k = \sum_{i+j=k} a_i b_j \qquad \forall k \geqslant 0.$$

Le *polynôme dérivé* P' *de* P est défini par

$$P'(X) = a_1 + 2a_2 X + \cdots + p a_p X^{p-1}.$$

Le polynôme *composé* $P \circ Q$ est donné par

$$(P \circ Q)(X) = a_0 + a_1 Q(X) + a_2 Q(X)^2 + \cdots + a_p Q(X)^p.$$

Si P est à coefficients complexes, on définit *le conjugué* $\bar{P}$ de P par

$$\bar{P}(X) = \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_p X^p.$$

Pour $z \in \mathbb{C}$, on a

$$\bar{P}(z) = \overline{P(\bar{z})}.$$

Remarque. Toutes ces opérations sont compatibles avec les opérations analogues sur les fonctions polynomiales, c'est-à-dire commutent à la substitution. Ainsi, pour $x \in \mathbb{C}$, on a $(P + Q)(x) = P(x) + Q(x)$, $(PQ)(x) = P(x)Q(x)$, $(P \circ Q)(x) = P(Q(x))$.

Voici comment se comporte le degré relativement à ces opérations.

Lemme IX.104

$$\deg(PQ) = \deg(P) + \deg(Q)$$
$$\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$$
$$\deg(P') = \deg(P) - 1$$
$$\deg(P \circ Q) = \deg(P).\deg(Q)$$

2.3 Division euclidienne

Comme pour les entiers, on a une division euclidienne avec reste. Ce résultat est très important.

Théorème IX.105. Division Euclidienne

Soit A et B deux polynômes à coefficients complexes avec $B \neq 0$.
Il existe un unique couple de polynômes (Q, R) tels que

(i) $A = BQ + R$;

(ii) $R = 0$ ou $\deg(R) < \deg(B)$.

La démonstration de ce théorème consiste à démontrer (au prix de notations un peu lourdes et d'une récurrence) que l'algorithme décrit ci-dessous fonctionne. Plutôt que de rédiger cette démonstration, nous allons comprendre cet algorithme grâce à quelques exemples.
L'algorithme fonctionne ainsi :

(i) On dispose les polynômes A et B comme pour la division des entiers en les écrivant en puissances décroissantes.

(ii) Le premier monôme (dominant) αX^e de Q est choisi de telle sorte que les termes dominants de $\alpha X^e B$ et de A coïncident.

(iii) On calcule alors $A - \alpha X^e B$.

(iv) On reprend l'étape deux avec $A - \alpha X^e B$ à la place de A.

(v) On s'arrête lorsque le polynôme « A » courant est nul ou de degré strictement inférieur à celui de B.

Voici un premier exemple où $A = x^3 + x^2 - 1$ et $B = x - 1$.

$$\begin{array}{rrrr|rrr}
x^3 & +x^2 & & -1 & x & -1 & \\
\cline{5-7}
-x^3 & +x^2 & & & x^2 & +2x & +2 \\
\cline{1-2}
 & 2x^2 & & & & & \\
 & -2x^2 & +2x & & & & \\
\cline{2-3}
 & & 2x & & & & \\
 & & -2x & +2 & & & \\
\cline{3-4}
 & & & 2 & & &
\end{array}$$

On trouve donc $Q = x^2 + 2x + 2$ et $R = 2$. On pourra vérifier que

$$x^3 + x^2 - 1 = (x-1)(x^2 + 2x + 2) + 1.$$

Un autre exemple $A = 6x^3 - 10x^2 + x + 3$ et $B = x^2 - 6x + 1$:

$$\begin{array}{r|l} 6x^3-10x^2+x+3 & x^2- \ x+1 \\ \cline{2-2} 6x^3-6x^2+6x & 6x-4 \\ \cline{1-1} -4x^2-5x+3 & \\ -4x^2+4x-4 & \\ \cline{1-1} -9x+7 & \end{array}$$

On trouve donc $Q = 6x - 4$ et $R = -9x + 7$. On pourra vérifier que

$$A = BQ + R.$$

Définition IX.106: Divise

On dit que B (supposé non nul) *divise* A si le reste de la division euclidienne de A par B est nul. Ceci équivaut à l'existence d'un polynôme Q tel que

$$A = BQ.$$

2.4 Racines d'un polynôme

Théorème IX.107: Racine d'un polynôme

Soit P un polynôme à coefficients complexes et $z \in \mathbb{C}$. Alors se valent :

(i) $P(z) = 0$;

(ii) $X - z$ divise P.

On dit alors que z est *une racine* de P.

L'ingrédiant principal de la preuve ci-dessous est la division euclidienne.

Preuve

Supposons que $X - z$ divise P : $P(X) = (X - z)Q(X)$. On a évidemment $P(z) = 0Q(z) = 0$. Supposons que $P(z) = 0$. Ecrivons la division euclidienne de P par $X - z$: $P = (X - z)Q + R$ et $\deg(R) < \deg(X - z) = 1$. Donc R est un polynôme constant. De plus, $P(z) = R(z) = 0$. Donc R est nul. Donc $X - z$ divise P.

Corollaire IX.108

Soit P un polynôme complexe non nul de degré d. Alors P a au plus d racines.

Preuve

Soit $z_1, \ldots, z_k$ des racines 2 à 2 distinctes de P. Montrons par récurrence sur i que

$$(X - z_1) \cdots (X - z_i) \text{ divise } P \text{ pour tout } i \in \{1, \ldots, k\}.$$

Initialisation : comme $P(z_1) = 0$, la proposition montre que $(X - z_1)$ divise P.
Hérédité : Soit $i \in \{2, \ldots, k\}$. Supposons que $(X - z_1) \cdots (X - z_{i-1})$ divise P. Montrons que $(X - z_1) \cdots (X - z_i)$ divise P.

On a $P = (X - z_1) \cdots (X - z_{i-1})Q$. Alors comme $P(z_i) = 0$ et $z_i - z_j \neq 0$ pour tout $j < i$, on a $Q(z_i) = 0$. On applique alors la proposition à Q : $Q = (X - z_i)Q_1$. Donc $P = (X - z_1) \cdots (X - z_i)Q_1$. cqfd.

On conclut le corollaire en remarquant que si un polynôme Π divise P alors $\deg(\Pi) \leqslant \deg(P)$.

Remarque. Le corollaire IX.108 est souvent utilisé sous la forme suivante : « Tout polynôme P qui a une infinité de racines est nul ».

2.5 Polynômes irréductibles

Ici la distinction entre $\mathbb{R}$ et $\mathbb{C}$ est importante. Notons $\mathbb{K}$ un de ces deux ensembles.

Définition IX.109: Polynôme irréductible

Un polynôme $P \in \mathbb{K}[X]$ est dit *irréductible dans* $\mathbb{K}[X]$ s'il est non nostant et ne peut pas s'écrire comme le produit de deux polynômes de degrés strictement inférieurs.

Remarque. Attention, un polynôme P de $\mathbb{R}[X]$ appartient aussi à $\mathbb{C}[X]$. En revanche il peut être irréductible dans $\mathbb{R}[X]$ sans l'être dans $\mathbb{C}[X]$.
Regardons le cas de $P = X^2 + 1$. Comme $P = (X - i)(X + i)$, P n'est pas irréductible dans $\mathbb{C}[X]$.
Montrons que P est irréductible dans $\mathbb{R}[X]$. Sinon, il existerait A et B dans $\mathbb{R}[X]$ tels que $P = AB$ et $\deg(A) < \deg(P) = 2$ et $\deg(B) < \deg(P) = 2$. Comme $2 = \deg(P) = \deg(A) + \deg(B)$, on en déduit que $\deg(A) = \deg(B) = 1$. Mais alors $A = aX + b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. Donc $A(-\frac{b}{a}) = 0$, puis $P(-\frac{b}{a}) = 0$. On en déduit que $P = X^2 + 1$ a une racine réelle, ce qui constitue une contradiction.

Proposition IX.110

(i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

(ii) Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Preuve

Il est clair que les polynômes de degré 1 sont irréductibles. Réciproquement, soit $P \in \mathbb{C}[X]$ un polynôme irréductible. D'après le théorème de D'Alembert-Gauss, il existe z dans $\mathbb{C}$ tel que $P(z) = 0$. Mais alors la proposition IX.107 montre que $X - z$ divise P. Comme P est irréductible, il existe $\lambda \in \mathbb{C}$ tel que $P = \lambda(X - z)$. Donc P est de degré 1.

Soit $P \in \mathbb{R}[X]$ un polynôme de degré 2 et de discriminant strictement négatif. Si P n'était pas irréductible, il serait divisible par un polynôme de degré 1. Il aurait donc une racine. Contradiction.

Soit P un polynôme irréductible à coefficients réels. S'il est de degré 1, il n'y a rien à démontrer. Supposons donc que $\deg(P) \geqslant 2$.
D'après le théorème de D'Alembert-Gauss, il existe z dans $\mathbb{C}$ tel que $P(z) = 0$. La proposition IX.107 montre que $X - z$ divise P. Ce qui constitue une contradiction si $z \in \mathbb{R}$. Ainsi $\bar{z} \neq z$. Dans $\mathbb{C}[X]$, on écrit : $P = (X - z)Q$. On remarque, que puisque $P \in \mathbb{R}[X]$,

$$P(\bar{z}) = \overline{P(z)}.$$

Donc $0 = (\bar{z} - z)Q(\bar{z})$ et $Q(\bar{z}) = 0$. Alors Q s'écrit à son tour $Q = (X - \bar{z})Q_1$. On obtient $P = (X - z)(X - \bar{z})Q_1$.
Remarquons que $B := (X - z)(X - \bar{z}) = X^2 - 2\mathrm{Re}(z)X + z\bar{z} \in \mathbb{R}[X]$. On a $P = BQ_1$ et $P = \bar{P} = \bar{B}\bar{Q}_1 = B\bar{Q}_1$. Par unicité de la division euclidienne, on en déduit que $Q_1 = \bar{Q}_1$, donc $Q_1 \in \mathbb{R}[X]$. Comme P est irréductible, on en déduit que Q_1 est constant. Donc P est de degré 2 et n'a pas de racine réelle.

Les polynômes irréductibles jouent le rôle des nombres premiers :

Théorème IX.111

Ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $P \in \mathbb{K}[X]$ non nul. Il existe une écriture de P sous la forme

$$n = \lambda P_1^{\alpha_1} \dots P_s^{\alpha_s},$$

où

(i) $\lambda \in \mathbb{K}$ est une constante ;
(ii) les polynômes P_i sont irréductibles dans $\mathbb{K}[X]$;
(iii) les polynômes P_i sont unitaires et non constants ;
(iv) les exposants α_i sont des entiers naturels non nuls : $\alpha_i \geqslant 1$;

De plus, cette écriture est unique à la numérotation des P_i près.

Nous démontrons maintenant l'existence et nous montrerons l'unicité plus tard.

Preuve

On prouve l'existence par récurrence forte sur le degré de P.
Pour $\deg(P) = 0$ ou 1, l'énoncé est clair.
Pour d dans $\mathbb{N}$, on définit l'assertion H_d : « tout polynôme de degré d peut s'écrire comme un produit de polynômes irréductibles comme dans l'énoncé du théorème ».
Soit $d \geqslant 2$ dans $\mathbb{N}^*$. Supposons H_k vraie pour tout $k \in \{0, 1, \dots, d-1\}$. Montrons H_d.
Soit P tel que $\deg(P) = d$. Si P est irréductible, il n'y a rien à démontrer. Sinon $P = AB$ avec $\deg(A)$ et $\deg(B)$ inférieur à $\deg(P) - 1$. On obtient le résultat en appliquant l'hypothèse de récurrence à A et B.

Le théorème IX.111 et la proposition IX.110 montrent que tout polynôme P à coefficients complexes peut s'écrire sous la forme

$$P = \lambda(X - z_1)^{\alpha_1} \dots (X - z_s)^{\alpha_s},$$

où les z_i sont des nombres complexes deux à deux distincts, $\lambda \in \mathbb{C}$ est le coefficient dominant de P et les exposants α_i appartiennent à $\mathbb{N}^*$.

L'unicité dans le théorème IX.111, permet de montrer facilement, que tout polynôme P à coefficients réels peut s'écrire sous la forme

$$P = \lambda(X - x_1)^{\alpha_1} \dots (X - x_s)^{\alpha_s} . ((X - z_1)(X - \bar{z}_1))^{\beta_1} \dots ((X - z_t)(X - \bar{z}_t))^{\beta_t},$$

où

(i) les x_i sont des nombres réels deux à deux distincts,
(ii) les z_i sont des nombres complexes non réels deux à deux distincts,
(iii) $\lambda \in \mathbb{R}$ est le coefficient dominant de P
(iv) les exposants α_i et β_j appartiennent à $\mathbb{N}^*$.

Le théorème IX.111 et la proposition IX.110 montrent que tout polynôme P à coefficients réels peut s'écrire sous la forme

$$P = \lambda(X - x_1)^{\alpha_1} \dots (X - x_s)^{\alpha_s} . (X^2 + b_1 X + c_1)^{\beta_1} \dots (X^2 + b_t X + c_t)^{\beta_t},$$

où

(i) les x_i sont des nombres réels deux à deux distincts ;
(ii) les $X^2 + b_i X + c_i$ sont des polynômes à coefficients réels deux à deux distincts tels que $b_i^2 - 4c_i < 0$;
(iii) $\lambda \in \mathbb{R}$ est le coefficient dominant de P ;
(iv) les exposants α_i et β_j appartiennent à $\mathbb{N}^*$.

2.6 PGCD

Le théorème suivant permet de définir le pgcd de deux polynômes.

Théorème IX.112. PGCD

Soit A et B deux polynômes, non tous les deux nuls. Il existe un unique diviseur commun unitaire de A et B de degré maximal. On note $\text{pgcd}(A, B)$ ce diviseur commun. Soit D un polynôme non nul. Alors, se valent

(i) D divise A et B ;

(ii) D divise $\text{pgcd}(A, B)$.

Preuve

Soit P un diviseur commun à A et B de degré maximal, c'est-à-dire, que pour tout Q diviseur commun à A et B, on a $\deg(Q) \leqslant \deg(P)$. Supposons de plus que P est unitaire. Montrons que, se valent

(i) D divise A et B ;

(ii) D divise P.

Si D divise P alors D divise A et B. On démontre la réciproque par récurrence sur $\deg(A)+\deg(B)$. Si cette somme vaut 0, l'énoncé est évident. Supposons que D divise A et B. Quitte à échanger A et B supposons que $\deg(A) \geqslant \deg(B)$. On effectue la division euclidienne : $A = BQ + R$. On vérifie que, pour tout polynôme S, les assertions suivantes sont équivalentes :

(i) S divise A et B ;

(ii) S divise R et B.

Il suffit alors de démontrer le résultat pour R et B. Ce qui est fait par l'hypothèse de récurrence puisque $\deg(R) + \deg(B) < \deg(A) + \deg(B)$.

Montrons maintenant l'unicité. Soit P_1 un diviseur commun unitaire de même degré que P. D'après l'équivalence que nous venons de démontrer P_1 divise P. Comme ces deux polynômes sont de même degré, il existe $\lambda \in \mathbb{K}$ tel que $P_1 = \lambda P$. Or les deux polynômes P et P_1 sont unitaires ; donc $\lambda = 1$ et $P = P_1$.

Lorsque les polynômes sont décomposés en produits de polynômes irréductibles, il est facile de calculer leur pgcd :

Théorème IX.113

Soit A et B deux polynômes non nuls. Soit $\lambda, \mu \in \mathbb{K}$, $P_1, \ldots, P_s$ irréductibles unitaires, 2 à 2 distincts tels qu'il existe des entiers naturels $\alpha_1, \ldots, \alpha_s$ et $\beta_1, \ldots, \beta_s$ tels que

$$A = \lambda P_1^{\alpha_1} \ldots P_s^{\alpha_s} \qquad B = \mu P_1^{\beta_1} \ldots P_s^{\beta_s}.$$

Alors

$$\text{pgcd}(A, B) = P_1^{\min(\alpha_1,\beta_1)} \ldots P_s^{\min(\alpha_s,\beta_s)}.$$

Preuve

Nous prouverons ce résultat plus tard.

Algorithme d'Euclide. Cet algorithme très efficace permet de calculer le pgcd de deux polynômes A et B. Le principe de l'algorithme est le suivant :

```
Quitte à échanger A et B on suppose que deg(A) ⩾ deg(B).
Si B = 0, pgcd(A, B) = A.
Si B ≠ 0 on fait la division euclidienne de A par B : A = BQ + R
On écrit que pgcd(A, B) = pgcd(B, R).
```

2.7 Polynômes premiers entre eux

Définition IX.114: Premiers entre eux

On dit que A et B sont premiers entre eux, si $\text{pgcd}(A, B) = 1$.

Théorème IX.115. Bezout

Soit A et B deux polynômes non nuls. Alors A et B sont premiers entre eux si et seulement si il existe U et V dans $\mathbb{K}[X]$ tels que $AU + BV = 1$.

Preuve

S'il existe U et V comme dans l'énoncé, tout diviseur commun de A et B divise 1. Donc $\text{pgcd}(A, B) = 1$.
Supposons à présent que $\text{pgcd}(A, B) = 1$. On fait encore une preuve par récurrence sur $\deg(A) + \deg(B)$. Le point clé, est que si $A = BQ + R$, alors :

$$RU + BV = 1$$

équivaut à

$$AU + B(V - QU) = 1.$$

Exercice 19. *Soit A et B deux polynômes non nuls. Alors il existe U et V dans $\mathbb{K}[X]$ tels que $AU+BV = \text{pgcd}(A, B)$.*

Preuve

Il suffit de diviser A et B par leur pgcd, puis d'appliquer Bezout.

Théorème IX.116. Gauss

Soit A, B et C trois polynômes non nuls. On suppose que A et B sont premiers entre eux et que A divise BC. Alors A divise C.

Exercice 20. *Trouver 3 polynômes tels que A divise BC mais A ne divise ni B ni C. Quel est le pgcd des polynômes A et B que vous avez trouvés ?*

Preuve

D'après le théorème de Bezout IX.92, il existe U et V dans $\mathbb{K}[X]$ tels que

$$AU + BV = 1.$$

Multiplions par C :

$$AUC + BVC = C.$$

Alors A divise AUC mais aussi BVC, donc A divise C.

Corollaire IX.117

Soit P un polynôme irréductible et A et B deux polynômes quelconques. Si P divise AB alors il divise A ou B.

Preuve

Supposons que P ne divise pas A. Alors le pgcd de A et P est un diviseur strict de P : c'est donc 1 puisque P est premier. Mais alors, le théorème de Gauss montre que P divise B.

Exercice 21. *Comme nous l'avons fait pour les entiers, montrer les théorèmes IX.111 et IX.113 en utilisant les théorèmes IX.115 et IX.116.*

2.8 PPCM

Cette notion est complémentaire de la notion de PGCD. Nous ne montrerons pas les résultats qui s'obtiennent de manière analogue au cas du PGCD.

Définition IX.118: PPCM

Soit A et B deux polynômes, non tous les deux nuls. L'ensemble des multiples communs à A et B a un unique élément unitaire de degré minimal appelé *plus petit commun multiple de A et B* et noté $ppcm(A, B)$.

Théorème IX.119. PPCM

Soit A et B deux polynômes, non tous les deux nuls. Soit D un polynôme non nul. Alors, se valent

(i) D est un multiple de A et B ;

(ii) D est un multiple de $\text{ppcm}(A, B)$.

Lorsque les polynômes sont décomposés en produits de polynômes irréductibles, il est facile de calculer leur ppcm :

Théorème IX.120. PPCM

Soit A et B deux polynômes non nuls comme dans le théorème IX.113.
Alors

$$\text{ppcm}(A, B) = P_1^{\max(\alpha_1,\beta_1)} \dots P_s^{\max(\alpha_s,\beta_s)}.$$

Le corollaire suivant précise le fait que pgcd et ppcm sont des notions complémentaires.

Corollaire IX.121

Soit A et B deux polynômes non nuls. Alors, il existe une constante λ telle que

$$AB = \lambda \text{pgcd}(A, B)\text{ppcm}(A, B).$$

Avec ce résultat l'algorithme d'Euclide permet de calculer le ppcm de deux polynômes.

2.9 Congruence

Définition IX.122: Congruence

Soit P un polynôme non nul. Soit A et B deux polynômes. On dit que A *et* B *sont congrus modulo* P et on note $A \equiv B\ [P]$ si P divise $A - B$.

Remarque. $A \equiv B\ [P]$ si et seulement si les restes des divisions euclidiennes de A et B par P sont égaux. Ces congruences ont le bon goût de bien se comporter par rapport à la somme et au produit :

Proposition IX.123

Soit P un polynôme non nul. Soit A, B, C et D quatre polynômes tels que

$$\begin{cases} A \equiv B\ [P] \\ C \equiv D\ [P] \end{cases}$$

Alors

(i) $A + C \equiv B + D\ [P]$; et

(ii) $AC \equiv BD\ [P]$.

Preuve

La preuve est laissée en exercice.

Théorème IX.124. Théorème chinois

Soient P et Q deux polynômes non nuls et premiers entre eux. Soient A et B deux polynômes. Notons $\mathcal{S}$ l'ensemble des $S \in \mathbb{K}[X]$ tels que

$$\begin{cases} S \equiv A\ [P] \\ S \equiv B\ [Q] \end{cases}$$

Alors, il existe un unique S_0 tel que

(i) $\mathcal{S} = S_0 + PQ\mathbb{K}[X]$;

(ii) $\deg(S_0) < \deg(P) + \deg(Q)$.

Preuve

Commençons par montrer que $\mathcal{S}$ est non vide. D'après le théorème de Bezout, il existe U et V dans $\mathbb{K}[X]$ tels que

$$UQ + VP = 1.$$

Posons

$$S_0 = BUP + AVQ.$$

En remarquant que $UP \equiv 1\ [Q]$, la proposition IX.123 montre que $BUP \equiv 1\ [Q]$. Mais alors, $S_0 \equiv B\ [Q]$.
De même, on montre que $S_0 \equiv A\ [P]$. Ainsi $S_0 \in S$.

Montrons que si $T \in \mathcal{S}$ et $C \in \mathbb{K}[X]$ alors $T + CPQ \in \mathcal{S}$.
En remarquant que $CPQ \equiv 0\ [Q]$, la proposition IX.123 montre que $T + CPQ \equiv B\ [Q]$. De même, $T + CPQ \equiv A\ [P]$.

Soit T_1 et T_2 deux élément de $\mathcal{S}$. Montrons que PQ divise $T_1 - T_2$.
La proposition IX.123 implique que $T_1 - T_2 \equiv 0\ [Q]$ et $T_1 - T_2 \equiv 0\ [P]$. Ainsi, Q et P divisent $T_1 - T_2$. Comme Q et P sont premiers entre eux, le théorème de Gauss montre que PQ divise $T_1 - T_2$.

Soit C_0 le reste de la division euclidienne de S_0 par PQ. Alors $C_0 \in S$. On vient de démontrer que

$$\mathcal{S} = C_0 + PQ\mathbb{K}[X].$$

Exercice 22. *Trouver 4 polynômes P, Q, A et B tels que le système*

$$\begin{cases} S \equiv A\ [P] \\ S \equiv B\ [Q] \end{cases}$$

n'a pas de solution. Et avec $P \neq Q$?

2.10 Ordre de multiplicité d'une racine

Définition IX.125: Ordre d'une racine

Soit P un polynôme à coefficients complexes, $z \in \mathbb{C}$ et $\alpha \in \mathbb{N}$.
On dit que z est une racine d'ordre α si $(X - z)^\alpha$ divise P et $(X - z)^{\alpha+1}$ ne divise pas P.

Le vocabulaire est étrange parfois : une racine d'ordre 0 n'est pas une racine.

On note $P^{(k)}$ la dérivée k-ième de P : $P^{(k)}(X) = (P^{(k-1)})'(X)$. On peut caractériser l'ordre d'une racine en termes des polynômes dérivés.

Théorème IX.126. Ordre d'une racine

Soit P un polynôme à coefficients complexes, $z \in \mathbb{C}$ et $\alpha \in \mathbb{N}$.
Alors, se valent :

(i) $(X - z)^\alpha$ divise P ;
(ii) $P(z) = \cdots = P^{(\alpha-1)}(z) = 0$.

Preuve

Supposons d'abord que $(X - z)^\alpha$ divise P. Il existe alors $Q \in \mathbb{C}[X]$ tel que $P = (X - z)^\alpha Q$. On

rappelle la formule le Leibnitz :

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)} g^{(k-i)}.$$

La preuve de cette formule se fait par récurrence sur k en utilisant la formule de dérivation d'un produit.
On obtient pour P et $k \leqslant \alpha - 1$:

$$(P)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} ((X-z)^{\alpha})^{(i)} Q^{(k-i)}. \tag{2.1}$$

On remarque alors que

$$((X-z)^{\alpha})^{(i)} = (\alpha.(\alpha-1)\dots(\alpha-i+1))(X-z)^{\alpha-i} \quad \text{si } i \leqslant \alpha,$$

et

$$((X-z)^{\alpha})^{(i)} = 0 \quad \text{si } i > \alpha.$$

En particulier, pour tout $i \leqslant k < \alpha$, on a

$$\Big(((X-z)^{\alpha})^{(i)}\Big)(z) = 0.$$

En injectant dans la formule (2.1), on déduit que $P^{(k)}(z) = 0$.

Réciproquement, supposons que $P(z) = \cdots = P^{(\alpha-1)}(z) = 0$. Ecrivons la division euclidienne de P par $(X-z)^{\alpha}$:

$$P = (X-z)^{\alpha} Q + R,$$

avec $\deg(R) < \alpha$. L'assertion déjà démontrée implique que

$$R(z) = \cdots = R^{(\alpha-1)}(z) = 0.$$

Considérons le polynôme auxiliaire

$$S(X) = R(z+X) \quad R(X) = S(X-z).$$

La formule de dérivation d'un polynôme composé implique que

$$S^{(k)}(X) = R^{(k)}(z+X),$$

donc

$$S(0) = \cdots = S^{(\alpha-1)}(0) = 0.$$

Ecrivons $S = a_0 + a_1 X + \cdots + a_{\alpha-1} X^{\alpha-1}$. Par une récurrence immédiate, on montre que

$$S^{(k)}(0) = k! a_k \quad \forall k = 0, \dots, \alpha - 1.$$

On en déduit que $S = 0$, puis que $R = 0$. Ainsi $(X-z)^{\alpha}$ divise P.

3 Ecriture en base b

On sait depuis l'école primaire que 352 signifie $3 \times 100 + 5 \times 10 + 2$ et que tout entier peut s'écrire ainsi de manière unique. Cela est basé l'énoncé suivant.

Théorème IX.127

Soit b un entier supérieur à deux. Pour tout entier naturel non nul n, il existe un unique uple $(a_0, a_1, \ldots, a_p)$ tel que :

(i) $a_i \in \{0, 1, \ldots, b-1\}$;

(ii) $a_p \neq 0$;

(iii) $b = a_0 + a_1 b + a_2 b^2 + \cdots + a_p b^p$.

Application. Un nombre $n = a_p a_{p-1} \ldots a_0$ écrit en base 10 est divisible par 9 si et seulement si $a_p + a_{p-1} + \cdots + a_0$ l'est.
En effet, $n = a_p a_{p-1} \ldots a_0 = \sum_i a_i 10^i \equiv \sum_i a_i [9]$ car $10 \equiv 1[9]$. On a même montré que n est $a_p + a_{p-1} + \cdots + a_0$ ont le même reste par la division euclidienne par 9.

Chapitre 10

Dérivabilité

Sommaire

1 Définition

Définition X.128: Dérivabilité

Soit I un intervalle de $\mathbb{R}$ et $f : I \longrightarrow \mathbb{R}$ une fonction définie sur I. Soit a un point dans l'intérieur de I.
On dit que f est *dérivable en* a si la limite suivante existe dans $\mathbb{R}$

$$\lim_{h\to 0} \frac{f(a+h)-f(a)}{h}.$$

On note alors $f'(a)$ la valeur de cette limite et on l'appelle la *dérivée de* f *en* a.

Comme pour les fonctions continues, on dit que f est dérivable sur I ouvert si f est dérivable en tout point de I. La valeur $f'(a)$ est la pente de la tangente au graphe de f en le point $(a, f(a))$.

Théorème X.129. Dérivabilité et continuité

Toute fonction dérivable est continue.

Preuve

Soit a unn point de I où $f : I \longrightarrow \mathbb{R}$ est dérivable. Alors

$$f(a+h) = h.\frac{f(a+h)-f(a)}{h} + f(a)$$

tend vers $f(a)$ lorsque h tend vers 0.

Remarque. Le fait que f soit dérivable sur I signifie intuitivement qu'elle est continue et que son graphe est lisse. Les anglo-saxons utilisent le mot « smooth ».

2 Opérations

2.1 Somme, produit, quotient

Théorème X.130. Opérations et dérivées

Soit f et g deux fonctions dérivables en un point a.

(i) Alors $f+g$ est dérivable en a et

$$(f+g)'(a) = f'(a) + g'(a).$$

(ii) Alors fg est dérivable en a et

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a).$$

(iii) Si $g(a) \neq 0$, alors $\frac{f}{g}$ est dérivable en a et

$$(\frac{f}{g})'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2}.$$

Preuve

On fait ici la preuve pour le produit. Il s'agit de montrer qu'elle existe et calculer la limite du taux de variation. Pour $h \in \mathbb{R}$, on a

$$\begin{aligned}\frac{(fg)(a+h)-(fg)(a)}{h} &= \frac{f(a+h)g(a+h)-f(a)g(a+h)+f(a)g(a+h)-f(a)g(a)}{h} \\ &= \frac{f(a+h)-f(a)}{h}g(a+h) + \frac{g(a+h)-g(a)}{h}f(a).\end{aligned}$$

Comme $g(a+h)$ tend vers $g(a)$, le premier terme tend vers $f'(a)g(a)$ lorsque h tend vers 0. Le second terme tend vers $f(a)g'(a)$ lorsque h tend vers 0. Ce qui permet de conclure.

Remarque. On écrit quelquefois pour résumer ce théorème $(u+v)' = u' + v'$, $(uv)' = u'v + uv'$ et

$$(\frac{u}{v})' = \frac{u'v + uv'}{v^2}.$$

2.2 Composée

Théorème X.131. Dérivée d'une composée

Soit $f : J \longrightarrow \mathbb{R}$ et $g : I \longrightarrow J$ deux fonctions. Soit a dans l'intérieur de I. On suppose que g est dérivable en a et f est dérivable en $g(a)$.
Alors, $f \circ g$ est dérivable en a et

$$(f \circ g)'(a) = g'(a)f'(g(a)).$$

Preuve

Il s'agit de montrer qu'elle existe et calculer la limite du taux de variation. Pour $h \in \mathbb{R}$, on a

$$\frac{(f \circ g)(a+h) - (f \circ g)(a)}{h} = \frac{f(g(a+h)) - f(g(a))}{g(a+h) - g(a)} \times \frac{g(a+h) - g(a)}{h}.$$

Le second facteur de ce produit tend vers $g'(a)$. Comme $g(a+h)$ tennd vers $g(a)$, le premier facteur tend vers $f'(g(a))$.
Cette preuve suppose implicitement que $g(a+h) - g(a) \neq 0$. Elle n'est donc pas complètement correcte.

Remarque. On écrit quelquefois pour résumer ce théorème

$$(u \circ v)' = v'.u' \circ v.$$

Exemple 13. En appliquant ce théorème on obtient

$$(\sin(3x^2+2))' = 6x\cos(3x^2+2) \qquad (\sqrt{x^2+x+1})' = \frac{2x+1}{2\sqrt{x^2+x+1}}.$$

2.3 Réciproque

Théorème X.132. Dérivée de la réciproque

Soit $f : I \longrightarrow J$ une fonction bijective. On note $g : J \longrightarrow I$ la réciproque de f. Soit a dans l'intérieur de J.

On suppose que f est dérivable en $g(a)$ et que $f'(g(a))$ est non nul. Alors g est dérivable en a et

$$g'(a) = \frac{1}{f'(g(a))}.$$

Preuve

On pose $b = g(a)$. Fixons $h \in \mathbb{R}$ tel que $a + h \in J$. On regarde alors

$$\frac{g(a+h) - g(a)}{h}.$$

On pose $b' = g(a+h)$. On a $f(b) = a$ et $f(b') = a + h$. Donc $h = (a+h) - a = f(b') - f(b)$. Ainsi

$$\frac{g(a+h) - g(a)}{h} = \frac{b' - b}{f(b') - f(b)}.$$

Comme g est continue en a, b' tend vers b lorsque h tend vers 0. Par conséquent, le taux de variation tend vers

$$\frac{1}{f'(g(a))}.$$

cqfd

Remarque. Si $f'(g(a)) = 0$ la formule ne définit pas un nombre réel. Géométriquement cela signifie que la tangente au graphe de f en $b = g(a)$ est horizontale. Alors, la tangente en a au graphe de g est verticale : donc g n'est pas dérivable en a.
Plus généralement, l'interprétation de la dérivée comme la pente de la tangente permet de comprendre (voire de démontrer) le théorème.

Exemples 14. (i) La fonction $f :]0;+\infty[\longrightarrow]0;+\infty[,\ x \longmapsto x^2$ est dérivable et bijective. De plus, $f'(x) = 2x$ ne s'annule pas.
Soit $y \in]0;+\infty[$ et $x \in]0;+\infty[$ tel que $x^2 = y$. On retrouve

$$g'(y) = \frac{1}{f'(g(y))} = \frac{1}{2\sqrt{y}}.$$

(ii) La fonction $\sin :]-\frac{\pi}{2};\frac{\pi}{2}[\longrightarrow]-1;1[$ est bijective. On note $\arcsin :]-1;1[\longrightarrow]-\frac{\pi}{2};\frac{\pi}{2}[$ l'application réciproque.
Sur $]-\frac{\pi}{2};\frac{\pi}{2}[$, la dérivée cos de sin ne s'annule pas. Donc arcsin est dérivable sur $]-1;1[$. Soit $y \in]-1;1[$. On a

$$\arcsin'(y) = \frac{1}{\cos(\arcsin(y))}.$$

Or $\arcsin(y) \in]-\frac{\pi}{2};\frac{\pi}{2}[$, donc $\cos(\arcsin(y)) > 0$. En particulier,

$$\cos(\arcsin(y)) = \sqrt{\cos(\arcsin(y))^2} = \sqrt{1 - \sin(\arcsin(y))^2} = \sqrt{1-y^2}.$$

Ainsi

$$\arcsin'(y) = \frac{1}{\sqrt{1-y^2}}.$$

(iii) La fonction $\tan :]-\frac{\pi}{2};\frac{\pi}{2}[\longrightarrow \mathbb{R}$ est bijective. On note $\arctan : \mathbb{R} \longrightarrow]-\frac{\pi}{2};\frac{\pi}{2}[$ l'application réciproque.
Sur $]-\frac{\pi}{2};\frac{\pi}{2}[$, la dérivée de tan vaut

$$1 + \tan^2$$

et ne s'annule pas. Donc arctan est dérivable sur $\mathbb{R}$. Soit $y \in \mathbb{R}$. On a

$$\arctan'(y) = \frac{1}{1 + \tan(\arctan(y))^2} = \frac{1}{1+y^2}.$$

3 Théorème des accroissements finis

3.1 Extremum et dérivée

Définition X.133: Extremum (local)

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle et $a \in I$. On dit que a est un *maximum* de f si

$$\forall x \in I \qquad f(x) \leqslant f(a).$$

On dit que a est un *minimum* de f si

$$\forall x \in I \qquad f(x) \geqslant f(a).$$

On dit que a est un *maximum local* de f si

$$\exists \varepsilon > 0 \qquad \forall x \in I \cap]a-\varepsilon; a+\varepsilon[\qquad f(x) \leqslant f(a).$$

On dit que a est un *minimum local* de f si

$$\exists \varepsilon > 0 \qquad \forall x \in I \cap]a-\varepsilon; a+\varepsilon[\qquad f(x) \geqslant f(a).$$

On dit que a est un *extremum (local)* s'il est un maximum (local) ou unn minimum (local).

La dérivation est un moyen de trouver les extremums locaux d'une fonction. En effet, la dérivation transforme ces extremums est zéros :

Théorème X.134. Extremum et dérivée

Soit $f : I \longrightarrow \mathbb{R}$ une fonction et a un point dans **l'intérieur de** I. On suppose que f est dérivable en a.
Alors, si a est unn extremum local de f alors

$$f'(a) = 0.$$

Preuve

Pour fixer les idées, on suppose que a est un maximum local. Fixons $\varepsilon > 0$ tel que $]a-\varepsilon; a+\varepsilon[\subset I$ et a est un maximum de $f_{]a-\varepsilon;a+\varepsilon[}$.
Pour tout $h \in]0; \varepsilon[$, on a

$$\frac{f(x+h) - f(x)}{h} \leqslant 0.$$

En passant à la limite lorsque h tend vers 0, on obtient $f'(a) \leqslant 0$.
Pour tout $h \in]-\varepsilon; 0[$, on a

$$\frac{f(x+h) - f(x)}{h} \geqslant 0.$$

En passant à la limite lorsque h tend vers 0, on obtient $f'(a) \geqslant 0$.
Finalement $f'(a) = 0$.

Remarque. Prenez garde au fait que la réciproque du théorème X.134 est fausse. Il se peut que la dérivée soit nulle en a sans que pour autant a soit un extremum local. La fonction $x \longmapsto x^3$ est un exemple avec $a = 0$.

3.2 Théorème de Rolle

Théorème X.135. Théorème de Rolle

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle I. Soit $a < b$ deux points de I tels que

(i) $f(a) = f(b)$;

(ii) f est continue sur $[a; b]$;

(iii) f est dérivable sur $]a; b[$.

Alors il existe $c \in]a; b[$ tel que

$$f'(c) = 0.$$

Preuve

La restriction de f à l'intervalle fermé borné $[a; b]$ est continue.D'après le théorème VIII.80, $f_{|[a;b]}$ est bornée et atteint ses bornes. Posons

$$M := \sup\{f(x) : x \in [a; b]\} \quad \text{et} \quad m := \inf\{f(x) : x \in [a; b]\}.$$

On distingue deux cas :
Cas 1. $m = M$.
Alors f est constante et $f' = 0$. Le théorème est évident.

Cas 2. $m < M$.
Alors $f(a) \neq m$ ou $f(a) \neq M$. Supposons que $f(a) \neq M$, le second cas se traitant de manière analogue. D'après le théorème VIII.80, il existe c tel que $f(c) = M$. Mais alors $c \neq a$ et $c \neq b$. Ainsi $c \in]a; b[$ et f est dérivable en c.
Mais alors, le théorème X.134 implique que $f'(c) = 0$.

3.3 Théorème des accroissements finis

Théorème X.136. TAF

Soit $f : I \longrightarrow \mathbb{R}$ une fonction définie sur un intervalle I. Soit $a < b$ deux points de I tels que

(i) f est continue sur $[a; b]$;

(ii) f est dérivable sur $]a; b[$.

Alors il existe $c \in]a; b[$ tel que

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

Preuve

Si $f(b) = f(a)$, le TAF ne dit rien de plus que le théorème de Rolle. Le principe est de se ramener à ce cas.
Considérons la fonction

$$\begin{array}{rccc} g : & I & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) - x\frac{f(b)-f(a)}{b-a} \end{array}$$

Cette fonction est dérivable sur $]a; b[$ et continue sur $[a; b]$. De plus, un calcul direct montre que $g(a) = g(b)$. D'après le théorème de Rolle, il existe $c \in]a; b[$ tel que $g'(c) = 0$. Or

$$g'(x) = f'(x) - \frac{f(b) - f(a)}{b - a}.$$

Ainsi

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Exercice 23. *Interpréter géométriquement ce théorème.*

Le TAF est un pilier de l'analyse réelle puisque c'est lui que l'on utilise lorsqu'on dresse un tableau de variation :

Corollaire X.137

Soit $f : I \longrightarrow \mathbb{R}$ une fonction dérivable sur un intervalle ouvert I.
Alors f est croissante si et seulement si sa dérivée est positive.
De même, f est décroissante si et seulement si sa dérivée est négative.

Preuve

Supposons que f est croissante. Soit $x \in I$. Alors, pour tout $h \neq 0$,

$$\frac{f(x+h) - f(x)}{h} \geqslant 0.$$

En passant à la limite $f'(x) \geqslant 0$.
Supposons à présent que $f'(x) \geqslant 0$ pour tout $x \in I$. Soit $a < b$ deux points de I. Par le TAF, il existe c tel que

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

Mais alors

$$f(b) - f(a) = (b - a)f'(c) \geqslant 0.$$

Donc f est croissante.
Le cas d'une fonction décroissante se démontre de manière analogue.

Ce théorème sert aussi à décorer les ponts à Pékin :

4 Prolongement de fonctions dérivables

Le théorème suivant permet de montrer qu'une fonction est dérivable en un point en calculant une fonction dérivée et une limite. Lorsqu'il s'applique il est plus simple que de faire appel au taux de variation.

Théorème X.138. Prolongement de fonctions dérivables

Soit $f : I \longrightarrow \mathbb{R}$ une fonction continue sur un intervalle I et a un point de I. On suppose que f est dérivable sur $I - \{a\}$ et que

$$\lim_{\substack{x \to a \\ x \in I - \{a\}}} f'(x) = l \in \mathbb{R}$$

Alors, f est dérivable en a et $f'(a) = l$.

Preuve

Pour tout $x \in I - \{a\}$, le théorème des accroissements finis montre qu'il existe c_x tel que

$$\frac{f(x) - f(a)}{x - a} = f'(c_x).$$

De plus, si $x > a$ (resp. $x < a$) alors $c_x \in]a; x[$ (resp. $c_x \in]x; a[$). En particulier $|c_x - a| < |x - a|$. Donc lorsque $x \to a$, $c_x \to a$. Par composition des limites, on en déduit que le taux de variation tend vers l.

Exemple 15. Soit f la fonction définie par

$$\begin{array}{rccccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R} & & \\ & x & \longmapsto & e^{-\frac{1}{x}} & \text{si} & x > 0 \\ & & & 0 & \text{si} & x \leqslant 0 \end{array}$$

On se propose de montrer que f est dérivable sur $\mathbb{R}$.

Méthode 1 : Sans théorème de prolongement.
Comme composée de fonctions dérivables f est dérivable sur $]0; +\infty[$. Comme fonction constante, f est dérivable sur $]-\infty; 0[$. On a

$$\frac{f(h) - f(0)}{h - 0} = \frac{f(h)}{h} = \begin{cases} e^{-\frac{1}{h}}/h & \text{si } h > 0 \\ 0 & \text{si } h < 0 \end{cases}$$

Or en posant $y = -1/h$, on obtient

$$\lim_{h \to 0^+} e^{-\frac{1}{h}}/h = \lim_{y \to -\infty} -ye^y = 0.$$

Ainsi, à droite comme à gauche le taux de variation tend vers 0. Donc f est dérivable en 0 et $f'(0) = 0$.

Méthode 2 : Avec le théorème de prolongement.
On remarque que $\lim_{x \to 0^+} e^{-\frac{1}{x}} = \lim_{x \to 0^-} 0 = 0 = f(0)$. Donc f est continue en 0.
Pour tout $x \in]0; +\infty[$, on a

$$f'(x) = \frac{e^{-\frac{1}{x}}}{x^2}.$$

Donc $f'(x) \longrightarrow_{x \to 0^+} 0$. Par ailleurs $f'(x) \longrightarrow_{x \to 0^-} 0$. Donc $f'(x) \longrightarrow_{x \to 0} 0$.
Comme f est continue sur $\mathbb{R}$, dérivable sur $\mathbb{R} - \{0\}$ et sa dérivée a une limite en 0, le théorème de prolongement montre que f est dérivable sur $\mathbb{R}$. De plus, $f'(0) = 0$.

5 Cas des bornes de l'intervalle de définition

Si f est définie sur un itervalle fermé $[a;b]$ (ou semi-fermé $[a;b[$) on étend la notion de dérivabilité en a et b. On dit que f est dérivable a si

$$\frac{f(x+h)-f(x)}{h}$$

a une limite lorsque h tend vers 0 et $h>0$.
L'ensemble des résultats s'étendent à ce contexte à une exception notable près : le théorème X.134 sur les extremums. En effet, la fonction $f : [0;1] \longrightarrow [0;1],\ x \longmapsto x$ est dérivable, 0 est un minimum mais $f'(0)=1$.

Remarques sur oraux rattrapage

(i) Des difficultés avec les calculs simples : distributivité, fractions, racines

(ii) Insister sur récurrence faible, forte, à deux crans...