

Chapitre 1

Ensembles et sous-ensembles

1. Notion d'ensemble - Élément d'un ensemble

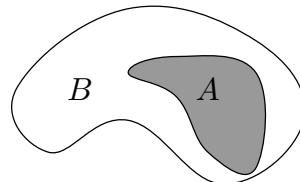
Un *ensemble* est une collection d'objets satisfaisant un certain nombre de propriétés et chacun de ces objets est appelé *élément* de cet ensemble. Si x est un élément de l'ensemble E , on dit aussi que x *appartient* à E et on note $x \in E$. Si x n'appartient pas à E , on note $x \notin E$. Deux ensembles sont *égaux* s'ils ont les mêmes éléments. On admet l'existence d'un ensemble n'ayant aucun élément. Cet ensemble est appelé *ensemble vide* et noté \emptyset .

Notations

- Il y a des notations réservées pour certains ensembles ; par exemple, \mathbb{N} est l'ensemble des entiers naturels ; \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} désignent respectivement l'ensemble des entiers relatifs, des nombres rationnels, des nombres réels et des nombres complexes ; \mathbb{R}^* , \mathbb{R}_+ , \mathbb{R}_+^* désignent les réels non nuls, les réels positifs, les réels strictement positifs, etc.
- L'ensemble E dont les éléments sont 1, 2, 3, 4 est noté $E = \{1, 2, 3, 4\}$.
- Un ensemble à un seul élément x est noté $\{x\}$ et on l'appelle le *singleton* $\{x\}$. On a donc $x \in \{x\}$ (et pas $x = \{x\}$).
- L'ensemble E' dont les éléments sont les entiers naturels x tels que $x \leq 4$ est noté $E' = \{x \in \mathbb{N} \mid x \leq 4\}$ (et on a aussi $E' = \{0, 1, 2, 3, 4\}$).
- Plus généralement, soit E un ensemble et $\mathbf{P}(x)$ une propriété vérifiée ou non suivant la valeur de x , élément de E ; l'ensemble A dont les éléments sont les éléments x de E qui vérifient $\mathbf{P}(x)$ est noté $A = \{x \mid x \in E \text{ et } \mathbf{P}(x)\}$ ou $A = \{x \in E \mid \mathbf{P}(x)\}$.

2. Relation d'inclusion

Définition 1.1 – Soient A et B deux ensembles. On dit que A est inclus dans B si chaque élément de A est un élément de B . On note $A \subset B$. On dit aussi “ A est contenu dans B ” ou “ A est une partie de B ” ou “ A est un sous-ensemble de B ”.



$$A \subset B$$

Remarques - • $A \subset A$

- Si $A \subset B$ et $B \subset C$, alors $A \subset C$
- $A = B$ si et seulement si ($A \subset B$ et $B \subset A$).

On traduit les propriétés précédentes en disant que la relation d'inclusion est respectivement *réflexive*, *transitive* et *antisymétrique*. On peut rapprocher ces propriétés de celles de la relation d'inégalité \leq dans \mathbb{R} : pour tous a, b, c réels, on a $a \leq a$, si ($a \leq b$ et $b \leq c$) alors $a \leq c$ et si ($a \leq b$ et $b \leq a$), alors $a = b$. De telles relations sont appelées *relations d'ordre*.

Exemples - • $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

- $\{x \in \mathbb{R} \mid 0 < x < 4\} \subset \mathbb{R}_+$

Définition 1.2 – Soit E un ensemble. Les sous-ensembles de E forment un ensemble appelé *ensemble des parties de E* et noté $\mathcal{P}(E)$.

Exemple - Si $E = \{1, 2\}$, alors $\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, E\}$.

Remarque - Les trois assertions $x \in E$, $\{x\} \subset E$ et $\{x\} \in \mathcal{P}(E)$ sont équivalentes.

Exercice - 1°) Soit $E = \{1, 2, 3\}$. Donner tous les sous-ensembles de E .

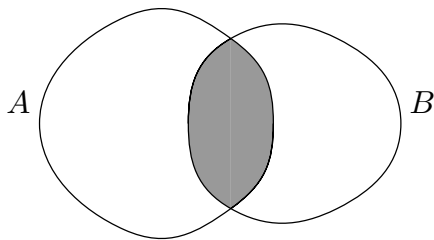
2°) Montrer, par récurrence sur n , qu'un ensemble à n éléments a 2^n sous-ensembles.

3°) Soient A et B des sous-ensembles d'un ensemble E . Montrer que ($A \subset B$ si et seulement si $\mathcal{P}(A) \subset \mathcal{P}(B)$).

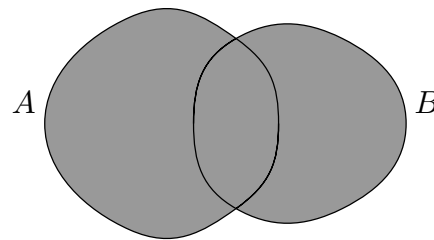
3. Intersection et réunion

Définition 1.3 – Soient A et B deux sous-ensembles d'un ensemble E . L'ensemble $\{x \mid x \in A \text{ et } x \in B\}$ est appelé l'intersection des ensembles A et B et est noté $A \cap B$. Si $A \cap B = \emptyset$, on dit que A et B sont disjoints.

L'ensemble $\{x \mid x \in A \text{ ou } x \in B\}$ est appelé l'union des ensembles A et B et est noté $A \cup B$.



$$A \cap B = \{x \mid x \in A \text{ et } x \in B\}$$



$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

Soient A et B deux sous-ensembles d'un ensemble E . On a :

- 1) $A \cap \emptyset = \emptyset$ et $A \cup \emptyset = A$
- 2) $A \cap B \subset A$ et $A \cap B \subset B$
- 3) $A \subset A \cup B$ et $B \subset A \cup B$
- 4) $A \cup B = A$ si et seulement si $B \subset A$
- 5) $A \cap B = A$ si et seulement si $A \subset B$

Propriétés de \cap et \cup -

Soient A, B, C trois sous-ensembles d'un ensemble E . On a :

- 1) $A \cup B = B \cup A$
- 2) $A \cap B = B \cap A$
- 3) $A \cup (B \cap C) = (A \cup B) \cap C$
- 4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- 5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- 6) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

On traduit ces propriétés en disant que \cup et \cap sont *commutatives* (propriétés 1 et 2), *associatives* (propriétés 3 et 4), que \cup est *distributive par rapport à \cap* (propriété 5) et \cap est *distributive par rapport à \cup* (propriété 6). Ces propriétés seront étudiées dans le chapitre sur les lois de composition internes. Pour s'en souvenir, on peut les comparer aux propriétés analogues de l'addition et de la multiplication dans \mathbb{R} : pour a, b, c réels, on a $a+b = b+a$, $ab = ba$, $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$, $a(b+c) = ab+ac$. Mais on n'a pas l'équivalent de la propriété 5 ; en général, on n'a pas $a+(bc) = ab+ac$ (trouver un exemple).



Ne pas oublier les parenthèses. Par exemple, $A \cap B \cup C$ n'a pas de sens. Si $A = [0, 1]$, $B = [1, 2]$ et $C = [2, +\infty[$, on a $(A \cap B) \cup C = \{1\} \cup [2, +\infty[$, et $A \cap (B \cup C) = \{1\}$.

Généralisation - Si A_1, A_2, \dots, A_n sont des sous-ensembles d'un ensemble E , on définit de même la réunion $A_1 \cup A_2 \cup \dots \cup A_n$ comme l'ensemble des x qui appartiennent à au moins l'un des ensembles A_1, A_2, \dots ou A_n et l'intersection $A_1 \cap A_2 \cap \dots \cap A_n$ comme l'ensemble des x qui appartiennent à tous les ensembles A_1, A_2, \dots, A_n :

$$A_1 \cup A_2 \cup \dots \cup A_n = \{x \mid \exists i \in \{1, 2, \dots, n\}, x \in A_i\}$$

$$A_1 \cap A_2 \cap \dots \cap A_n = \{x \mid \forall i \in \{1, 2, \dots, n\}, x \in A_i\}$$

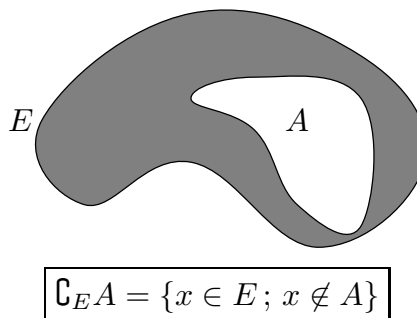
Exercice - 1°) Soient A, B, C, D des sous-ensembles d'un ensemble E . Montrer que $(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D)$. Simplifier le résultat lorsque l'on a $A \subset C$.

2°) Soit E un ensemble qui est la réunion de deux sous-ensembles A et B . On suppose que A et B sont finis et ont respectivement n et m éléments. Si A et B sont disjoints, combien E a-t-il d'éléments ?

Plus généralement, si $A \cap B$ a p éléments, montrer que E en a $n + m - p$.

4. Complémentaire d'un ensemble

Définition 1.4 – Soient E un ensemble et A un sous-ensemble de E . Le complémentaire de A dans E est l'ensemble $\{x \mid x \in E \text{ et } x \notin A\}$. On le note $\complement_E A$ ou $E \setminus A$ ou encore lorsqu'il n'y a pas d'ambiguïté sur E , ${}^c A$, A^c ou \overline{A} .



Propriétés du complémentaire (Lois de De Morgan) -

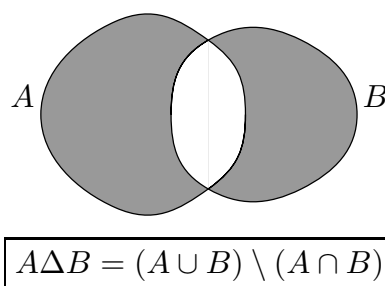
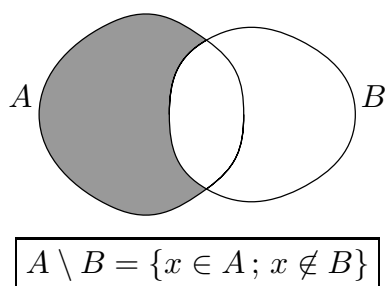
Soient E un ensemble, A et B des sous-ensembles de E .

- 1) $\complement_E(\complement_E A) = A$
- 2) $A \subset B$ si et seulement si $(\complement_E B) \subset (\complement_E A)$
- 3) $\complement_E(A \cup B) = (\complement_E A) \cap (\complement_E B)$
- 4) $\complement_E(A \cap B) = (\complement_E A) \cup (\complement_E B)$

Définition 1.5 – Soient A et B deux sous-ensembles d'un ensemble E . On note

- 1 – $A \setminus B$ l'ensemble $\{x \in A \mid x \notin B\}$ et on l'appelle différence de A et B .
- 2 – $A \Delta B$ l'ensemble $(A \cup B) \setminus (A \cap B)$ et on l'appelle différence symétrique de A et B .

Proposition 1.6 – $A \Delta B = (A \setminus B) \cup (B \setminus A)$.



Remarques - • La différence symétrique correspond au 'ou' exclusif : $A \Delta B$ est l'ensemble des points qui appartiennent à A ou à B , mais PAS à A et B en même temps.

- Lorsque l'on a $B \subset A$, la différence de A et B est aussi le complémentaire de B dans A .
- $A \setminus B = A \cap B^c$.
- $A \subset B$ si et seulement si $A \setminus B = \emptyset$.



Ne pas oublier les parenthèses.

Trouver un exemple d'ensembles vérifiant $(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$.

*Exercice - 1°) Soient $A = \{x \in \mathbb{R} \mid x^2 - 3x + 1 > 0\}$ et $B = \{x \in \mathbb{R} \mid x > 0\}$.
Montrer que les ensembles $A^c, B^c, A \cap B, A \cup B, A \setminus B, B \setminus A$ et $A \Delta B$ sont des intervalles ou des réunions d'intervalles et préciser lesquels.*

2°) Soient A et B des sous-ensembles d'un ensemble E . Montrer que les trois propriétés suivantes sont équivalentes :

1) $A = B$ 2) $A \setminus B = B \setminus A$ 3) $A \Delta B = \emptyset$

3°) Même question pour les six propriétés suivantes. (On peut montrer qu'elles sont toutes équivalentes à la première) :

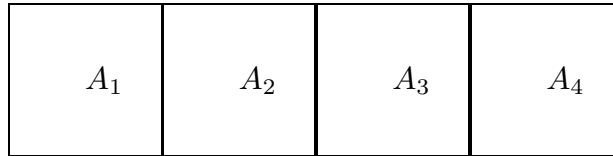
1) $A \subset B$ 2) $B^c \subset A^c$ 3) $A \cap B = A$

4) $A \cup B = B$ 5) $A \setminus B = \emptyset$ 6) $A \Delta B = B \setminus A$

5. Partitions

Définition 1.7 – Soient E un ensemble et A_1, A_2, \dots, A_n des sous-ensembles de E . On dit que ces sous-ensembles forment une partition de E si les trois conditions suivantes sont vérifiées :

- 1) Leur réunion est égale à E : $E = A_1 \cup A_2 \cup \dots \cup A_n$
- 2) Ils sont deux à deux disjoints : si $i, j \in \{1, 2, \dots, n\}$ et $i \neq j$ alors $A_i \cap A_j = \emptyset$
- 3) Chacun de ces ensembles est non vide : pour tout $i \in \{1, 2, \dots, n\}$, $A_i \neq \emptyset$.



←————— E —————→

Sur le dessin ci-dessus, les ensembles A_1, \dots, A_4 forment une partition de l'ensemble E .

Exemples - • Soient $E = \mathbb{N}$, A_1 le sous-ensemble formé des entiers pairs, A_2 le sous-ensemble formé des entiers impairs. Alors, les sous-ensembles A_1 et A_2 forment une partition de E .

• Soient $E = \mathbb{R}$, $A_1 = \mathbb{R}_+^*$, $A_2 = \mathbb{R}_-^*$, $A_3 = \{0\}$. Alors, les sous-ensembles A_1, A_2 et A_3 forment une partition de E .



Attention à ne pas confondre les termes “disjoint” et “distinct.” \mathbb{R}^- et \mathbb{R}^+ sont distincts, mais pas disjoints. \mathbb{R}^{-*} et \mathbb{R}^{+*} sont distincts et disjoints.

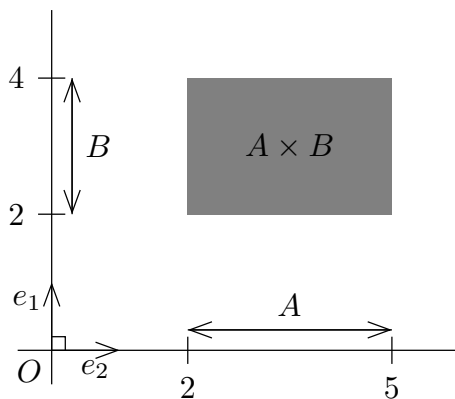
Exercice - Soient a, b et c des réels, avec $a \geq 0$. A quelle condition les sous-ensembles $]0, a[$, $] - \infty, b]$ et $[c, +\infty[$ forment-ils une partition de \mathbb{R} ?

6. Produit

Définition 1.8 - - Soient E et F deux ensembles, x un élément de E et y un élément de F . Le couple (x, y) est la donnée des deux éléments x et y dans cet ordre. Les éléments x et y sont appelés respectivement première et deuxième coordonnée du couple (x, y) . Deux couples (x, y) et (x', y') sont égaux si et seulement si on a $(x = x'$ et $y = y')$. Le produit cartésien $E \times F$ est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$.

Exemples -

- Si $E = F = \mathbb{R}$, le produit $\mathbb{R} \times \mathbb{R}$ est aussi noté \mathbb{R}^2 . On le représente souvent par l'ensemble des points du plan affine euclidien, en choisissant un repère orthonormé (O, e_1, e_2) . Le couple (x, y) est représenté par le point d'abscisse x et d'ordonnée y .
- Si $A = [2, 5]$ et $B = [2, 4]$, le produit $A \times B$ est un sous-ensemble de \mathbb{R}^2 qui peut être représenté par le rectangle sur la figure ci-dessous.



Remarques -

- Il ne faut pas confondre le couple (x, y) et l'ensemble $\{x, y\}$. Si $x \neq y$, on a $(x, y) \neq (y, x)$, mais $\{x, y\} = \{y, x\}$. Le couple (x, x) est représenté par un point de la première diagonale et l'ensemble $\{x, x\}$ est le singleton $\{x\}$.
- $A \subset E$ et $B \subset F$ si et seulement si $A \times B \subset E \times F$.
- Un produit cartésien de deux ensembles est vide si et seulement si l'un au moins des deux ensembles est vide.

Généralisation - Si on considère des ensembles E_1, E_2, \dots, E_n , on peut de même définir les n-uples (x_1, x_2, \dots, x_n) où $x_1 \in E_1, x_2 \in E_2, \dots, x_n \in E_n$

et le produit $E_1 \times E_2 \times \dots \times E_n$. En particulier, $\underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ facteurs}}$ est encore noté \mathbb{R}^n . De même, on note E^n l'ensemble $\underbrace{E \times \dots \times E}_{n \text{ facteurs}}$.

Exercice - 1°) Soit $A = B = \{1, 2\}$. Donner tous les sous-ensembles de $A \times B$.

2°) On considère les ensembles

$$E = \{1, 2, 3, 4\},$$

$$A = \{(i, j) \in E^2 \mid i < j\},$$

$$B = \{(i, j) \in E^2 \mid i = j\},$$

$$C = \{(i, j) \in E^2 \mid i > j\}$$

Les représenter par un dessin, et montrer que A, B et C forment une partition de $E \times E$.

EXERCICES D'APPLICATION

Exercice n°1

Soient $E = \mathbb{C}$, $A = \{z \in E \mid |z| \leq 1\}$ et $B = \{z \in E \mid \Re(z) < 1\}$. Représenter $\complement_E A$, $\complement_E B$, $A \cap B$, $A \cup B$, $A \setminus B$, $B \setminus A$ et $A \Delta B$.

Exercice n°2

Soient A , B et C des sous-ensembles d'un ensemble E . Les égalités suivantes sont-elles toujours vraies ? (Sinon, donner un contre-exemple)

- 1) $A \setminus (B \setminus C) = (A \setminus B) \setminus C$
- 2) $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$

Exercice n°3

Soient A , B , C et D des sous-ensembles d'un ensemble E . Montrer les égalités $A \setminus B = (A \cup B) \setminus B$ et $A \Delta B = (A \cap B^c) \cup (A^c \cap B)$.

Exercice n°4

Soient A , B et C des sous-ensembles d'un ensemble E .

- 1) Simplifier $(A \setminus C) \cup (B \setminus C) \cup (A \cup B)^c \cup C$.
- 2) Simplifier $(A \setminus (B^c \cup C)) \cup A^c \cup B^c \cup C$.

Exercice n°5

Soient A , B , C et D des sous-ensembles d'un ensemble E .

- 1) Montrer que l'on a $((A \cap B) \cup B^c = A \cup B^c)$ et $((A \setminus B) \cup B = A \cup B)$.
- 2) En déduire que l'on a $E = (C \setminus D) \cup (A \cap B \cap C^c) \cup A^c \cup B^c \cup D$.

Exercice n°6

Léon et Nicole travaillent dans un centre de lexicographie. Ils disposent de trois dictionnaires A , B et C . Leur patron donne à Léon le travail suivant : former d'abord une liste des mots communs aux dictionnaires A et B , former ensuite une liste de mots communs aux dictionnaires B et C , enfin chercher les mots qui figurent dans l'une ou l'autre liste, mais pas dans les deux à la fois. Léon demande à Nicole de l'aider en dressant une liste des mots figurant dans le dictionnaire A ou dans le dictionnaire C , mais pas dans les deux à la fois. Ensuite Léon se charge de trouver les mots communs à cette liste et au dictionnaire B .

Le patron obtiendra-t-il le résultat demandé ?

Exercice n°7

Soient E et F deux ensembles, A et B deux sous-ensembles de E et C et D deux sous-ensembles de F . Les égalités suivantes sont-elles toujours vraies ?

- 1) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.

2) $(A \times C) \setminus (B \times C) = (A \setminus B) \times C$.

Exercice n°8

Soient E et F deux ensembles. Un sous-ensemble X de $E \times F$ est-il toujours de la forme $A \times B$ où A appartient à $\mathcal{P}(E)$ et B appartient à $\mathcal{P}(F)$?

Exercice n°9

On suppose que les sous-ensembles A_1, A_2, A_3 et A_4 forment une partition de l'ensemble E . Combien y-a-t-il de façons de former une partition de E avec des sous-ensembles qui sont des réunions de certains des A_i ?

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°2

- 1) Non - Contre-exemple : $A = C = \mathbb{R}, B = \emptyset, A \setminus (B \setminus C) = \mathbb{R}, (A \setminus B) \setminus C = \emptyset$.
2) Non - Contre-exemple : $A = \mathbb{R}, B = C = \emptyset, A \cup (B \setminus C) = \mathbb{R}, (A \cup B) \setminus (A \cup C) = \emptyset$.

Exercice n°4

On trouve E .

Exercice n°6

Oui - Considérer A, B, C comme des ensembles (de mots) et utiliser la distributivité de \cap par rapport à Δ .

Exercice n°7

Oui.

Exercice n°8

Non - Contre-exemple : $E = F = \mathbb{R}$ et $X = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$.

Exercice n°9

15.

Chapitre 2

Eléments pour comprendre un énoncé

Ce chapitre est consacré à la *compréhension* d'un énoncé. Pour *démontrer* un énoncé donné, il faut se reporter au chapitre suivant.

Les tables de vérité données dans ce chapitre sont utiles pour connaître la valeur d'une proposition (dans quels cas est-elle vraie ou fausse), mais ne servent pas pour démontrer une proposition.

Un énoncé est parfois difficile à comprendre. Il peut contenir des mots utilisés dans un sens différent du sens courant ou des mots spécifiques au langage mathématique. S'il n'est pas écrit avec assez de soin, il peut devenir ambigu. Pour préciser ou mieux comprendre le sens d'un énoncé ou des mots employés, on s'efforce souvent de les écrire en utilisant des symboles mathématiques, des *et*, des *ou*, des \implies , des \iff , des \forall ou des \exists .

Exemples - Soit f une application de \mathbb{R} dans \mathbb{R} .

- L'énoncé "l'application f a un zéro entre -1 et 1" est ambigu : faut-il comprendre "un et un seul zéro" ou "au moins un zéro" ? 1 et -1 sont-ils admis ? Si on écrit $\exists x \in [-1, 1], f(x) = 0$, ces ambiguïtés sont levées.
- Dire que "la suite (u_n) converge vers ℓ " peut se traduire par :
$$\forall \varepsilon \in \mathbb{R}_+^*, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (n > N \implies |u_n - \ell| < \varepsilon).$$

L'intérêt de ce type d'écriture est de préciser la signification d'un énoncé complexe, mais il paraît parfois difficile à déchiffrer. Il faut être capable de bien comprendre le sens d'une telle formule, de la traduire en français et inversement de traduire sous cette forme un énoncé exprimé en français. L'objet de ce chapitre est de vous donner quelques éléments pour vous aider à y parvenir.

1. Propositions

Confronté à un énoncé, un mathématicien souhaite pouvoir décider dans quelles conditions il est vrai ou faux. Cet énoncé peut contenir une ou plusieurs variables. Nous appellerons *proposition* un énoncé mathématique dont on peut décider s'il est vrai ou faux lorsque toutes les variables ont été remplacées par des valeurs connues.

- Exemples** -
- " $2 \geq 1$ " est une proposition vraie.
 - " $1=2$ " est une proposition fausse.
 - Pour n entier, " $n \leq 6$ " est une proposition. Lorsque n est égal à 4, elle est vraie et lorsque n est égal à 7, elle est fausse.

- Si x et y sont des réels, " $x^2 = y$ " est une proposition.

A partir de propositions \mathbf{P} et \mathbf{Q} données, on peut définir de nouvelles propositions ($\text{non } \mathbf{P}$), (\mathbf{P} et \mathbf{Q}), (\mathbf{P} ou \mathbf{Q}), ($\mathbf{P} \implies \mathbf{Q}$), ($\mathbf{P} \iff \mathbf{Q}$), dont on connaît la valeur de vérité dès que l'on connaît celles de \mathbf{P} et \mathbf{Q} .

1.1. Négation

Définition 2.1 – Soit \mathbf{P} une proposition. La négation de \mathbf{P} est une proposition notée ($\text{non } \mathbf{P}$). Elle est vraie lorsque \mathbf{P} est fausse et fausse lorsque \mathbf{P} est vraie. On obtient la table de vérité suivante (où V est mis pour vraie et F pour fausse) :

\mathbf{P}	($\text{non } \mathbf{P}$)
V	F
F	V

Exemples - • Soit x un réel. La proposition ($\text{non } (x = 1)$) est notée ($x \neq 1$).
 • Soit n un entier naturel. La proposition ($\text{non } (n \leq 2)$) prend les mêmes valeurs de vérité que la proposition ($n > 2$).

Exercice - Déterminer l'ensemble des réels x qui vérifient la proposition :
 ($\text{non } (0 \leq x < 2)$)

1.2. Conjonction et disjonction


Définition 2.2 – Soient \mathbf{P} et \mathbf{Q} deux propositions.

- 1) La conjonction des deux propositions \mathbf{P} et \mathbf{Q} est une proposition notée (\mathbf{P} et \mathbf{Q}). Elle est vraie lorsque les deux propositions \mathbf{P} et \mathbf{Q} sont vraies, et elle est fausse lorsque l'une au moins des deux propositions est fausse.
- 2) La disjonction des deux propositions \mathbf{P} et \mathbf{Q} est une proposition notée (\mathbf{P} ou \mathbf{Q}). Elle est vraie lorsque l'une au moins des deux propositions \mathbf{P} ou \mathbf{Q} est vraie et elle est fausse lorsque les deux propositions \mathbf{P} et \mathbf{Q} sont fausses.

On peut résumer ce qui précède dans la table suivante :

\mathbf{P}	\mathbf{Q}	(\mathbf{P} et \mathbf{Q})	(\mathbf{P} ou \mathbf{Q})
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F


- Exemples -**
- Soient n un entier naturel, \mathbf{P} la proposition “ n est pair”, \mathbf{Q} la proposition “ n est divisible par 3”. Alors lorsque n est égal à 6, (\mathbf{P} et \mathbf{Q}) est vraie. Lorsque n est égal à 2, 3 ou 6, (\mathbf{P} ou \mathbf{Q}) est vraie.
 - Soient x un réel, \mathbf{P} la proposition ($x > 1$), \mathbf{Q} la proposition ($x \leq 2$). Alors, pour $x = 3/2$ la proposition (\mathbf{P} et \mathbf{Q}) est vraie, pour $x = 0$ elle est fautive et quelque soit la valeur de x , la proposition (\mathbf{P} ou \mathbf{Q}) est vraie.

 Dans le langage courant, le mot “ou” peut prendre deux sens différents : le sens inclusif qui est celui donné plus haut et le sens exclusif, qu’on précise parfois par “ou bien” : (\mathbf{P} ou bien \mathbf{Q}) est vraie si l’une des deux propositions est vraie et l’autre est fautive. Lorsque \mathbf{P} et \mathbf{Q} sont simultanément vraies, la proposition (\mathbf{P} ou \mathbf{Q}) est vraie, mais (\mathbf{P} ou bien \mathbf{Q}) est fautive. Nous n’utiliserons “ou” que dans le 1er sens.

*Exercice - Déterminer l’ensemble des réels x vérifiant la proposition :
 ($(x^2 > 1$ et $x < 2$) ou $(x^2 \leq 9$ et $x < 0$)).*

1.3. Implication

Définition 2.3 – Soient \mathbf{P} et \mathbf{Q} deux propositions. Alors ($\mathbf{P} \implies \mathbf{Q}$) est une proposition. Elle est fautive lorsque \mathbf{P} est vraie et \mathbf{Q} est fautive. Elle est vraie dans tous les autres cas. On l’énonce “ \mathbf{P} implique \mathbf{Q} ” ou “si \mathbf{P} , alors \mathbf{Q} ”. Elle s’énonce aussi “ \mathbf{P} entraîne \mathbf{Q} ”, “pour que \mathbf{P} , il faut que \mathbf{Q} ”, “pour que \mathbf{Q} , il suffit que \mathbf{P} ”, “une condition nécessaire pour que \mathbf{P} est que \mathbf{Q} ” ou “une condition suffisante pour que \mathbf{Q} est que \mathbf{P} ”.

 Dans le langage courant, on emploie souvent “il faut” à la place de “il suffit”. Par exemple, on dit “pour traverser la rivière, il faut prendre le bateau”, alors que c’est en fait suffisant, mais pas nécessaire. On peut le faire à la nage.

Proposition 2.4 – La proposition ($\mathbf{P} \implies \mathbf{Q}$) a la même table de vérité que la proposition ($(\text{non } \mathbf{P})$ ou \mathbf{Q}).

Exercice - Prouver cette proposition.

- Exemples -**
- Soit x un réel. Considérons la proposition ($x = 2 \implies x^2 = 4$). Si $x \neq 2$, elle est vraie, parce qu’alors la proposition ($x = 2$) est fautive et si $x = 2$ elle est vraie, parce qu’alors la proposition ($x^2 = 4$) est vraie. Cette proposition est donc toujours vraie. On l’énonce aussi “si x est égal à 2, alors x^2 est égal à 4”.

- La proposition $(x = 2 \implies 1 = 1)$ est vraie pour tout réel x , parce que $(1 = 1)$ est vraie, mais il faut bien dire qu'elle n'a pas beaucoup d'intérêt.
- Il en est de même pour la proposition $(1 = 0 \implies 2 = 3)$ qui est vraie, parce que la proposition $(1 = 0)$ est fausse.

⚠ L'affirmation précédente choque le sens courant. Cependant, on admet facilement que la proposition $(x + 1 = y \implies x + 3 = y + 2)$ est vraie pour tous les réels x et y ; et il suffit de prendre $x = y = 0$ pour obtenir $(1 = 0 \implies 2 = 3)$.

En fait, dans le langage courant, l'expression "**P** implique **Q**" a souvent un autre sens : elle sous-entend que **P** est vraie et permet d'affirmer que **Q** l'est aussi. Elle correspond donc en fait à $(\mathbf{P} \text{ et } (\mathbf{P} \implies \mathbf{Q}))$. Il faut de même se méfier de l'utilisation courante de "si" : la phrase "s'il fait beau, j'irai me promener" ou "j'irai me promener, s'il fait beau" sous-entend généralement "s'il ne fait pas beau, je n'irai pas me promener" (et correspond donc à une équivalence $((\mathbf{P} \implies \mathbf{Q}) \text{ et } (\mathbf{Q} \implies \mathbf{P}))$).

Exercice - Ecrire les implications suivantes en utilisant les symboles $\implies, \geq, >, \neq$ et dire si elles sont vraies pour tous les réels x .

1°) *Pour que x soit supérieur ou égal à 1, il faut que x soit strictement supérieur à 2.*

2°) *Pour que x soit supérieur ou égal à 1, il suffit que x soit strictement supérieur à 2.*

3°) *Une condition nécessaire pour que x soit supérieur ou égal à 1, est que x soit différent de 1.*

4°) *Si x est dans l'intervalle $[0, 1]$, alors $x^2 - 4x + 3$ est positif.*

1.4. Equivalence

Définition 2.5 – Soient **P** et **Q** deux propositions. Alors, $(\mathbf{P} \iff \mathbf{Q})$ est une proposition. Elle est vraie lorsque les propositions **P** et **Q** sont toutes les deux vraies ou toutes les deux fausses. Elle est fausse dans les autres cas. On l'énonce "**P** est équivalente à **Q**" ou "**P** et **Q** sont équivalentes". Cette proposition s'énonce aussi "**P** si et seulement si **Q**", "*pour que **P**, il faut et il suffit que **Q***", "*une condition nécessaire et suffisante pour que **Q** est que **P***".

Dire que **P** et **Q** sont équivalentes, c'est dire que ces propositions ont mêmes valeurs de vérité, c'est-à-dire qu'elles signifient la même chose.

Proposition 2.6 – Soient **P** et **Q** deux propositions. Alors, les deux propositions $(\mathbf{P} \iff \mathbf{Q})$ et $((\mathbf{P} \implies \mathbf{Q}) \text{ et } (\mathbf{Q} \implies \mathbf{P}))$ ont mêmes valeurs de vérité.

Pour le voir, on peut écrire la table de vérité suivante :

P	Q	(P\impliesQ)	(Q\impliesP)	(P\iffQ)
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

- Exemples -**
- Soit x un réel. La proposition $(x \geq 2 \iff x^2 \geq 4)$ est vraie pour tout $x \geq 0$, elle n'est pas toujours vraie lorsque $x < 0$ (par exemple, elle est fausse pour $x = -3$, vraie pour $x = -1$). Mais la proposition $(x \geq 2 \iff (x^2 \geq 4 \text{ et } x \geq 0))$ est vraie quelque soit x .
 - Soit n un entier naturel. On a vu que la proposition $(n > 2)$ est équivalente à la proposition $(\text{non}(n \leq 2))$.
 - Si **P** et **Q** sont deux propositions, on a vu que $(\mathbf{P} \implies \mathbf{Q})$ est équivalente à $((\text{non } \mathbf{P}) \text{ ou } \mathbf{Q})$.

Exercice - 1°) Soit x un réel. L'équivalence $(x^2 + |x| - 6 \leq 0 \iff -2 \leq x \leq 2)$ est-elle vraie ?

2°) Soit E l'ensemble des entiers naturels pairs. Peut-on caractériser les éléments de E par l'une des propositions suivantes ?

- 1) $x \in \mathbb{R}$ et $x/2 \in \mathbb{N}$.
- 2) $x \in \mathbb{R}$ et $2x \in \mathbb{N}$.
- 3) $x \in \mathbb{R}$ et x^2 est un entier pair.

2. Propositions avec des quantificateurs

Pour désigner une proposition qui contient une variable x , on adopte souvent une notation de la forme $\mathbf{P}(x)$ pour en faciliter la lecture et la compréhension.

- Exemples -**
- Pour n entier naturel, la proposition “ n est pair” pourra être notée $\mathbf{P}(n)$.
 - Si x et y sont des réels, “ $x \geq y$ ” pourra être notée $\mathbf{Q}(x, y)$.

Soit $\mathbf{P}(x)$ une proposition qui contient une variable x , où x désigne un élément de E . La valeur de vérité de $\mathbf{P}(x)$ peut dépendre de x et il est souvent important de savoir si elle est vraie pour tous les éléments x de E , pour au moins un, pour un et un seul... Les définitions suivantes précisent ceci.

Définition 2.7 – Soient E un ensemble et $\mathbf{P}(x)$ une proposition qui contient une variable x , où x désigne un élément de E .

- 1) La proposition $(\forall x \in E, \mathbf{P}(x))$ est vraie si la proposition $\mathbf{P}(x)$ est vraie pour tous les éléments x de E ; elle est fausse sinon. Elle se lit “quelque soit x de E , on a $\mathbf{P}(x)$ ”, ou “pour tout x de E , on a $\mathbf{P}(x)$ ”.
- 2) La proposition $(\exists x \in E, \mathbf{P}(x))$ est vraie s’il existe au moins un élément x de E tel que $\mathbf{P}(x)$ soit vraie ; elle est fausse sinon. Elle se lit “il existe au moins un x de E tel que $\mathbf{P}(x)$ ”.
- 3) La proposition $(\exists! x \in E, \mathbf{P}(x))$ est vraie s’il existe un élément x de E et un seul tel que $\mathbf{P}(x)$ soit vraie ; elle est fausse sinon. Elle se lit “il existe un et un seul x de E tel que $\mathbf{P}(x)$ ”.

Le symbole \forall est appelé quantificateur universel et \exists est appelé quantificateur existentiel.

- Exemples** -
- $(\forall x \in \mathbb{R}, x^2 \geq 0)$ est vraie.
 - $(\forall x \in \mathbb{R}, (x^2 = 1 \implies x = 1))$ est fausse.
 - $(\exists x \in \mathbb{R}, x^3 = 2)$ est vraie.
 - $(\exists! x \in \mathbb{R}, x^2 = 2)$ est fausse.

Remarque - On peut rapprocher les quantificateurs et connecteurs logiques *non*, *et*, *ou*, \implies et \iff des opérations ensemblistes : soient en effet A et B deux sous-ensembles d’un ensemble E . On a alors :

- 1) $\forall x \in E, (x \in \complement_E A \iff (\text{non } (x \in A)))$
- 2) $\forall x \in E, (x \in A \cap B \iff (x \in A \text{ et } x \in B))$
- 3) $\forall x \in E, (x \in A \cup B \iff (x \in A \text{ ou } x \in B))$
- 4) $A \subset B \iff \forall x \in E, (x \in A \implies x \in B)$
- 5) $A = B \iff \forall x \in E, (x \in A \iff x \in B)$

Proposition 2.8 – Soient E un ensemble, F un sous-ensemble de E et $\mathbf{P}(x)$ une proposition qui contient une variable x , où x désigne un élément de E .

- 1) La proposition $(\forall x \in E, (x \in F \implies \mathbf{P}(x)))$ est équivalente à la proposition $(\forall x \in F, \mathbf{P}(x))$.
- 2) La proposition $(\exists x \in E, (x \in F \text{ et } \mathbf{P}(x)))$ est équivalente à la proposition $(\exists x \in F, \mathbf{P}(x))$.

Exemples - Soit f une application de \mathbb{N} dans lui-même.

- La proposition $(\exists n \in \mathbb{N}, (n \neq 0 \text{ et } f(n) > 2))$ est équivalente à la proposition $(\exists n \in \mathbb{N}^*, f(n) > 2)$.
- De même, il est équivalent de dire $(\forall n \in \mathbb{N}, (n \neq 0 \implies f(n) > 2))$ ou $(\forall n \in \mathbb{N}^*, f(n) > 2)$.

⚠ ⚠ 1) L'expression "il existe un x tel que..." dans le langage courant est ambiguë, car elle signifie parfois "il existe exactement un x tel que...", (ce qui correspond au symbole $\exists!$). C'est pourquoi, on préfère préciser "il existe au moins un x tel que..." (c'est-à-dire un ou plusieurs) ou "il existe un et un seul x tel que..." (c'est-à-dire exactement un). On rencontre aussi l'expression "il existe au plus un x tel que..." qui veut dire "il n'existe pas de x tel que... ou il en existe exactement un".

2) Lorsqu'une proposition contient des quantificateurs \forall et \exists , leur ordre est essentiel.

Par exemple, la proposition $(\forall x \in \mathbb{R}, (\exists y \in \mathbb{R}, y = x^2))$ est vraie, mais la proposition

$(\exists y \in \mathbb{R}, (\forall x \in \mathbb{R}, y = x^2))$ est fausse.

3) Les propositions $(\forall x \in E, \mathbf{P}(x))$ et $(\exists x \in E, \mathbf{P}(x))$ ne traduisent pas des propriétés de x , mais de l'ensemble E ; on dit que x est une variable muette. On obtient une proposition équivalente en remplaçant partout x par une autre lettre. Mais il est plus prudent de choisir une lettre qui n'a pas déjà été utilisée.

Exercice - 1°) Soit $(u_n)_{n \in \mathbb{N}}$ une suite de réels. Traduire avec des quantificateurs la propriété " $(u_n)_{n \in \mathbb{N}}$ est bornée".

2°) Soit f une application de \mathbb{R} dans \mathbb{R} . Traduire par une phrase la proposition suivante $\forall A \in \mathbb{R}, \exists x \in \mathbb{R}, f(x) > A$.

3°) Soit f une application de \mathbb{R} dans \mathbb{R} . Donner une proposition ne contenant plus le signe \implies équivalente à la proposition $(\forall x \in \mathbb{R}, ((x \geq 0 \text{ et } x \leq 1) \implies f(x) = 1))$.

3. Négation d'une proposition

Proposition 2.9 – Soient \mathbf{P} et \mathbf{Q} des propositions. Les équivalences suivantes sont toujours vraies :

- 1) $(\text{non}(\text{non } \mathbf{P})) \iff \mathbf{P}$.
- 2) $(\text{non}(\mathbf{P} \text{ et } \mathbf{Q})) \iff ((\text{non } \mathbf{P}) \text{ ou } (\text{non } \mathbf{Q}))$.
- 3) $(\text{non}(\mathbf{P} \text{ ou } \mathbf{Q})) \iff ((\text{non } \mathbf{P}) \text{ et } (\text{non } \mathbf{Q}))$.
- 4) $(\text{non}(\mathbf{P} \implies \mathbf{Q})) \iff (\mathbf{P} \text{ et } (\text{non } \mathbf{Q}))$.
- 5) $(\mathbf{P} \implies \mathbf{Q}) \iff ((\text{non } \mathbf{Q}) \implies (\text{non } \mathbf{P}))$.

Exercice - Vérifier la proposition précédente en écrivant une table de vérité.

Proposition 2.10 – Soient E un ensemble et $\mathbf{P}(x)$ une proposition qui contient une variable x , x désignant un élément de E . On a les équivalences suivantes :

- 1) $(\text{non } (\forall x \in E, \mathbf{P}(x))) \iff \exists x \in E, (\text{non } \mathbf{P}(x))$
- 2) $(\text{non } (\exists x \in E, \mathbf{P}(x))) \iff \forall x \in E, (\text{non } \mathbf{P}(x))$

Exemple - Les règles précédentes peuvent se combiner. Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres réels. Par définition, $(u_n)_{n \in \mathbb{N}}$ est une suite convergente si l'on a :

$$\exists l \in \mathbb{R}, \forall \varepsilon \in \mathbb{R}_+^*, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (n \geq N \implies |u_n - l| < \varepsilon).$$

La négation de cette proposition est :

$$\forall l \in \mathbb{R}, \exists \varepsilon \in \mathbb{R}_+^*, \forall N \in \mathbb{N}, \exists n \in \mathbb{N}, (n \geq N \text{ et } |u_n - l| \geq \varepsilon).$$

Exercice - 1°) Soient $I \subset \mathbb{R}$ un intervalle et f une application de I dans \mathbb{R} . Exprimer les propositions suivantes à l'aide de quantificateurs et donner leur négation.

- a) *L'application f n'est pas de signe constant sur I .*
- b) *L'application f est majorée sur I .*
- c) *L'intervalle I est inclus dans $]1, 2[$.*

*2°) Ecrire la négation de la proposition
 (($x^2 \geq 1$ et $x^3 < 2$) ou ($x^2 \leq 9$ et $x < 0$)).*

4. Quelques conseils pratiques

Lorsque l'on écrit une proposition en utilisant le langage formalisé que nous venons de décrire, il faut être sûr que ce que l'on écrit a bien le sens voulu. Donnons quelques indications en ce sens.

- 1) On n'est pas obligé de tout formaliser. Souvent, une formalisation partielle est plus lisible et permet de mieux contrôler le sens. Par exemple, la proposition "le carré de tout nombre entier naturel impair est impair" peut être partiellement formalisée par :

$$(\forall x \in \mathbb{N}, (x \text{ est impair} \implies x^2 \text{ est impair}))$$

ce qui est préférable à la formalisation complète :

$$(\forall x \in \mathbb{N}, ((\forall y \in \mathbb{N}, x \neq 2y) \implies (\forall z \in \mathbb{N}, x^2 \neq 2z))).$$

- 2) Cependant, une des principales difficultés pour formaliser correctement une proposition est que les quantificateurs sont trop souvent implicites en français. Pensez à les restituer. Par exemple, si l'on donne le système

$$\begin{cases} x - y + 2z = a \\ 3x + 5y + z = b \end{cases}$$
 et si on pose la question "ce système a-t-il des solutions réelles pour tous les réels a et b ?", il faut étudier si la proposition

$\forall(a, b) \in \mathbb{R}^2, \exists(x, y, z) \in \mathbb{R}^3, \begin{cases} x - y + 2z = a \\ 3x + 5y + z = b \end{cases}$ est vraie. Or on trouve

souvent “il faut regarder si $\begin{cases} x - y + 2z = a \\ 3x + 5y + z = b \end{cases}$ ”, ce qui est voué à l’échec :

qui sont les données ? Qui sont les inconnues ?

- 3) Une définition résume par un mot ou une expression une proposition qui peut être assez complexe. Pour comprendre un énoncé, il est indispensable de savoir traduire les définitions utilisées. Par exemple, si l’énoncé contient la phrase “soient E un ensemble, A un sous-ensemble de E et $B = E \setminus A$ ”, on traduira : $B = \{x \in E \mid x \notin A\}$.

- 4) La formalisation ayant pour objectif de clarifier la signification des propositions en les précisant, il est évidemment inefficace et dangereux d’écrire des propositions de façon approximative. En particulier, l’oubli des parenthèses crée de graves ambiguïtés.

Par exemple, que signifie $(\exists x \in \mathbb{R}, x^2 = y \implies y < 0)$? Faut-il comprendre $(\exists x \in \mathbb{R}, (x^2 = y \implies y < 0))$ ou $((\exists x \in \mathbb{R}, x^2 = y) \implies y < 0)$?

- 5) On a vu que l’ordre dans lequel apparaissent les symboles \forall et \exists est important. Laissez-les à leur place. Par exemple, écrire “ $f(x) > 0, \forall x \in \mathbb{R}$ ”, donne la négation “ $f(x) \leq 0, \exists x \in \mathbb{R}$ ”, qui ne veut plus rien dire.

EXERCICES D'APPLICATION

Exercice n°1

Ecrire avec des quantificateurs les propriétés suivantes

- 1) Une suite réelle $(u_n)_{n \in \mathbb{N}}$ a pour limite $+\infty$.
- 2) Si tout élément x d'un ensemble E est un élément de l'ensemble F , E est inclus dans F .

Exercice n°2

Soient x et y deux réels, écrire la négation des propositions suivantes :

- 1) $0 < x \leq 1$
- 2) $xy = 0$
- 3) $x^2 = 1 \Rightarrow x = 1$

Exercice n°3

Soient E un ensemble et $\mathbf{P}(x)$ une proposition qui contient une variable x , x désignant un élément de E . Ecrire avec des quantificateurs une proposition qui signifie "il y a au plus un x tel que $\mathbf{P}(x)$ " et une proposition qui signifie "il y a exactement deux x tels que $\mathbf{P}(x)$ ".

Exercice n°4

La proposition suivante est-elle vraie ? Ecrire sa négation.

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \exists z \in \mathbb{Z}, \exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}, (x = zu \text{ et } y = zv)$$

Exercice n°5

Soient f et g deux applications de \mathbb{R} dans \mathbb{R} . Les propositions suivantes sont-elles vraies ?

- 1) $(\forall x \in \mathbb{R}, f(x)g(x) = 0) \iff [(\forall x \in \mathbb{R}, f(x) = 0) \text{ ou } (\forall x \in \mathbb{R}, g(x) = 0)]$.
- 2) $(\forall x \in \mathbb{R}, f^2(x) + g^2(x) = 0) \iff [(\forall x \in \mathbb{R}, f(x) = 0) \text{ et } (\forall x \in \mathbb{R}, g(x) = 0)]$.

Exercice n°6

- 1) Indiquer si chacune des propositions suivantes est vraie lorsque $E = \mathbb{N}$.
 - a) $\forall x \in E, \exists y \in E, y < x$
 - b) $\exists y \in E, \forall x \in E, y < x$
 - c) $\forall x \in E, \exists y \in E, y + x = 0$
- 2) Même question si $E = \mathbb{Z}$.

Exercice n°7

Pour tous réels x et y , on note $P(x, y)$ la proposition $x + y^2 = 0$. Les propositions suivantes sont-elles vraies ?

- 1) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$
- 2) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, P(x, y)$
- 3) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$
- 4) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, P(x, y)$
- 5) $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, P(x, y)$.

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°1

- 1) $\forall A > 0, \exists n \in \mathbb{N}, \forall n \in \mathbb{N}, (n \geq N \implies u_n \geq A)$
- 2) $(\forall x \in E, x \in F) \implies (E \subset F)$

Exercice n°2

- 1) $x \leq 0$ ou $x > 1$
- 2) $x \neq 0$ et $y \neq 0$
- 3) $x^2 = 1$ et $x \neq 1$

Exercice n°3

$[((\exists x \in E, \mathbf{P}(x)) \text{ et } (\forall y \in E, (\mathbf{P}(y) \implies x = y)))]$ ou $(\forall x \in E, \text{non } P(x))$.
 $(\exists(x, y) \in E \times E, (x \neq y \text{ et } \mathbf{P}(x) \text{ et } \mathbf{P}(y) \text{ et } (\forall z \in E, (\mathbf{P}(z) \implies (z = x \text{ ou } z = y))))))$

Exercice n°4

La proposition est vraie. Elle signifie que deux entiers quelconques ont toujours un diviseur commun (par exemple 1).
Sa négation est

$$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, \forall z \in \mathbb{Z}, \forall u \in \mathbb{Z}, \forall v \in \mathbb{Z}, (x \neq zu \text{ ou } y \neq zv)$$

Exercice n°5

- 1) Faux. Un contre-exemple est donné par :
 $f(x) = 0$ si $x < 0$ et $f(x) = 1$ si $x \geq 0$
 $g(x) = 0$ si $x \geq 0$ et $g(x) = 1$ si $x < 0$
- 2) Vrai.

Exercice n°6

- 1-a) Faux b) Faux c) Faux
- 2-a) Vrai b) Faux c) Vrai

Exercice n°7

- 1) Faux : $x = y = 1$
- 2) Faux : $x = 1$
- 3) Faux
- 4) Vrai
- 5) Vrai : $x = y = 0$

Chapitre 3

Eléments pour comprendre et écrire des démonstrations

Une des tâches essentielles en mathématique est de chercher à s'assurer que telle ou telle proposition est vraie ou fausse. Il ne suffit pas de bien la comprendre pour cela. Par exemple, Pierre de Fermat a énoncé vers 1640 le théorème qui porte son nom depuis : “si n est un entier strictement supérieur à 2, il n'existe pas d'entiers non nuls a, b, c tels que $a^n + b^n = c^n$ ”. Le sens de cet énoncé est parfaitement clair, mais il a cependant fallu attendre plus de trois siècles pour être sûr qu'il était vrai, grâce à la démonstration d'Andrew Wiles (1994).

Pour s'assurer de la vérité d'une proposition, les mathématiciens écrivent des textes spécifiques, appelés *démonstrations*. Ces textes sont souvent complexes, ce qui explique que de nombreuses erreurs soient commises par les débutants. Ils mettent en oeuvre un certain nombre de règles dont la connaissance est le plus souvent seulement implicite, ce qui rend la compréhension et la correction de ses erreurs difficiles. Ils s'articulent autour de la distinction entre *propositions données* (encore appelées *hypothèses*) et *propositions à démontrer*, qui n'est pas toujours clairement perçue.

Tout ceci explique qu'il soit difficile d'apprendre à rédiger soi-même une démonstration. L'objet de ce chapitre est de vous y aider. Pour cela, on va d'abord donner quelques éléments pour mieux comprendre la structure des démonstrations. Puis, on donnera quelques stratégies pour trouver une démonstration, des exemples de problèmes à résoudre et enfin quelques conseils de rédaction.

1. Pour comprendre la structure d'une démonstration

Quand on rédige une démonstration, la proposition que l'on cherche à démontrer s'appelle la *conclusion*. Au cours de la démonstration, on utilise des résultats déjà connus, par exemple, des définitions, des théorèmes ou des propositions déjà démontrés dans le cours ; mais aussi les prémices offerts par l'énoncé ou des résultats intermédiaires que l'on a obtenus préalablement. Toutes ces propositions s'appellent des *données*.

Une des raisons de la complexité des démonstrations est que l'on peut être amené pendant la démonstration à ajouter provisoirement de nouvelles données qui ne font pas partie de celles dont nous venons de parler et aussi de nouveaux objets qui ne sont pas décrits dans l'énoncé. Leur introduction est signalée par des expressions comme “Supposons que ...”, “Soit ...”, “Considérons...”.

Il faut aussi noter qu'une démonstration ne contient pas que des propositions vraies. L'exemple le plus évident en est celui des raisonnements par l'absurde où l'on ajoute aux données une proposition ($\text{non}(A)$) afin de montrer que c'est A qui est vraie.

Les paragraphes suivants essaieront d'expliquer tout ceci, en explicitant les principales règles d'écriture sous-jacentes. Ils permettront de mieux comprendre les différents statuts des propositions qui apparaissent dans un texte de démonstration.

1.1. Règle de l'hypothèse auxiliaire

Beaucoup d'énoncés sont du type "Montrer que si l'on a \mathbf{P} , alors on a \mathbf{Q} ", c'est-à-dire "démontrer ($\mathbf{P} \implies \mathbf{Q}$)".

Dans la pratique, on commence souvent en écrivant "on suppose \mathbf{P} ", c'est-à-dire que l'on considère \mathbf{P} comme une nouvelle donnée, puis on cherche à démontrer \mathbf{Q} . La démonstration s'achève par une phrase du genre "on a montré \mathbf{Q} " et il peut être bon de prendre la peine de rappeler la conclusion globale "on a montré ($\mathbf{P} \implies \mathbf{Q}$)". On peut expliciter cette démarche par la règle suivante :

Pour démontrer ($\mathbf{P} \implies \mathbf{Q}$) :

- 1) on ajoute \mathbf{P} aux données.
- 2) on démontre que \mathbf{Q} est vraie.

Exemple

- *Énoncé* - Soit n un entier. Montrer que si n est pair, alors n^2 est pair.
- *Démonstration* - On suppose que n est pair. Par définition d'un nombre pair, on peut donc écrire $n = 2k$ où k est un entier. On en déduit $n^2 = 4k^2$, donc $n^2 = 2k'$ où $k' = 2k^2$. Donc n^2 est pair.
On a montré que si n est pair, alors n^2 l'est aussi.
- *Commentaire* - Soient \mathbf{P} la proposition " n est pair" et \mathbf{Q} la proposition " n^2 est pair". La proposition à démontrer est "si \mathbf{P} , alors \mathbf{Q} ", c'est-à-dire ($\mathbf{P} \implies \mathbf{Q}$). La première ligne de la démonstration revient à ajouter \mathbf{P} aux données, le deuxième paragraphe démontre \mathbf{Q} , le troisième est la conclusion.

Exercice - Soit n un entier naturel. Montrer que si n est impair, alors n^2 est impair.

1.2. Règle du quel que soit

On a aussi très souvent à montrer une proposition du type ($\forall x \in E, \mathbf{P}(x)$). Dans la pratique, on commence en écrivant une expression du style "Soit x un élément de E ", ou "Considérons un élément x de E ", puis on écrit une démonstration de $\mathbf{P}(x)$. Lorsque cette démonstration est un peu longue, on peut l'encadrer par l'annonce "On va montrer qu'on a $\mathbf{P}(x)$ " et la conclusion

partielle “On a montré $\mathbf{P}(x)$ ”. On peut ajouter la conclusion globale “On a montré $(\forall x \in E, \mathbf{P}(x))$ ”. Cette démarche peut être explicitée par la règle suivante :

Pour démontrer $(\forall x \in E, \mathbf{P}(x))$:

- 1) on choisit une lettre x qui n’a pas déjà été utilisée ailleurs et on ajoute la donnée $x \in E$;
- 2) on démontre que $\mathbf{P}(x)$ est vraie.

Exemple

- *Énoncé* - Montrer que pour tout x de \mathbb{R} , on a $(x > 1 \implies x^2 + x + 1 > 3)$.
- *Démonstration* - Soit x un nombre réel.
Supposons $x > 1$. On a alors $x^2 > 1$. On en déduit $x^2 + x + 1 > 1 + 1 + 1$, c’est à dire $x^2 + x + 1 > 3$.
On a bien le résultat.
- *Commentaire* - Ici $\mathbf{P}(x)$ est la proposition $(x > 1 \implies x^2 + x + 1 > 3)$. Le premier alinea correspond au point 1. La proposition $\mathbf{P}(x)$ est une implication de la forme $(\mathbf{P}_1 \implies \mathbf{Q}_1)$. Pour la démontrer, on utilise la règle de l’hypothèse auxiliaire, en ajoutant \mathbf{P}_1 aux données (on a écrit “Supposons que l’on a $x > 1$ ”) et on démontre \mathbf{Q}_1 . Les deux premières phrases reviennent à ajouter les données “ x réel” et “ $x > 1$ ”. On aurait pu les condenser en écrivant “Soit x un réel tel que $x > 1$ ”.

Exercice - Démontrer que pour tout réel x , on a $(x > 2 \implies 2e^x + x^2 - 3x > 0)$.

1.3. Règle des cas

Pour démontrer une proposition \mathbf{P} , on peut vouloir se servir d’une proposition déjà démontrée de la forme $(\mathbf{A} \text{ ou } \mathbf{B})$. Pour cela :

- 1) on suppose \mathbf{A} vraie et on démontre \mathbf{P} ;
- 2) on suppose \mathbf{B} vraie (sans hypothèse sur \mathbf{A}) et on démontre \mathbf{P} .

La règle peut être annoncée au début par une phrase du genre “il y a deux cas”, ou mise en évidence par deux paragraphes, un pour chaque cas ; le point 1 se traduit par une expression du genre “supposons \mathbf{A} ”, le point 2 par “supposons maintenant \mathbf{B} ” ou “dans le cas où \mathbf{B} ”.

On applique souvent la règle des cas en prenant pour proposition \mathbf{B} une proposition équivalente à $(\text{non } \mathbf{A})$; (en effet, $\mathbf{A} \text{ ou } (\text{non } \mathbf{A})$ fait partie des propositions vraies, quel que soit \mathbf{A}). Le point 2 se réduit alors à supposer $(\text{non } \mathbf{A})$ vraie et se traduit par “dans le cas où $(\text{non } \mathbf{A})$ ”.

Exemple

- *Énoncé* - Soient x, y, λ des nombres réels, avec $\lambda < 0$.
Montrer que l’on a $\max(\lambda x, \lambda y) = \lambda \min(x, y)$.
- *Démonstration* - Il y a deux cas : le cas $x \leq y$ et le cas $x > y$;

Supposons d'abord $x \leq y$. Alors comme on a $\lambda < 0$, on a $\lambda x \geq \lambda y$, donc $\max(\lambda x, \lambda y) = \lambda x$. D'autre part, on a $\min(x, y) = x$.

On a donc bien $\max(\lambda x, \lambda y) = \lambda \min(x, y)$.

On suppose maintenant $x > y$. Alors comme on a $\lambda < 0$, on a $\lambda x < \lambda y$, donc $\max(\lambda x, \lambda y) = \lambda y$. D'autre part, on a $\min(x, y) = y$.

On a donc encore $\max(\lambda x, \lambda y) = \lambda \min(x, y)$.

Dans les deux cas, on a l'égalité demandée.

- *Commentaire* - La proposition A est la proposition $x \leq y$ et la proposition B est $x > y$ qui est équivalente à (*non* \mathbf{A}). Les deux cas sont clairement annoncés dans le premier alinea. Ils sont successivement traités dans les deux paragraphes suivants. Les deux points sont seulement suggérés par la succession "d'abord", "maintenant". La dernière ligne est la conclusion.

Exercice - Montrer que pour tout réel x , $(\sqrt{x^2} = 2x + 3 \implies x = -1)$.

1.4. Nommer un objet

Pour démontrer une proposition \mathbf{Q} en utilisant une donnée de la forme $(\exists x \in E, \mathbf{P}(x))$:

- 1) on choisit une lettre x_0 par exemple, qui n'a pas été déjà utilisée et surtout qui n'apparaît pas dans la proposition \mathbf{Q} ;
- 2) on ajoute aux hypothèses la proposition $(x_0 \in E \text{ et } \mathbf{P}(x_0))$;
- 3) on démontre \mathbf{Q} .

En pratique, les points 1 et 2 sont traduits par une expression de la forme "Soit x_0 un élément de E tel que $\mathbf{P}(x_0)$ " ou "On sait que $(\exists x \in E, \mathbf{P}(x))$; soit x_0 un tel élément". Il est souvent bon de justifier le "On sait que" par la référence à une définition ou à un théorème.

Exemple

- *Enoncé* - Soit a un réel. Montrer que si $([0, 1] \cap [a - 1/2, a + 1/2] \neq \emptyset)$, alors $-1/2 \leq a \leq 3/2$.
- *Démonstration* - Soit $E = [0, 1] \cap [a - 1/2, a + 1/2]$. On suppose que E est non vide. Soit x_0 un élément de cet ensemble. On a donc $0 \leq x_0 \leq 1$ et $a - 1/2 \leq x_0 \leq a + 1/2$, d'où $0 \leq x_0 \leq a + 1/2$ et $a - 1/2 \leq x_0 \leq 1$. On en déduit $0 \leq a + 1/2$ et $a - 1/2 \leq 1$, d'où $-1/2 \leq a \leq 3/2$. On a bien le résultat demandé.
- *Commentaire* - Dire que E est non vide, c'est dire $(\exists x \in E)$. On utilise la règle "nommer un objet" en considérant l'un des éléments de E (il peut y en avoir beaucoup) et en l'appelant x_0 . Les inégalités vérifiées par x_0 permettent de contrôler a .

Exercice - Montrer que tout entier multiple de 6 est multiple de 2.

1.5. Raisonnement par l'absurde

Principe - On veut démontrer **P**. Pour cela :

- 1) on ajoute (*non P*) aux données ;
- 2) on démontre qu'on a à la fois **Q** et (*non Q*) pour une certaine proposition **Q**.

En pratique, le point 1 s'exprime en disant "supposons (*non P*)". La démonstration contient souvent des phrases au conditionnel. La fin du raisonnement par l'absurde est indiquée par une expression comme "Il y a contradiction" ou "C'est impossible". On peut annoncer "Raisonnons par l'absurde" et conclure "On a donc **P**".

Exemple

- *Enoncé* - Montrer que 0 n'est pas racine de $A(x) = x^4 + 12x - 1$.
- *Démonstration* - On raisonne par l'absurde. Supposons que 0 soit racine de A . Par définition, on aurait donc $A(0) = 0$; or le calcul montre que $A(0) = -1$, d'où $-1 = 0$. On obtient une contradiction.
- *Commentaire* - La proposition **P** est ici "0 n'est pas racine du polynôme A " et (*non P*) est "0 est racine de A " ; la proposition **Q** n'est pas précisée, ce pourrait être ($-1 \neq 0$).

Exercice - Soit f l'application de $[1, +\infty[$ dans \mathbb{R} définie, pour $x \geq 1$, par $f(x) = \sqrt{x-1} + \sqrt{x+1}$. Montrer en utilisant un raisonnement par l'absurde que f n'est pas dérivable au point 1.

1.6. Raisonnement par contraposition

La proposition ($(\text{non Q}) \Rightarrow (\text{non P})$) est appelée la *contraposée* de la proposition ($\text{P} \Rightarrow \text{Q}$). Elle lui est équivalente.

Pour démontrer ($\text{P} \Rightarrow \text{Q}$), on peut donc démontrer ($(\text{non Q}) \Rightarrow (\text{non P})$).

Exemple

- *Enoncé* - Soit x un nombre réel. Montrer que $(x^3 = 2 \Rightarrow x < 2)$.
- *Démonstration* - On suppose $x \geq 2$. On a donc $x^3 \geq 8$ et en particulier $x^3 \neq 2$. On a donc bien le résultat.
- *Commentaire* - Ici, **P** est la proposition ($x^3 = 2$) et **Q** la proposition ($x < 2$). La contraposée est donc la proposition ($x \geq 2 \Rightarrow x^3 \neq 2$). On lui applique la règle de l'hypothèse auxiliaire en disant "on suppose $x \geq 2$ ".

On aurait pu annoncer au début "On va raisonner par contraposition, c'est-à-dire démontrer ($x \geq 2 \Rightarrow x^3 \neq 2$).". On a sous-entendu cette phrase, car l'exemple proposé est assez simple pour que le lecteur la restitue lui-même.

Exercice - Montrer que pour tout entier n , si n^2 est pair, alors n est pair.

1.7. Pour démontrer une équivalence

Pour démontrer $(\mathbf{P} \iff \mathbf{Q})$:

- on peut démontrer d'abord $(\mathbf{P} \implies \mathbf{Q})$, puis $(\mathbf{Q} \implies \mathbf{P})$, (la proposition $(\mathbf{Q} \implies \mathbf{P})$ est appelée la *réciproque* de $(\mathbf{P} \implies \mathbf{Q})$).
- on peut aussi démontrer d'abord $(\mathbf{P} \implies \mathbf{Q})$, puis $(\text{non } \mathbf{P}) \implies (\text{non } \mathbf{Q})$ (qui est la *contraposée* de $(\mathbf{Q} \implies \mathbf{P})$).

Exemple

- *Enoncé* - Montrer que pour tout x réel, $(\sqrt{2x^2 + 2} = 3 + x)$ est équivalent à $(x \in \{-1, 7\})$.

- *Démonstration* - Soit x un réel.

Supposons que $(\sqrt{2x^2 + 2} = 3 + x)$. En élevant les deux membres au carré, on obtient $2x^2 + 2 = (3 + x)^2 = x^2 + 6x + 9$. Donc x est racine de l'équation du second degré $x^2 - 6x - 7 = 0$. On obtient donc $(x \in \{-1, 7\})$.

Réciproquement, supposons $(x \in \{-1, 7\})$. Dans le cas où $x = -1$, on a $2x^2 + 2 = 4$, donc $\sqrt{2x^2 + 2} = 2$, et $3 + x = 2$ donc $\sqrt{2x^2 + 2} = 3 + x$. Lorsque $x = 7$, on a $2x^2 + 2 = 100$, donc $\sqrt{2x^2 + 2} = 10$, et $3 + x = 10$ donc $\sqrt{2x^2 + 2} = 3 + x$.

On a bien démontré l'équivalence cherchée.

- *Commentaire* - L'énoncé contient l'expression "pour tout x réel" ; il est de la forme $(\forall x \in \mathbb{R}, (\mathbf{P}(x) \iff \mathbf{Q}(x)))$, où $\mathbf{P}(x)$ est la proposition $(\sqrt{2x^2 + 2} = 3 + x)$ et $\mathbf{Q}(x)$ la proposition $(x \in \{-1, 7\})$.

A la première ligne, la phrase "Soit x un réel" signale l'utilisation de la règle du quel que soit. Ensuite, on démontre $(\mathbf{Q}(x) \iff \mathbf{P}(x))$.

Au premier paragraphe, on montre $(\mathbf{P}(x) \implies \mathbf{Q}(x))$. Le deuxième commence par "Réciproquement", qui annonce qu'on va montrer $(\mathbf{Q}(x) \implies \mathbf{P}(x))$ et pour cela on utilise la règle des cas.

Autre exemple :

- *Enoncé* - Montrer que l'entier n est pair si et seulement si n^2 est divisible par 4.

- *Démonstration* - Supposons n pair, on peut écrire $n = 2k$ où k est un entier ; alors on a $n^2 = 4k^2$, donc on a $n^2 = 4k'$ où $k' = k^2$. Donc n^2 est divisible par 4.

Réciproquement, supposons que n est impair ; on peut écrire $n = 2k + 1$ où k est un entier ; alors on a $n^2 = 4k^2 + 4k + 1$; le reste de la division de n^2 par 4 est égal à 1, donc n^2 n'est pas divisible par 4.

- *Commentaire* - Ici, \mathbf{P} est la proposition "n est pair" et \mathbf{Q} est la proposition " n^2 est divisible par 4". Au premier paragraphe, on a montré $(\mathbf{P} \implies \mathbf{Q})$. Au deuxième, on a montré $(\text{non } \mathbf{P} \implies \text{non } \mathbf{Q})$

Exercice - 1°) Compléter la première démonstration en ajoutant des phrases de conclusion.

2°) Dans la deuxième démonstration, on a utilisé implicitement la règle “nommer un objet”. Repérer à quels endroits. Compléter la démonstration pour la rendre plus explicite.

- ⚠ • Ne pas confondre la réciproque d’une proposition ($\mathbf{P} \implies \mathbf{Q}$) qui est ($\mathbf{Q} \implies \mathbf{P}$) avec sa contraposée qui est ($(\text{non } \mathbf{Q}) \implies (\text{non } \mathbf{P})$).
- Pour démontrer une équivalence, beaucoup d’étudiants utilisent systématiquement une suite d’équivalences. Bien sûr, cela est légitime s’il s’agit de vraies équivalences. Mais le plus souvent les propositions qu’elles font intervenir contiennent des quantificateurs sous-entendus, qu’on a tendance à oublier, ce qui conduit à la faute. Il faut en règle générale rester prudent dans l’utilisation des équivalences, (voir l’exercice d’application n°5 pour un exemple).

1.8. Pour démontrer (\mathbf{Q} ou \mathbf{R})

Dans le cas où \mathbf{Q} est vraie, (\mathbf{Q} ou \mathbf{R}) est automatiquement vraie. On suppose donc \mathbf{Q} fausse et on montre que \mathbf{R} est vraie, c’est-à-dire que l’on montre ($(\text{non } \mathbf{Q}) \implies \mathbf{R}$).

Remarque - Les propositions (\mathbf{Q} ou \mathbf{R}) et (\mathbf{R} ou \mathbf{Q}) sont équivalents. Il peut être plus simple de prendre la négation de \mathbf{R} que de \mathbf{Q} .

Exemple

- *Énoncé* - Soit n un entier. Montrer que n est impair ou n^2 est pair.
- *Démonstration* - On suppose que n n’est pas impair, c’est à dire que n est pair. Soit k un entier tel que $n = 2k$. On a $n^2 = 4k^2$, donc $n^2 = 2k'$ où $k' = 2k^2$. Donc n^2 est pair. On a donc bien n impair ou n^2 pair.
- *Commentaire* - La proposition à démontrer est de la forme (\mathbf{Q} ou \mathbf{R}) où \mathbf{Q} est la proposition “ n est impair ” et \mathbf{R} la proposition “ n^2 est pair”. \mathbf{Q} est fausse est introduit par “On suppose que n n’est pas impair”.

1.9. Raisonnement par récurrence

On note \mathbb{N} l’ensemble des entiers naturels.

Le raisonnement par récurrence s’applique aux propositions dont l’énoncé dépend d’un entier naturel n . Il est une conséquence de la construction de l’ensemble des entiers naturels \mathbb{N} (basée sur les axiomes de Peano). Ce raisonnement peut prendre différentes formes.

• RECURRENCE SIMPLE

C’est le type le plus utilisé. Si les hypothèses suivantes sont vérifiées

- la propriété est vraie en n_0 ,
- lorsque la propriété est vraie pour $k \geq n_0$, elle est vraie pour $k + 1$,

alors la propriété est vraie pour tout entier $n \geq n_0$.

Exercice - Montrer que, pour tout entier naturel n , $2^n > n$.

• **RECURRENCE FORTE**

C'est la forme la plus générale du raisonnement par récurrence. Si les hypothèses suivantes sont vérifiées

- la propriété est vraie en n_0 ,
- lorsque la propriété est vraie pour tout entier p tel que $n_0 \leq p \leq k$, elle est vraie pour $k + 1$,

alors la propriété est vraie pour tout entier $n \geq n_0$.

Exercice - Soit $(x_n)_n$ la suite réelle définie par

$$x_0 = 1$$

$$x_{n+1} = x_0 + x_1 + \dots + x_n \text{ pour tout entier } n \geq 0.$$

Montrer que, pour tout entier naturel n , $x_n \leq 2^n$.

Remarques - • Définissez clairement l'hypothèse de récurrence, donnez-lui un nom qui mette en évidence qu'elle dépend d'un entier.

- Si l'hypothèse de récurrence ne vous est pas donnée, il faut essayer de la découvrir avec les cas $n = n_0$, $n = n_0 + 1, \dots$

SOMME ET PRODUIT

Soit p et q deux entiers naturels avec $p \leq q$ et f une application de \mathbb{N} dans \mathbb{C} . On note

$\sum_{i=p}^q f(i)$ la somme des nombres $f(i)$ lorsque i varie de p à q :

$$\sum_{i=p}^q f(i) = f(p) + f(p+1) + \dots + f(q-1) + f(q).$$

$\prod_{i=p}^q f(i)$ le produit de ces mêmes termes :

$$\prod_{i=p}^q f(i) = f(p) \times f(p+1) \times \dots \times f(q-1) \times f(q).$$

Remarques - • $\sum_{i=p}^q f(i) = \sum_{j=p}^q f(j)$.

- $\sum_{i=1}^n f(i) = \sum_{i=1}^{n-1} f(i) + f(n)$.

Exemples - • $\sum_{i=1}^n 1 = n$
 • $\prod_{i=1}^n 1 = 1$

Remarque - La récurrence ne sert pas qu'à démontrer certaines propriétés sur l'ensemble des entiers naturels ; elle permet de donner des définitions. Par exemple, le symbole \sum est défini de manière correcte par

$$\text{pour } q - p = 0 \quad \sum_{i=p}^q f(i) = f(p)$$

$$\text{si } q \geq p \geq 0 \quad \sum_{i=p}^{q+1} f(i) = \sum_{i=p}^q f(i) + f(q+1)$$

Exemple - Pour n entier naturel, calculer la somme

$$S_n = \sum_{i=0}^n (2i + 1).$$

On peut commencer par étudier les cas $n = 1, n = 2$, etc. On trouve $S_0 = 1, S_1 = 4, S_2 = 9$ et on peut deviner que l'on a $S_n = (n + 1)^2$ pour tout n . Reste à le vérifier en écrivant une démonstration de cette proposition.

• *Démonstration* - On va montrer que pour tout entier n , on a :

$$\sum_{i=0}^n (2i + 1) = (n + 1)^2.$$

Pour n entier naturel, notons S_n la somme

$$S_n = \sum_{i=0}^n (2i + 1).$$

et $\mathbf{P}(n)$ la propriété $S_n = (n + 1)^2$. Il faut montrer que $\mathbf{P}(n)$ est vraie pour tout n . On procède par récurrence sur n .

Montrons que $\mathbf{P}(0)$ est vraie. Pour $n = 0$, on a :

$$S_0 = \sum_{i=0}^0 (2i + 1) = 1 \quad \text{et} \quad (n + 1)^2 = 1.$$

Donc $\mathbf{P}(0)$ est vraie.

Soit k un entier tel que $\mathbf{P}(k)$ est vraie ; montrons qu'alors $\mathbf{P}(k + 1)$ est vraie. L'hypothèse est $S_k = (k + 1)^2$ et on veut montrer que l'on a $S_{k+1} = (k + 2)^2$. Or on a :

$$S_{k+1} = \sum_{i=0}^{k+1} (2i + 1) = S_k + (2k + 3).$$

En utilisant l'hypothèse, on obtient :

$$S_{k+1} = (k + 1)^2 + (2k + 3) = k^2 + 4k + 4 = (k + 2)^2.$$

Donc $\mathbf{P}(k + 1)$ est vraie.

On a donc montré que $\mathbf{P}(n)$ est vraie pour tout n , ce qui est équivalent au résultat cherché. • *Commentaire* - L'utilisation d'une récurrence permet très souvent de répondre à ce type de question. Il faut prendre la peine de bien préciser l'hypothèse de récurrence, de lui donner un nom (ici $\mathbf{P}(n)$) et de bien signaler les étapes. Il faut également faire attention au démarrage : vérifiez que le passage de k à $k + 1$ marche dès le départ et qu'il n'y ait pas un cas particulier pour $n_0, n_0 + 1, \dots$

Exercice - 1°) Montrer, par récurrence sur n , que $\sum_{i=1}^n i = n(n+1)/2$.

2°) Démontrer la formule du binôme :

pour tous les complexes a et b , $(a + b)^n = \sum_{i=0}^n C_n^i a^i b^{n-i}$ avec

$$C_n^i = \frac{n!}{i!(n-i)!}.$$

1.10. D'autres règles

Il y a beaucoup d'autres règles qui peuvent intervenir dans une démonstration. Par exemple, la règle dite du *modus ponens* : "si on a \mathbf{P} et $(\mathbf{P} \implies \mathbf{Q})$, alors on a \mathbf{Q} ", ou des *sylogismes* : "si on a $(\forall x \in E, \mathbf{P}(x))$ et si a est un élément de E , alors on a $\mathbf{P}(a)$ ". L'exemple célèbre de syllogisme est "Tous les hommes sont mortels et Socrate est un homme ; donc Socrate est mortel." Nous ne décrivons pas davantage ces règles, car leur utilisation est simple et occasionne généralement peu de fautes.

Exercice - Expliciter le syllogisme précédent à l'aide de quantificateurs.

2. Pour trouver une démonstration

Bien sûr, on ne peut pas rédiger une démonstration complète d'un énoncé lorsque l'on n'a aucune idée des raisons qui font que cet énoncé est vrai. Cependant, même lorsqu'on a bien compris ces raisons, il peut être difficile de rédiger une bonne démonstration. A l'inverse, pour trouver des idées qui conduisent à une solution, il est souvent efficace de commencer à écrire une démonstration, même si au départ, on ne sait pas encore comment on va la terminer. Il y a donc complémentarité entre la recherche de la solution d'un problème et l'écriture de textes qui pourraient devenir une démonstration. Pour débiter une démonstration, il faut d'abord bien examiner la structure de la proposition à démontrer. Il y a en effet de nombreuses stratégies possibles, et cela aidera à en choisir une qui soit bien adaptée.

2.1. On peut décider d'aborder le problème directement.

- 1) Lorsque la proposition est de la forme $(\mathbf{P} \implies \mathbf{Q})$, on applique la règle de l'hypothèse auxiliaire, on commence le texte par "Supposons que \mathbf{P} " et le nouvel objectif est de démontrer \mathbf{Q} .
- 2) Lorsque la proposition est de la forme $(\forall x \in E, \mathbf{P}(x))$, on utilise la règle du "quel que soit". On commence par "Soit $x \in E$, démontrons $\mathbf{P}(x)$ ".
- 3) Lorsque la proposition est de la forme $(\exists x \in E, \mathbf{P}(x))$, il s'agit de trouver un élément x_0 qui vérifie $\mathbf{P}(x_0)$. Le premier travail sera d'essayer de deviner quel élément pourrait convenir.
- 4) Lorsque la proposition est de la forme $(\mathbf{P} \text{ et } \mathbf{Q})$, on démontre successivement \mathbf{P} puis \mathbf{Q} . On commence par écrire "Démontrons d'abord \mathbf{P} ", puis dans un autre paragraphe "Démontrons maintenant \mathbf{Q} ."
- 5) Lorsque la proposition est de la forme $(\mathbf{P} \text{ ou } \mathbf{Q})$, il suffit de démontrer l'une des deux propositions ; lorsque l'on essaie de trouver une démonstration, on s'aperçoit parfois que l'une des propositions paraît plus facile à démontrer que l'autre ; c'est elle que l'on pourra alors décider d'essayer de démontrer.

Exemple

- *Énoncé* - Montrer qu'il existe un réel x tel que
$$\sqrt{x^2 - x + 9} > \sqrt{x^2 + x + 4}.$$
- *Démonstration* - On prend $x = 0$; on a $x^2 - x + 9 = 9$ et $x^2 + x + 4 = 4$, donc $\sqrt{x^2 - x + 9} = 3$ et $\sqrt{x^2 + x + 4} = 2$. Or, $3 > 2$, donc 0 convient.

Autre exemple :

- *Énoncé* - Montrer que pour tous les réels x et y , on a $||x| - |y|| \leq |x - y|$.
- *Démonstration* - Soient x et y deux réels. On doit démontrer que

$$|x| - |y| \leq |x - y| \text{ et } |y| - |x| \leq |x - y|.$$

Démontrons d'abord la première proposition. On a $|x| = |(x - y) + y|$ donc par l'inégalité triangulaire $|x| \leq |x - y| + |y|$ et on en déduit $|x| - |y| \leq |x - y|$.

Pour la deuxième proposition, on a de même $|y| \leq |y - x| + |x|$ et on en déduit $|y| - |x| \leq |y - x|$.

On a bien le résultat cherché.

- *Commentaire* - Les réels x et y ayant été fixés, on a à démontrer une proposition du genre $(\mathbf{P}(x, y) \text{ et } \mathbf{Q}(x, y))$. On aurait pu choisir de démontrer $(\forall (x, y) \in \mathbb{R}^2, \mathbf{P}(x, y))$ puis $(\forall (x, y) \in \mathbb{R}^2, \mathbf{Q}(x, y))$. Pour démontrer la deuxième proposition, il aurait alors suffi d'utiliser la première en y remplaçant partout le couple (x, y) par le couple (y, x) .

2.2. On peut utiliser des moyens indirects.

- 1) On peut commencer un raisonnement par l'absurde.
- 2) On peut décider de démontrer la contraposée de la proposition demandée.
- 3) On peut introduire des cas, (en particulier lorsque l'on dispose d'une hypothèse de la forme $(\mathbf{A} \text{ ou } \mathbf{B})$).

- 4) On peut utiliser des méthodes spécifiques au domaine concerné : par exemple, une démonstration par récurrence pour une proposition de la forme $(\forall n \in \mathbb{N}, \mathbf{P}(n))$, ou l'utilisation de tableaux de variations lorsque la proposition concerne une fonction de la variable réelle etc.
- 5) On peut obtenir le résultat d'un seul coup par un théorème approprié.

Exemple

- *Enoncé* - Soit $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$
 $x \longmapsto \ln x + 1/x - 2$. Montrer que f s'annule en un point x de \mathbb{R}_+^* au moins.
- *Démonstration* - L'application f est continue et $f(1) = -1$. L'image de f contient l'intervalle $f(1), \lim_{x \rightarrow +\infty} f(x)[$, c'est à dire $[-1, +\infty[$. Donc 0 est dans l'image de f , ce qui veut dire qu'il existe un x de \mathbb{R}_+^* tel que $f(x) = 0$.
- *Commentaire* - La proposition que l'on veut démontrer est de la forme $(\exists x \in \mathbb{R}_+^*, f(x) = 0)$. Il n'y a pas de zéro évident. On utilise une propriété des fonctions continues (l'image d'un intervalle par une fonction continue est un intervalle).

2.3. On peut essayer de se ramener à une proposition plus simple.

Par exemple, pour démontrer une proposition du genre $(\mathbf{P} \implies \mathbf{Q})$ dans beaucoup de cas, on peut simplifier la démonstration car on a de façon évidente (par un théorème ou une définition) $(\mathbf{P} \iff \mathbf{P}')$ et $(\mathbf{Q}' \iff \mathbf{Q})$; on se ramène donc à prouver $(\mathbf{P}' \implies \mathbf{Q}')$.

Exemple

- *Enoncé* - Soit x un réel strictement positif. Montrer que si l'on a $x^2 - 3x \geq 0$, alors on a $x^2 + 8 \geq 5x + 4/x$.
- *Démonstration* - On a $x^2 - 3x = x(x-3)$, donc comme x est strictement positif, $x^2 - 3x$ est positif si et seulement si x est supérieur à 3. D'autre part, en multipliant les deux membres de l'inégalité $(x^2 + 8 \geq 5x + 4/x)$ par le réel strictement positif x on obtient l'inégalité équivalente $(x^3 + 8x \geq 5x^2 + 4)$; celle-ci est encore équivalente à $(x^3 - 5x^2 + 8x - 4 \geq 0)$. Or on a $x^3 - 5x^2 + 8x - 4 = (x-1)(x^2 - 4x + 4) = (x-1)(x-2)^2$.
 On se ramène donc à démontrer que si l'on a $x \geq 3$, alors on a $(x-1)(x-2)^2 \geq 0$, ce qui est évident.
- *Commentaire* - Notons respectivement $\mathbf{P}(x)$, $\mathbf{P}'(x)$, $\mathbf{Q}(x)$ et $\mathbf{Q}'(x)$ pour $x > 0$ les propositions $x^2 - 3x \geq 0$, $x \geq 3$, $(x^2 + 8 \geq 5x + 4/x \geq 0)$ et $(x-1)(x-2)^2 \geq 0$.
 On a montré les équivalences $(\mathbf{P}(x) \iff \mathbf{P}'(x))$ et $(\mathbf{Q}'(x) \iff \mathbf{Q}(x))$; l'implication $(\mathbf{P}'(x) \implies \mathbf{Q}'(x))$ est ici évidente. Tout ceci permet de conclure que l'on a $(\mathbf{P}(x) \implies \mathbf{Q}(x))$.

⚠ Lorsque l'on part comme ici de la proposition à démontrer Q , il faut être certain d'assurer le 'retour' et pour cela il faut faire bien attention à procéder par équivalences. Une faute fréquente est de commencer par écrire "si on a Q , alors on a Q ", ce qui consiste à prendre la conclusion cherchée comme hypothèse. Même si l'on démontre ensuite que P entraîne Q' , cela ne prouve rien sur la proposition à démontrer $P \implies Q$.

3. Quelques types de problèmes à résoudre

3.1. Résultats sur les ensembles

Ces résultats sont souvent faciles à obtenir en adoptant une stratégie très liée à la formule que l'on veut démontrer. Par exemple, si A et B sont deux sous-ensembles d'un ensemble E , et si on demande de démontrer $A \subset B$, il s'agit de montrer $(\forall x \in A, x \in B)$. On commence par écrire "Soit x un élément de A ; montrons que x appartient à B ". Si on demande de démontrer $A = B$, on peut démontrer successivement $(A \subset B)$ et $(B \subset A)$.

Exemple

- *Énoncé* - Soient A et B deux sous-ensembles d'un ensemble E . Montrer que l'on a $(A \subset B \implies E \setminus B \subset E \setminus A)$.
- *Démonstration* - Supposons que $A \subset B$ et montrons que $E \setminus B \subset E \setminus A$, c'est-à-dire que $(\forall x \in E \setminus B, x \in E \setminus A)$. Soit donc x un élément de $E \setminus B$. Par définition, x appartient à E et x n'appartient pas à B . On veut montrer que x n'appartient pas à A . Raisonnons par l'absurde et supposons que x appartienne à A . Alors l'hypothèse $A \subset B$ montre que $x \in B$. Il y a contradiction.
Donc $x \in E \setminus A$.
- *Commentaire* - On voit bien que cette démonstration est complètement guidée à chaque étape par la forme de la proposition que l'on cherche à démontrer, sauf lorsqu'on a introduit un raisonnement par l'absurde.

3.2. Énoncés d'analyse

Les énoncés d'analyse contiennent souvent beaucoup de quantificateurs, (par exemple, quand on parle d'une application de \mathbb{R} dans \mathbb{R} , le quantificateur $\forall x \in \mathbb{R}$ apparaît presque toujours). On utilise donc très fréquemment les règles du "quel que soit" (pour le quantificateur \forall) et "nommer un objet" (pour le quantificateur \exists). Il faut bien expliciter dans la démonstration ce que désignent les lettres que l'on y introduit, et être attentif à leur ordre d'apparition qui doit correspondre à l'ordre des quantificateurs. En effet, beaucoup d'erreurs viennent d'une interversion de deux quantificateurs ou d'une mauvaise quantification qui masque le fait qu'une variable dépend d'une autre.

Exemple

- *Enoncé* - Montrer que si une application de \mathbb{R} dans \mathbb{R} est bornée, alors son carré l'est aussi.
- *Démonstration* - Soit f une application bornée de \mathbb{R} dans \mathbb{R} . Montrer que f^2 est bornée, c'est trouver un majorant de $|f^2|$, c'est-à-dire un réel M tel que $(\forall x \in \mathbb{R}, |f^2(x)| \leq M)$.
On sait que f est bornée. Considérons un majorant M_0 de $|f|$. Soit x un réel. On a $|f(x)| \leq M_0$, donc $|f(x)^2| \leq M_0^2$.
On a donc montré que $(\forall x \in \mathbb{R}, |f^2(x)| \leq M_0^2)$, c'est-à-dire que M_0^2 est un majorant de $|f^2|$; donc f^2 est bornée. On a bien le résultat demandé.
- *Commentaire* - On utilise la règle du "quel que soit" en introduisant f . On examine la proposition qui reste à démontrer (" f^2 bornée") et on la traduit. On utilise la règle "nommer un objet" en introduisant M_0 . L'existence de M_0 est justifiée par le rappel de l'hypothèse " f bornée" et la définition d'une application bornée. C'est après avoir fixé M_0 qu'on réutilise la règle du "quel que soit" en introduisant x . Ainsi, on est sûr que M_0 ne dépend pas du choix de x . Une erreur fréquente est d'écrire "Soit x un réel. Soit M_0 un réel tel que $|f(x)| \leq M_0$ etc" En effet, M_0 et donc M_0^2 dépendent alors a priori de x ; on peut prendre $M_0 = |f(x)^2|$ par exemple, ce qui ne donnera évidemment pas du tout le résultat cherché.

3.3. Résolution d'équations.

Dans ce type de problème, on a souvent à raisonner en deux temps : l'analyse du problème puis la synthèse. On a intérêt à donner un nom, S par exemple, à l'ensemble des solutions. Dans l'analyse, on suppose que x est solution et on essaye de préciser x . Pratiquement, on montre $S \subset S'$, où S' est un ensemble dont on connaît explicitement les éléments, ou qui en donne du moins une description simple. Dans la synthèse, on regarde si réciproquement $S' \subset S$.

Exemple

- *Enoncé* - Résoudre dans \mathbb{R} l'équation $x = \sqrt{x} + 2$.
- *Démonstration* - Notons S l'ensemble des solutions.
Analyse - Soit $x \in S$. L'équation doit avoir un sens et donc il faut $x \geq 0$. D'autre part, on a $\sqrt{x} = x - 2$. En élevant cette dernière équation au carré, on obtient $x = x^2 - 4x + 4$, d'où $x^2 - 5x + 4 = 0$. Les solutions de cette nouvelle équation sont 1 et 4 qui sont toutes les deux positives. Donc $S \subset \{1, 4\}$.
Synthèse - Soit $x = 4$; \sqrt{x} a un sens, et $\sqrt{x} + 2 = 4 = x$, donc $4 \in S$. Soit $x = 1$; on a $\sqrt{x} + 2 = 3 \neq x$. Donc $1 \notin S$. On obtient donc $S = \{4\}$. Il y a une et une seule solution qui est 4.
- *Commentaire* - On a pris soin ici de vérifier que la formule a un sens. C'est un réflexe à acquérir et dans beaucoup de problèmes, cela permet d'éliminer certaines solutions dès le stade de l'analyse et simplifie la synthèse.

3.4. Contre-exemples

Supposons qu'on pose la question ouverte "la proposition $(\forall x \in E, \mathbf{P}(x))$ est elle vraie ?"

Si l'on trouve un x de E tel que $\mathbf{P}(x)$ soit fausse, alors on peut affirmer que la proposition est fausse. On dit qu'on a trouvé un contre-exemple. (Par contre, si on trouve des x tels que la proposition soit vraie, au mieux, on peut se convaincre qu'elle est toujours vraie et avoir une idée de la façon d'aborder la démonstration, mais on n'a rien démontré.)

Exemple - A-t-on $(\forall x \in \mathbb{R}, \sqrt{x^2 - x + 9} \leq \sqrt{x^2 + x + 4})$?

La réponse est non. En effet, si on prend $x = 0$, on obtient $x^2 - x + 9 = 9$ et $x^2 + x + 4 = 4$, donc $\sqrt{x^2 - x + 9} = 3$ et $\sqrt{x^2 + x + 4} = 2$. Or, on a $3 > 2$. Donc 0 fournit un contre-exemple.

Pour répondre à cette question, il est inutile de chercher à déterminer quels sont exactement les x qui vérifient $\sqrt{x^2 - x + 9} \leq \sqrt{x^2 + x + 4}$. Une erreur fréquente est de se contenter d'écrire :

"Soit x un réel.

Si $\sqrt{x^2 - x + 9} \leq \sqrt{x^2 + x + 4}$, alors on a $x^2 - x + 9 \leq x^2 + x + 4$, donc $2x + 5 \leq 0$. Or ceci est faux." En effet, la proposition $(2x + 5 \leq 0)$ n'est pas toujours fausse. Il faudrait ajouter "Pour $x = 0$ par exemple, on a $(2x + 5 = 5)$ qui est strictement positif."

4. Quelques conseils pour résoudre un problème et écrire une démonstration.

Pour parvenir à résoudre un problème, il faut commencer par bien comprendre le texte. Ensuite, on peut commencer à chercher une solution et essayer de démarrer un texte de démonstration. Quand on a compris, il reste à rédiger une démonstration rigoureuse.

4.1. Pour bien lire le texte

Il ne faut pas hésiter à formaliser toutes les propositions de l'énoncé que l'on juge peu claires ou complexes. Il faut en particulier restituer les quantificateurs sous-entendus dans le texte, se rappeler et traduire les définitions des mots utilisés. On peut aussi introduire des notations pour préciser le texte. Il faut bien repérer ce qui est donné et ce que l'on cherche à démontrer.

4.2. Pour chercher une solution.

Tous les moyens sont bons ! On peut essayer de démarrer une démonstration au vu de la structure de la proposition à démontrer ou de la forme des hypothèses, comme on l'a dit plus haut. On peut essayer de voir les liens entre hypothèses et conclusion, se rappeler les théorèmes qui ont un rapport avec l'une ou l'autre, tirer des conséquences élémentaires des définitions et des hypothèses. Il ne faut pas hésiter parallèlement à essayer des exemples, à faire des dessins. On peut aussi se rappeler la solution d'un problème analogue.

Si on est 'coincé', il faut vérifier qu'on n'a pas oublié ou affaibli une hypothèse (en utilisant seulement une conséquence de cette hypothèse, qui contient moins d'informations qu'elle) ou que la clé de la solution ne se trouve pas à la question précédente.

4.3. Pour rédiger une démonstration.

Annoncez ce que vous allez faire et donnez vos conclusions (en disant "on va montrer que ..." , "on va raisonner par l'absurde", "on a montré que ..."). Cela permet de structurer les démonstrations et de les rendre plus claires. C'est aussi un bon moyen pour ne pas se tromper. Vous pouvez aussi admettre provisoirement un résultat dont la démonstration semble difficile ou ennuyeuse ("supposons qu'on ait démontré que... , alors...").

N'hésitez à être assez explicite et à détailler les étapes au début. Même si cela donne des démonstrations trop longues, ne cherchez pas à les raccourcir avant d'avoir acquis assez d'aisance pour écrire des démonstrations exactes qui soient plus courtes.

Fixez vos notations. Il ne faut pas hésiter à introduire des notations pour préciser le texte, mais elles doivent être expliquées clairement.

En particulier, on voit que dans la rédaction d'une démonstration peu de quantificateurs apparaissent dans le corps du texte (par exemple, si l'on utilise les règles du "quel que soit" et "nommer un objet", on élimine les \forall et \exists). En revanche, on est amené à introduire de nouvelles lettres (en disant par exemple "soit x tel que ...") Il est indispensable d'être très explicite sur le statut de ces lettres, c'est-à-dire sur les objets qu'elles représentent et les propriétés qu'elles possèdent. De façon générale, il faut se donner pour règle de *vérifier à chaque fois qu'une lettre apparait dans une démonstration, qu'elle a été convenablement "déclarée"*, c'est-à-dire que son statut a été clairement précisé. Les fautes les plus fréquentes et les plus dangereuses sont dues à l'oubli de cette règle. Par exemple, écrire $\ln(x) = 2$ sans avoir précisé que x est un réel strictement positif est inadmissible, écrire " e^x est toujours positif" conduira (pour un θ réel) à " $e^{i\theta} \geq 0$ ", ce qui ne veut plus rien dire. Ecrivez par exemple, "soit x un réel strictement positif tel que $\ln(x) = 2$ " ou "pour tout x réel, e^x est positif".

Justifiez les étapes de votre démonstration. Pour cela citez les théorèmes utilisés et rappelez les définitions. Vérifiez que les formules que vous écrivez ont un sens, ce qui vous aidera souvent à mieux préciser le statut des lettres utilisées et vous permettra d'éviter certains pièges. En particulier, validez les petits calculs qui posent souvent problème (division d'une égalité, multiplication d'une inégalité par une constante, changement de variable etc). Par exemple, $(x^2 > 1 \implies x > 1)$ n'est pas vraie pour tout réel x ; même si les hypothèses précisent que x est positif, rappelez-le à cet endroit, cela vous évitera d'oublier le cas x négatif ou nul une autre fois.

Refusez les abus de langage. Une partie de l'énoncé peut être formalisée (par exemple “si $n = 2$, alors $n^2 = 4$ ”), mais vous devez pouvoir restituer une phrase intelligible en énonçant la partie formalisée ($n = 2$ s'énonce “ n est égal à 2”). N'utilisez pas le symbole \implies comme abréviation de “donc” ni \iff comme abréviation de “ce qui est équivalent à”, ni \forall et \exists comme abréviations de “pour tout” et “il existe”. Tant que les démonstrations sont simples ces abus de langage ont peu de conséquences, mais pour une démonstration compliquée, ils rendent le texte incompréhensible ou engendrent des fautes. Par exemple, la rédaction suivante est correcte :

“on a $x > 2$ et on sait que si $x > 2$, alors $x^2 \neq 1$; on en déduit $2x^2 \neq 2$.”

On peut l'abrégé en :

“on a $x > 2$, donc $x^2 \neq 1$ et donc $2x^2 \neq 2$.”

Mais la rédaction suivante est inadmissible car illisible :

“ $x > 2$ et $x > 2 \implies x^2 \neq 1 \implies 2x^2 \neq 2$.”

et celle-ci (où les \implies ont probablement été mis pour “donc”) énonce un résultat généralement faux (lequel ?) :

$(x > 2 \implies x^2 \neq 1) \implies 2x^2 \neq 2$.

On peut se donner pour règle de *ne pas remplacer les mots qui articulent le texte par des symboles*.

Relisez-vous toujours quand vous pensez avoir fini, pour contrôler s'il n'y a pas d'erreur et améliorer vos explications. Il peut y avoir beaucoup de démonstrations d'un même problème ; en vous relisant, vous trouverez peut-être moyen de simplifier la vôtre.

EXERCICES D'APPLICATION

Exercice n°1

On demande de montrer que pour tout entier n tel que $n \geq 3$, si n est premier, alors n est impair. On propose la démonstration suivante :

“Soit n un entier tel que $n \geq 3$.

Démontrons que si n est pair, n n'est pas premier, ce qui est équivalent au résultat demandé.

Supposons n pair.

Alors n est divisible par 2 et comme on a $n \geq 3$, n n'est pas premier.”

- 1) Formalisez l'énoncé (en gardant les expressions “ n premier” et “ n impair”).
- 2) Quelles règles utilise-t-on dans chacun des trois premiers alinéas ?
- 3) Compléter la dernière ligne pour la rendre plus explicite.
- 4) Quelles données y utilise-t-on ?
- 5) Quelle conclusion peut-on tirer des alinéas 3 et 4 ?

Exercice n°2

On a demandé de montrer que $(\forall x \in \mathbb{R}_+^*, (x + 1/x) \geq 2)$. Pourquoi le raisonnement ci-dessous a-t-il valu la note zéro à son auteur ?

“Si $(x + 1/x) \geq 2$, on a $x^2 + 1 \geq 2x$, donc $x^2 - 2x + 1 \geq 0$. Or, $x^2 - 2x + 1 = (x - 1)^2$ qui est positif. On a bien le résultat demandé.”

Pouvez-vous écrire une démonstration correcte ?

Exercice n°3

Voici un énoncé : “Soit E un ensemble non vide et A, B et C trois sous-ensembles non vides de E . Montrer que : $A\Delta B = A\Delta C \implies B = C$ ”.

On propose le texte incomplet suivant :

“..... $A\Delta B = A\Delta C$; Pour montrer que $B = C$, ilde montrer que $B \subset C$ et $C \subset B$ $x \in B$ $x \in A$, $x \notin A$.
..... x appartient à A , $x \in A \cap B$, $x \notin A\Delta B$.
..... $A\Delta B = A\Delta C$, $(A \setminus C) \subset A\Delta C$, $x \notin (A \setminus C)$
et $x \in A$, $x \in C$ x n'appartient pas à A ,
..... $x \in A \cup B$ et $x \notin A \cap B$, $x \in A\Delta B = A\Delta C$
 $x \notin A$; que $x \in C \setminus A$; encore $x \in C$. On a donc montré
que Le problème étant symétrique en B et C , $C \subset B$.
..... $B = C$.”

- 1) Compléter ce texte pour en faire une démonstration et séparer-le en paragraphes pour rendre sa structure plus claire :
- 2) Les hypothèses “non vides” ont-elles servi ?

Exercice n°4

On considère l'énoncé suivant : "l'application $f : \begin{matrix} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{matrix}$ est-elle surjective?" (pour la définition de "surjective" voir la section 5.5. du polycopié).

Trouver la faute dans le raisonnement suivant :

"Soit y un réel ; il y a deux cas : le cas $y \geq 0$ et le cas $y < 0$.

Lorsque $y \geq 0$, l'équation $y = x^2$ a deux solutions $x = \sqrt{y}$ et $x = -\sqrt{y}$; donc f est surjective.

Dans le cas où $y < 0$, l'équation $y = x^2$ n'a pas de solution ; donc f n'est pas surjective.

On conclut que f est surjective si $y \geq 0$ et f n'est pas surjective sinon."

Exercice n°5

On propose le texte suivant :

Énoncé -

Soient $u = (a, b)$ et $u' = (a', b')$ deux vecteurs de \mathbb{R}^2 . Les deux vecteurs u et u' sont proportionnels si et seulement si $ab' - a'b = 0$.

Démonstration -

Dire que u et u' sont proportionnels est équivalent à dire qu'il existe un réel k tel que $u = k.u'$, c'est-à-dire ($a = ka'$ et $b = kb'$), ce qui se traduit par :

- si $a' \neq 0$, $k = \frac{a}{a'}$ donc $b = \frac{a}{a'}b'$ et $ab' - a'b = 0$.

- si $a' = 0$, alors $a = 0$ et donc aussi $ab' - a'b = 0$.

Finalement, on a bien l'équivalence annoncée. "

Cette "démonstration" n'en est pas une. Pourquoi ?

Exercice n°6

Montrer par récurrence que, pour tout entier $n \geq 2$,

$$\sum_{k=1}^n k(k-1) = \frac{n(n-1)(n+1)}{3}.$$

Exercice n°7

Soient a et b deux réels tels que $(\forall \varepsilon \in \mathbb{R}_+^*, \quad a < b + \varepsilon)$.

Montrer, en utilisant un raisonnement par l'absurde, qu'alors $a \leq b$.

Exercice n°8

Soit \mathcal{F} l'ensemble des fonctions définies sur \mathbb{R} et à valeurs dans \mathbb{R} . A-t-on :

$$\forall (f, g) \in \mathcal{F} \times \mathcal{F}, \quad (fg = 0 \implies (f = 0 \text{ ou } g = 0)) \quad ?$$

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°1

- 1) L'énoncé peut se traduire par :
 $\forall n \in \{m \in \mathbb{N} \mid m \geq 3\} (n \text{ premier} \implies n \text{ impair})$
ou encore par :
 $\forall n \in \mathbb{N}, (n \geq 3 \implies (n \text{ premier} \implies n \text{ impair}))$
- 2) - "Soit n un entier tel que $n \geq 3$." : On utilise la règle du "quel que soit" ;
- "Démontrons que si n est pair, n n'est pas premier, ce qui est équivalent au résultat demandé" : On annonce que l'on va démontrer la contraposée de la proposition ($n \text{ premier} \implies n \text{ impair}$) ;
- "Supposons n pair." : On utilise la règle de l'hypothèse auxiliaire.
- 3) On peut compléter en disant : "par définition d'un nombre pair, n est divisible par 2. Comme $n \geq 3$, 2 est un diviseur de n qui est différent de 1 et de n . La définition d'un nombre premier montre que n n'est pas premier."
- 4) On utilise les données suivantes : " n est pair", la définition de " n pair" (qui est " n est divisible par 2"), " $n \geq 3$ " et la définition de " n est premier" (qui est " n n'a pas de diviseur différent de 1 et de n ").
- 5) La conclusion des deux derniers alinéas est "si n est pair, n n'est pas premier".

Exercice n°2

Une démonstration correcte serait :

"Soit $x \in \mathbb{R}_+^*$. Comme x est strictement positif, l'inégalité à démontrer est équivalente à l'inégalité obtenue en multipliant ses deux membres par x , c'est-à-dire : $(x^2 + 1 \geq 2x)$. Celle-ci est encore équivalente à $(x^2 - 2x + 1 \geq 0)$. Or, $(x^2 - 2x + 1)$ est égal à $(x - 1)^2$, qui est positif. La dernière inégalité est donc vraie et on a bien le résultat demandé."

Le raisonnement proposé comporte trois fautes :

- il néglige de préciser qui est x ,
- il oublie de préciser que l'on a $x > 0$ pour valider la transformation de la première inégalité en la seconde,
- et surtout il ne démontre pas grand chose ! En effet, ce qu'il démontre est :
 $\forall x \in \mathbb{R}_+^*, ((x + 1/x) \geq 2 \implies (x - 1)^2 > 0)$.

Mais la proposition $((x - 1)^2 > 0)$ étant vraie pour tout réel x , une implication du style $(\mathbf{P}(x) \implies (x - 1)^2 > 0)$ est vraie que $\mathbf{P}(x)$ soit vraie ou fausse.

Exercice n°3

- 1) On suppose que $A\Delta B = A\Delta C$; Pour montrer que $B = C$, il est équivalent de montrer que $B \subset C$ et que $C \subset B$.
Soit $x \in B$. On a soit $x \in A$, soit $x \notin A$.

Supposons que x appartienne à A ; alors $x \in A \cap B$, donc $x \notin A \Delta B$. Comme $A \Delta B = A \Delta C$ et que $(A \setminus C) \subset A \Delta C$, on a $x \notin (A \setminus C)$ et comme $x \in A$, on en déduit $x \in C$.

Dans le cas où x n'appartient pas à A , alors $x \in A \cup B$ et $x \notin A \cap B$, donc $x \in A \Delta B = A \Delta C$. Or $x \notin A$; il faut donc que $x \in C \setminus A$; on obtient encore $x \in C$. On a donc montré que $B \subset C$.

Le problème étant symétrique en B et C , on prouve de même que $C \subset B$.

On en déduit que $B = C$.

2) On n'a pas utilisé les hypothèses E, A, B non vides.

Exercice n°4

La définition de f surjective est "pour tout y réel, l'équation $y = f(x)$ a au moins une solution réelle". Comme on le dit dans l'étude du premier cas, cette équation n'a pas de solution lorsque $y < 0$, par exemple pour $y = -1$. Donc f n'est pas surjective.

L'erreur est d'oublier le quantificateur "pour tout y réel", ce qui conduit à faire dépendre la surjectivité de f des valeurs de y .

Exercice n°5

La définition de " u et u' sont proportionnels" est "il existe un réel k tel que $u = k.u'$ ou il existe un réel k tel que $u' = k.u$ ". La définition proposée n'est pas bonne; elle exclut le cas où u' est nul et u ne l'est pas.

Lorsqu'on écrit "c'est-à-dire tel que ($a = ka'$ et $b = kb'$)", on sous-entend "il existe un réel k tel que", et lorsqu'on dit "ce qui se traduit par", on annonce une équivalence; mais la phrase "il existe un réel k tel que ($a = ka'$ et $b = kb'$)" n'est pas équivalente à "si $a' \neq 0$, $k = \frac{a}{a'}$ et $b = \frac{a}{a'}b'$, et si $a' = 0$, alors $a = 0$." Il ne s'agit que d'une implication et le statut de la lettre k n'est pas le même dans les deux phrases. Cette faute a probablement été commise parce qu'on a négligé le quantificateur "il existe".

Les "donc" qui suivent annoncent des implications et pas des équivalences.

Il manque la démonstration de la réciproque.

Une démonstration pourrait être la suivante :

lorsque u' est nul, les vecteurs sont automatiquement proportionnels, car on a $u' = 0.u$; on a également toujours $ab' - a'b = 0$.

Supposons maintenant que u' est non nul. Alors, dire que u et u' sont proportionnels est équivalent à dire qu'il existe un réel k tel que $u = k.u'$, ou encore qu'il existe un réel k tel que ($a = ka'$ et $b = kb'$).

Supposons ceci. Soit k_0 un tel réel. Lorsque $a' = 0$, on a alors $a = k_0 \times 0 = 0$, donc $ab' - ba' = 0$. Lorsque $a' \neq 0$, on a $k_0 = \frac{a}{a'}$ et donc $b = k_0b' = \frac{a}{a'}b'$ et $ab' - a'b = 0$.

Réciproquement, supposons $ab' - ba' = 0$. Dans le cas où $a' = 0$, on a $ab' = 0$. Or b' n'est pas nul, sinon u' serait nul; on obtient donc $a = 0$ et si on pose $k_0 = \frac{b}{b'}k$, on a $a = k_0a'$ et $b = k_0b'$. Dans le cas où $a' \neq 0$, on a $b = \frac{a}{a'}b'$. Posons $k_0 = \frac{a}{a'}$. On a $a = k_0a'$ et $b = k_0b'$. Dans les deux cas, u et u' sont proportionnels.

Finalement, on a bien l'équivalence annoncée.

Ici, on a tenu compte du quantificateur "il existe" en utilisant la règle "nommer un objet" pour démontrer la proposition directe et en exhibant un k convenable pour la réciproque.

Exercice n°6

Suivre la méthode donnée dans le polycopié.

Exercice n°7

On suppose $b < a$. Soit $\varepsilon_0 = a - b$. Par hypothèse, ε_0 est un nombre strictement positif. On a donc en appliquant l'hypothèse faite sur a et b : $a < b + \varepsilon_0 = b + (a - b) = a$, ce qui est impossible. Donc $a \leq b$.

Exercice n°8

Non. En effet, la négation de la proposition proposée est :

$\exists(f, g) \in \mathcal{F} \times \mathcal{F}$, ($fg = 0$ et $f \neq 0$ et $g \neq 0$). Si on prend f et g définies par : $f(x) = 0$ si $x < 0$ et $f(x) = 1$ si $x \geq 0$, $g(x) = 1$ si $x < 0$ et $g(x) = 0$ si $x \geq 0$, on obtient un contre-exemple, car on a $fg = 0$, $f \neq 0$ et $g \neq 0$.

Chapitre 4

Applications

1. Définitions et exemples

Définition 4.1 – Soient E et F deux ensembles. Une application f de E dans F est un “procédé” qui permet d’associer à chaque élément x de E un unique élément y de F ; cet élément y est alors noté $y = f(x)$, on l’appelle l’image de x et on dit que x est **un** antécédent de y par f . On dit que E est l’ensemble de départ ou ensemble source de f et que F est l’ensemble d’arrivée ou ensemble but de f .

On note $f : E \longrightarrow F$ ou $f : \begin{matrix} E \longrightarrow F \\ x \longmapsto f(x) \end{matrix}$.

L’ensemble $G = \{(x, y) \in E \times F \mid y = f(x)\}$ est appelé le graphe de f .

Exemples - • On définit une application f en prenant : $E = \{1, 2, 3\}$, $F = \{1, 2, 3, 4\}$, $f(1) = f(2) = 1$, $f(3) = 4$. Alors, l’image de 3 est 4 et 1 a deux antécédents : 1 et 2.

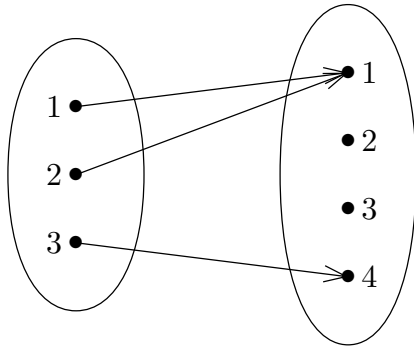


Diagramme sagittal

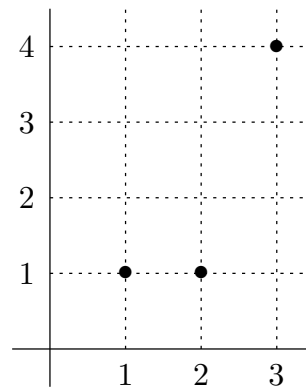


Diagramme cartésien

• L’application Logarithme : $\ln : \begin{matrix} \mathbb{R}_+^* \longrightarrow \mathbb{R} \\ x \longmapsto \ln(x) \end{matrix}$

• L’application : $\mathbb{R}^3 \longrightarrow \mathbb{R}^3$
 $(x, y, z) \longmapsto (2x + 3y, x - y + z, y + 5z)$

• L’application appelée “première projection” ou “première coordonnée” :

$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$
 $p_1 : (x, y) \longmapsto x$

• L’application “identité” : $Id_E : \begin{matrix} E \longrightarrow E \\ x \longmapsto x \end{matrix}$

Contre-exemples - Les énoncés suivants sont faux ou incomplets :

- “L’application de \mathbb{C} dans \mathbb{C} qui associe à chaque z de \mathbb{C} une de ses racines carrées complexes”.
- “L’application de \mathbb{R} dans \mathbb{R} définie par $f(x) = 1/x$ ”.
- “L’application f définie sur \mathbb{Z} par $f(x) = x^2$ ”

Remarques - • On note souvent $\mathcal{F}(E, F)$ l’ensemble des applications de E dans F .

- On parle plus généralement de fonctions : une fonction f d’un ensemble E dans un ensemble F associe à chaque élément x de E un élément de F *au plus*; l’ensemble des éléments x de E auxquels elle associe un élément y de F est appelé le domaine de définition de la fonction f et noté D_f . Si x appartient à D_f , l’élément y qui lui est associé est noté $y = f(x)$. On peut alors construire l’application (encore notée

$$f \text{ par abus de langage), } f : \begin{matrix} D_f & \longrightarrow & F \\ x & \longmapsto & f(x) \end{matrix} \text{ et c'est elle qu'on}$$

étudie en fait. Par exemple, si on parle de “la fonction réelle de la variable réelle définie par $f(x) = 1/x$ ”, on a $D_f = \mathbb{R}^*$,

$$\text{et on étudie l'application } f : \begin{matrix} \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 1/x \end{matrix}.$$

Exercice - Soient E et F deux ensembles finis non vides ayant respectivement n et m éléments. Montrer (par récurrence sur n par exemple) qu’il y a m^n applications de E dans F .

2. Egalité - Restriction - Prolongement

Définition 4.2 – Soient $f : E \longrightarrow F$ et $f_1 : E' \longrightarrow F'$ deux applications. On dit qu’elles sont égales et on note $f = f_1$ si les trois conditions suivantes sont vérifiées :

$$E = E', F = F' \text{ et } \forall x \in E, f(x) = f_1(x).$$

Exemples - • Soient $f : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto \cos(x) \end{cases}$ et $f_1 : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto 2 \cos^2(x/2) - 1 \end{cases}$
Alors, on a $f = f_1$.

• Les trois applications $f : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto x^2 \end{cases}$, $g : \begin{cases} \mathbb{R} \longrightarrow \mathbb{R}_+ \\ x \longmapsto x^2 \end{cases}$ et

$h : \begin{cases} \mathbb{R}_+ \longrightarrow \mathbb{R} \\ x \longmapsto x^2 \end{cases}$, sont deux à deux distinctes.

Définition 4.3 – Soient E et F deux ensembles, E_1 un sous-ensemble de E , $f : E \rightarrow F$ et $f_1 : E_1 \rightarrow F$. On suppose que pour tout élément x de E_1 , on a $f(x) = f_1(x)$. Alors, on dit que f_1 est la restriction de f à E_1 et que f est un prolongement de f_1 à E . On note $f_1 = f|_{E_1}$.

Exemple - Dans le deuxième exemple ci-dessus, h est la restriction de f à \mathbb{R}_+ , et f est un prolongement de h à \mathbb{R} . Mais l'application $k : \mathbb{R} \rightarrow \mathbb{R}$ telle que $(\forall x \in \mathbb{R}_+, k(x) = x^2 \text{ et } \forall x \in \mathbb{R}_-^* k(x) = 0)$ est un autre prolongement de h . (Dessiner et comparer les graphes de ces trois applications).

Remarque - Lorsque f est une application de E dans F et F_1 un sous-ensemble de F tel que pour tout élément x de E l'élément $f(x)$ appartienne à F_1 , on considère souvent l'application $g : \begin{matrix} E \rightarrow F_1 \\ x \mapsto f(x) \end{matrix}$. C'est le cas dans le deuxième exemple pour les applications f et g , si on prend $F_1 = \mathbb{R}_+$.

Exercice - Soit $f : \mathbb{R}_+ \rightarrow \mathbb{R}$ l'application donnée par $f(x) = 1$ pour tout x tel que $0 \leq x \leq 1$, $f(x) = 2$ pour tout x tel que $x > 1$. Trouver deux prolongements distincts de f à \mathbb{R} . Quelle est la restriction de f à $[0, 1]$? Trouver une application g de \mathbb{R}_+ dans \mathbb{N} telle que pour tout $x \in \mathbb{R}_+$, $g(x) = f(x)$.

3. Composition des applications

Définition 4.4 – Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications. On définit une application de E dans G notée $g \circ f$ en posant

$$\boxed{\forall x \in E, g \circ f(x) = g(f(x))}.$$

On l'appelle application composée de g et f .

Remarques - • Soient f et g deux éléments de $\mathcal{F}(E, E)$; les deux applications $f \circ g$ et $g \circ f$ sont définies, mais en général elles ne sont pas égales. Par exemple, si on a $f : \begin{matrix} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto x^2 \end{matrix}$ et $g : \begin{matrix} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto 2x \end{matrix}$,

on obtient $g \circ f : \begin{matrix} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto 2x^2 \end{matrix}$ et $f \circ g : \begin{matrix} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto 4x^2 \end{matrix}$ et ces deux applications sont différentes (prouvez le).

- On a $(g \circ f) \circ h = g \circ (f \circ h)$ (lorsque cela a un sens).
- Soient f et g deux applications $f : E \rightarrow F$, $g : F_1 \rightarrow G$ où F_1 est un sous-ensemble de F tel que pour tout $x \in E$, $f(x)$ appartienne à F_1 ; soit $f_1 : \begin{matrix} E \rightarrow F_1 \\ x \mapsto f(x) \end{matrix}$. L'application $g \circ f_1$ est souvent encore notée $g \circ f$ par abus de langage.

Exercice - 1°) Soit $E = \{1, 2, 3\}$, $f : E \rightarrow E$ et $g : E \rightarrow E$ les applications définies par $f(1) = 1, f(2) = 3, f(3) = 2, g(1) = 2, g(2) = 1, g(3) = 3$. Calculer $f \circ f, f \circ g$ et $g \circ f$. A-t-on $f \circ g = g \circ f$?
 2°) Dans le plan (affine euclidien orienté), on considère un (vrai) triangle OAB et f et g les symétries orthogonales par rapport à OA et OB respectivement. Calculer et comparer $f \circ g$ et $g \circ f$.

4. Familles

Une application u de \mathbb{N} dans un ensemble E est souvent notée $u : \begin{array}{l} \mathbb{N} \longrightarrow E \\ n \longmapsto u_n \end{array}$

plutôt que $u : \begin{array}{l} \mathbb{N} \longrightarrow E \\ n \longmapsto u(n) \end{array}$. On parle alors de la suite $(u_n)_{n \in \mathbb{N}}$ d'éléments de

E . Plus généralement, si u est une application d'un ensemble I dans E , on

la note parfois $u : \begin{array}{l} I \longrightarrow E \\ i \longmapsto u_i \end{array}$ et on parle alors de la famille $(u_i)_{i \in I}$ d'éléments

de E indexée par I . Lorsque E est l'ensemble des parties d'un ensemble X , on obtient ainsi des familles $(A_i)_{i \in I}$ de sous-ensembles de X .

On peut alors généraliser les notions de réunion, d'intersection et de partition. De façon naturelle, on définit :

- La réunion de la famille $(A_i)_{i \in I}$ est l'ensemble des éléments x de X qui appartiennent à l'un des ensembles A_i au moins :

$$\bigcup_{i \in I} A_i = \{x \in X \mid \exists i \in I, x \in A_i\}$$

- L'intersection de la famille $(A_i)_{i \in I}$ est l'ensemble des éléments x de X qui appartiennent à tous les ensembles A_i :

$$\bigcap_{i \in I} A_i = \{x \in X \mid \forall i \in I, x \in A_i\}$$

- La famille $(A_i)_{i \in I}$ de sous-ensembles de X forme une partition de X si

$$X = \bigcup_{i \in I} A_i$$

$$\forall i, j \in I, (i \neq j \implies A_i \cap A_j = \emptyset)$$

$$\forall i \in I, A_i \neq \emptyset$$

Exemple - Soit pour $n \in \mathbb{N}$, $A_n = [n, n+1[$. Alors, la famille $(A_n)_{n \in \mathbb{N}}$ forme une partition de $[0, +\infty[$.

Exercice - 1°) Pour tout $n \in \mathbb{N}$, on pose $A_n = [2^n, 2^{n+1}[$. Calculer la réunion $E = \bigcup_{n \in \mathbb{N}} A_n$. Que peut-on dire de la famille $(A_n)_{n \in \mathbb{N}}$?
 2°) Calculer $\bigcup_{x \in]0, 1/2[}]x - 1, x + 1[$ et $\bigcap_{x \in]0, 1/2[}]x - 1, x + 1[$.

5. Bijection - Injection - Surjection

Proposition et définition 4.5 – Soit $f : E \longrightarrow F$ une application.

1 – On dit que f est une surjection ou que f est surjective si chaque élément y de F est l'image d'un élément de E au moins, c'est-à-dire si pour chaque élément y de F , l'équation $y = f(x)$ a au moins une solution dans E , ce qui s'écrit :

$$\forall y \in F, \exists x \in E, y = f(x)$$

2 – On dit que f est une injection ou que f est injective si la proposition suivante est vraie :

$$\forall (x, x') \in E^2, (f(x) = f(x')) \implies x = x'.$$

c'est-à-dire si chaque élément y de F est l'image d'un élément de E au plus, ou encore, si pour chaque élément y de F , l'équation $y = f(x)$ a au plus une solution dans E .

3 – On dit que f est une bijection ou que f est bijective si elle est à la fois injective et surjective.

Preuve : on va démontrer l'équivalence concernant l'injectivité.

- 1) Supposons que tout élément de F admette au plus un antécédent par f . Soient x et x' deux éléments de E tels que $f(x) = f(x')$. Posons $y = f(x)$. C'est un élément de F qui admet x et x' pour antécédents. Or y a au plus un antécédent. Donc $x = x'$.
 On a montré que, si tout élément de F a au plus un antécédent par f , l'application f est injective.
- 2) Supposons qu'il existe un élément de F qui n'admette pas au plus un antécédent par f . Notons y un de ces éléments. y a (au moins) deux antécédents distincts x et x' . Par définition d'un antécédent, on a $f(x) = f(x') = y$. On a donc $x \neq x'$ et $f(x) = f(x')$.
 On a montré $\exists (x, x') \in E^2, (x \neq x' \text{ et } f(x) = f(x'))$, c'est-à-dire la négation de
 “ $\forall (x, x') \in E^2, (f(x) = f(x')) \implies x = x'$,” c'est-à-dire que f n'est pas injective. On a donc montré l'implication réciproque par contraposée.

Remarques - • L'écriture avec les quantificateurs est souvent plus commode pour montrer qu'une application est injective.

- L'expression "au plus" signifie qu'un élément de F soit n'a pas d'antécédent, soit en a un.

Remarques - Soit $f : E \longrightarrow F$ une application.

- Pour montrer que f n'est pas injective, il suffit de trouver deux éléments distincts x et x' de E tels que $f(x) = f(x')$.
- Pour montrer que f n'est pas surjective, il suffit de trouver un élément y de F qui n'a aucun antécédent.

Exemples -

- Soit v l'application de $[0, 1]$ dans \mathbb{R} définie par $v(x) = x^2 - 3x$. Montrons que v est injective. Soient x et x' deux éléments de $[0, 1]$. Supposons $v(x) = v(x')$. On a donc $(x - x')(x + x' - 3) = 0$, d'où $x = x'$ ou $x + x' - 3 = 0$. Mais comme x et x' sont inférieurs à 1, on a $x + x' \leq 2$ et on ne peut avoir $x + x' = 3$. Donc, on a $x = x'$. On a montré $(\forall x, x' \in E, (v(x) = v(x') \implies x = x'))$, donc v est injective. Mais v n'est pas surjective. En effet, si x appartient à $[0, 1]$, on a $x(x - 3) \leq 0$ donc $f(x) \leq 0$; si y est un réel strictement positif, l'équation $y = f(x)$ n'a aucune solution dans $[0, 1]$.
- Soit $u : \mathbb{R} \longrightarrow \mathbb{R}^+$ l'application telle que $u(x) = 0$ si $x < -1$ et $u(x) = x + 1$ si $x \geq -1$. Les réels -1 et -2 sont distincts et ont la même image : $u(-1) = u(-2) = 0$. Donc u n'est pas injective. Montrons que u est surjective. Soit y un réel positif. On veut montrer qu'il existe au moins un élément x de \mathbb{R} tel que $y = u(x)$. Posons $x = y - 1$. On a alors $x \geq -1$ et $y = x + 1$, donc $y = u(x)$. On a donc montré que pour tout $y \in \mathbb{R}^+$, il existe au moins un $x \in \mathbb{R}$ tel que $y = u(x)$, c'est-à-dire que u est surjective.

Exercice - 1°) L'application $f : \begin{matrix} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{matrix}$ est-elle injective? surjective? bijective?

2°) Soient E et F deux ensembles finis ayant respectivement n et m éléments et f une application de E dans F . On suppose que f est injective; comparer n et m . Même question lorsque f est surjective, lorsque f est bijective.

6. Etude des bijections

Définition 4.7 – Soit $f : E \longrightarrow F$ une bijection. Alors, l'application de F dans E qui à chaque élément y de F associe l'unique élément x de E solution de l'équation $y = f(x)$ est appelée application réciproque de f et notée f^{-1} .

Remarque - Si f est bijective, $x \in E$ et $y \in F$, il est équivalent de dire “ x est un antécédent de y pour f ”, “ $y = f(x)$ ”, “ $x = f^{-1}(y)$ ” ou “ y est un antécédent de x pour f^{-1} ”.

Exemples -

- Soit h l'application de $\{1, 2, 3\}$ dans $\{1, 5, 7\}$ telle que $h(1) = 5, h(2) = 1$ et $h(3) = 7$; elle est bijective. Sa réciproque h^{-1} est l'application de $\{1, 5, 7\}$ dans $\{1, 2, 3\}$ donnée par $h^{-1}(1) = 2, h^{-1}(5) = 1, h^{-1}(7) = 3$.

- Considérons la bijection $l : \mathbb{R} \longrightarrow \mathbb{R}$
 $x \longmapsto x^3$. L'application réciproque de l est

$$l^{-1} : \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto \sqrt[3]{x} \end{array} .$$

*Exercice - 1°) Montrer que l'application $h : \mathbb{R} \longrightarrow \mathbb{R}$
 $x \longmapsto 2x - 1$ est bijective et déterminer h^{-1} .*

*2°) Soit f l'application de \mathbb{R} dans \mathbb{R} définie par $f(x) = 0$ si $x < 0$,
 $f(x) = 2x$ si $x \in [0, 1/2]$, $f(x) = 1$ si $x > 1/2$. L'application f
est-elle injective? Surjective? Bijective? Trouver une restriction
de f qui soit injective. Est-elle bijective? Trouver une bijection g
d'un sous-ensemble E de \mathbb{R} sur un sous-ensemble F de \mathbb{R} telle que
 $\forall x \in E, f(x) = g(x)$. Déterminer g^{-1} .*

Proposition 4.8 – Soit $f : E \longrightarrow F$ une application bijective. Alors

- 1) f^{-1} est bijective et $(f^{-1})^{-1} = f$,
- 2) $f^{-1} \circ f = Id_E$ et $f \circ f^{-1} = Id_F$

*Preuve : 1) Soit x un élément de E . On considère l'équation $x = f^{-1}(y)$
(dans laquelle l'inconnue est y et la donnée x). On veut montrer
que cette équation a une solution dans F et une seule. Par définition
de f^{-1} , cette équation équivaut à l'équation $y = f(x)$. Elle a donc
une seule solution et c'est $f(x)$, d'où le résultat.*

*2) Il faut montrer que $f^{-1} \circ f$ est une application de E dans E et
que pour tout $x \in E, f^{-1} \circ f(x) = x$. Or on a $f : E \longrightarrow F$ et $f^{-1} : F \longrightarrow E$, donc $f^{-1} \circ f : E \longrightarrow E$. D'autre part, soit x appartenant
à E , et posons $y = f(x)$; on a alors $f^{-1} \circ f(x) = f^{-1}(y) = x$ par
définition de f^{-1} . D'où $f^{-1} \circ f = Id_E$.*

On fait de même pour montrer que $f \circ f^{-1} = Id_F$. □

La propriété 2 de la proposition précédente caractérise l'application réciproque f^{-1} . On a en effet la proposition suivante :

Proposition 4.9 – Soit $f : E \longrightarrow F$ une application. On suppose qu'il existe une application $g : F \longrightarrow E$ telle que $g \circ f = Id_E$ et $f \circ g = Id_F$. Alors, f et g sont bijectives, $g = f^{-1}$ et $f = g^{-1}$.

Preuve : montrons que f est bijective. Soit y un élément de F . On veut montrer que l'équation $y = f(x)$ (où x est l'inconnue, y la donnée) a une et une seule solution dans E .

Si x est solution, on a $g(y) = g \circ f(x)$ et comme $g \circ f = Id_E$, on a $x = g(y)$; inversement, si $x = g(y)$, x appartient à E et $f(x) = f \circ g(y)$; comme $f \circ g = Id_F$, on a $f(x) = y$, donc x est solution. Il y a une solution et une seule et c'est $g(y)$. De tout ceci, on déduit que f est bijective et $g = f^{-1}$. Le reste de la proposition est une conséquence de la proposition précédente. \square

Remarques -

- La proposition ci-dessus donne un autre moyen de montrer qu'une application f est bijective. On "devine" en effet parfois l'application réciproque. Il suffit en la notant g de vérifier qu'elle satisfait aux deux conditions $g \circ f = Id_E$ et $f \circ g = Id_F$. Soit par exemple l'application $f : \mathbb{N} \rightarrow \mathbb{N}$ définie par $f(2n) = 2n + 1$ et $f(2n + 1) = 2n$, pour tout $n \in \mathbb{N}$. Il est évident que $f \circ f = Id_{\mathbb{N}}$ et donc f est bijective et égale à son application réciproque.

- On peut voir une bijection comme un "codage". Par exemple, les informaticiens codent les entiers compris entre 0 et $2^{31} - 1$ par des suites $s = (s_0, s_1, \dots, s_{30})$ de 0 et de 1. On peut justifier cela de la façon suivante : on considère l'ensemble S de toutes les suites s de cette forme et l'ensemble

E de tous les entiers compris entre 0 et $2^{31} - 1$; si $s \in S$, l'entier $n = \sum_{i=0}^{30} 2^i s_i$

est dans E (pourquoi?). On peut donc construire l'application $f : S \rightarrow E$ qui à $s \in S$ associe cet entier n . On vérifie que f est bijective (on le prouve avec un raisonnement par récurrence et la division euclidienne que vous verrez dans la cours d'arithmétique); l'application inverse f^{-1} associe à chaque entier $n \in E$ une suite s qu'on appelle sa représentation en numération binaire. Il est équivalent de se donner l'entier n ou la suite s . Par exemple $11 = 1 + 2 + 2^3 = f(1, 1, 0, 1, 0, \dots, 0)$, donc $f^{-1}(11) = (1, 1, 0, 1, 0, \dots, 0)$.

- Si f est seulement injective, la situation est moins bonne. Il y a des éléments de F qui ne correspondent à aucun x . On peut cependant construire une bijection, en modifiant l'ensemble d'arrivée. Par exemple, chaque étudiant e se voit attribuer un numéro d'inscription $N(e)$ à son entrée à l'université de Rennes I. En notant E l'ensemble des étudiants inscrits, on peut construire

l'application $N : \begin{matrix} E & \longrightarrow & \mathbb{N} \\ e & \longmapsto & N(e) \end{matrix}$. Elle est injective et pas surjective. Un numéro

attribué permet de retrouver l'étudiant correspondant, mais tous les entiers ne sont pas des numéros attribués. Si on note M l'ensemble des numéros

attribués et N' l'application $N' : \begin{matrix} E & \longrightarrow & M \\ e & \longmapsto & N(e) \end{matrix}$, alors N' est bijective.

7. Image directe ou réciproque

On fixe toujours une application $f : E \rightarrow F$.

Définition 4.10 – Soit B un sous-ensemble de F . On appelle image réciproque de B par f l'ensemble des éléments x de E dont l'image $f(x)$

par f est dans B . C'est un sous-ensemble de E ; on le note $f^{-1}(B)$. On a donc pour tout élément x de E :

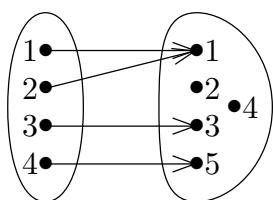
$$x \in f^{-1}(B) \iff f(x) \in B$$

Définition 4.11 – Soit A un sous-ensemble de E . On appelle image directe de A par f l'ensemble des images $f(x)$ des éléments x de A . C'est un sous-ensemble de F ; on le note $f(A)$. On a donc pour tout élément y de F :

$$y \in f(A) \iff \exists x \in A, y = f(x).$$

L'ensemble $f(E)$ est aussi appelé l'image de f .

Exemple - Considérons l'exemple de la figure ci-dessous



On a $f^{-1}(\{2\}) = \emptyset$,
 $f^{-1}(\{1\}) = f^{-1}(\{1, 2, 4\}) = \{1, 2\}$,
 $f(\{1, 4\}) = \{1, 5\}$ et l'image de f est
 $f(\{1, 2, 3, 4\}) = \{1, 3, 5\}$.

Exercice - 1°) Dans l'exemple de la figure précédente, calculer $f^{-1}(\{1, 2, 5\})$ et $f(\{2, 3\})$.


*2°) Soit $g : \mathbb{R} \longrightarrow \mathbb{R}$
 $x \longmapsto \sin(x)$. Calculer $g^{-1}(\{-1, 1\})$, l'image de g et $g([0, 3\pi/2])$.*

3°) Les applications f, g, h, k de \mathbb{R} dans \mathbb{R} définies respectivement par

$f(x) = x, g(x) = x^2, h(x) = x^3, k(x) = |x|$ pour x réel sont-elles injectives, surjective, bijectives ? Pour chacune de ces applications donner son image, l'image réciproque de \mathbb{R}_- et celle de $\{1\}$.

Remarques sur les notations - Il faut être très prudent avec la notation f^{-1} , qui n'est pas très heureuse.

⚠ Supposons que f soit bijective. Les deux applications f et f^{-1} sont alors définies et la notation $f^{-1}(B)$ désigne a priori deux ensembles distincts : l'image réciproque de B par f et l'image directe de B par f^{-1} . Mais si $x \in E$, dire que $f(x) \in B$ équivaut à dire qu'il existe $y \in B$ tel que $f^{-1}(y) = x$. Ces deux ensembles sont donc égaux et la notation est sans ambiguïté. Mais, lorsque l'on utilise la notation $f^{-1}(B)$, on ne suppose pas que l'application f^{-1} est définie : l'application f n'est pas forcément bijective.

 L'ensemble $f^{-1}(\{y\})$ est l'ensemble des antécédents de y par f . Lorsque f est bijective, cet ensemble a un et un seul élément $f^{-1}(y)$; et on a donc alors $f^{-1}(\{y\}) = \{f^{-1}(y)\}$ (comprenez vous la différence de notation entre les deux membres ?) Dans le cas général, c'est un *ensemble* qui peut avoir 0,1 ou plusieurs éléments (trouvez-en des exemples sur la figure précédente). L'usage est malheureusement de noter plus simplement $f^{-1}(y)$ au lieu de $f^{-1}(\{y\})$, ce qui n'aide pas les débutants... Astreignez-vous donc au moins au début, à mettre toutes les accolades nécessaires.

Proposition 4.12 – Soit $f : E \longrightarrow F$ une application. Alors, elle est surjective si et seulement si son image $f(E)$ est égale à l'ensemble d'arrivée F .

Remarque - Lorsque $f : E \longrightarrow F$ est surjective, on peut classer les éléments x de E suivant le "caractère" f . En effet, pour $y \in F$, notons $E_y = f^{-1}(\{y\})$. La famille $(E_y)_{y \in F}$ forme une partition de E . (Pourquoi ?) Si par exemple, f est l'application de \mathbb{N} dans $\{0, 1\}$ telle que $f(2n) = 0$ et $f(2n + 1) = 1$, alors f permet de classer les entiers en pairs et impairs. Qu'obtient-on si f est l'application de \mathbb{R} dans \mathbb{N} qui associe à chaque réel x sa partie entière $[x]$?

8. Compléments

Il y a plusieurs théorèmes que vous rencontrerez cette année, qui sont parfois bien utiles pour montrer qu'une application est bijective. En voici quelques uns que vous pourrez utiliser, à *condition évidemment de vérifier leurs hypothèses*.


Théorème 4.13 – Soit $I = [a, b]$ un intervalle de \mathbb{R} et une application $f : I \longrightarrow \mathbb{R}$. On suppose f continue et strictement croissante. Alors :

- 1) f est injective.
- 2) L'image de f est l'ensemble $[f(a), f(b)]$.
- 3) L'application f définit (par restriction de l'ensemble d'arrivée)

une application $g : \begin{matrix} [a, b] & \longrightarrow & [f(a), f(b)] \\ x & \longmapsto & f(x) \end{matrix}$ et cette application g est

bijective.

On a des théorèmes analogues pour f strictement décroissante ou pour un intervalle I quelconque.

 Une application bijective de $[a, b]$ dans $[f(a), f(b)]$ est-elle forcément monotone ? Fabriquez un contre-exemple.

Théorème 4.14 – Soient E et F deux ensembles finis ayant le même nombre d'éléments et une application $f : E \longrightarrow F$. Alors les affirmations suivantes sont équivalentes :

- 1) f est bijective
- 2) f est injective
- 3) f est surjective

 Le résultat est-il vérifié pour les applications suivantes ? Pourquoi ?

1) $\{1, 2\} \longrightarrow \{1, 4, 6\}$
 $x \longmapsto x^2$

2) $\mathbb{R} \longrightarrow \mathbb{R}_+$
 $x \longmapsto x^2$

3) $\mathbb{N} \longrightarrow \mathbb{N}$
 $n \longmapsto n + 1$

Enfin ce théorème que vous étudierez en MA3 :

Théorème 4.15 – Soit f une application linéaire de \mathbb{R}^n dans \mathbb{R}^n (ou plus généralement d'un espace vectoriel E de dimension finie dans un espace vectoriel F de même dimension). Alors les affirmations suivantes sont équivalentes :

- 1) f est bijective 2) f est injective 3) f est surjective

EXERCICES D'APPLICATION

Exercice n°1

Déterminer toutes les applications h de $E = \{0, 1, 2, 3, 4\}$ dans lui-même telles que pour tout x et tout y de E , on ait $h(x + y) = h(x) + h(y)$.

Exercice n°2

On définit deux fonctions f et g sur $[0, 1]$ à valeurs dans $[0, 1]$ par

$$f(x) = \begin{cases} 1/2 - x & \text{si } x \in [0, 1/2[\\ 0 & \text{sinon} \end{cases} \quad g(x) = \begin{cases} 0 & \text{si } x \in [0, 1/2[\\ x - 1/2 & \text{sinon} \end{cases}$$

Déterminer $f \circ g$ et $g \circ f$. Ces applications sont-elles égales ?

Exercice n°3

Soient F un ensemble, E un sous-ensemble de F et f l'injection canonique de E dans F ($f(x) = x$ pour tout x de E). A quelle condition existe-t-il une application h de F dans E telle que $f \circ h = Id_F$?

Exercice n°4

Pour tout $n \in \mathbb{N}^*$, on pose $A_n = [1/(n+1), 1/n[$. Calculer $E = \bigcup_{n \in \mathbb{N}^*} A_n$ et montrer que la famille $(A_n)_{n \in \mathbb{N}^*}$ forme une partition de E .

Exercice n°5

Soient a et b deux nombres rationnels et f l'application de l'ensemble des nombres rationnels dans lui-même qui à chaque rationnel x associe $f(x) = ax + b$. Cette application est-elle injective, surjective ?

Exercice n°6

Soit f l'application de \mathbb{R} dans $] -1, 1[$ définie par $f(x) = x/(1 + |x|)$. Montrer que f est bien définie, qu'elle est bijective et déterminer sa fonction réciproque f^{-1} .

Exercice n°7

Soit f l'application $f : \mathbb{C} \longrightarrow \mathbb{C}$
 $z \longmapsto 1 + z^2$

- 1) Montrer que f est surjective.
- 2) L'application f est-elle injective ?
- 3) Déterminer l'image $f(\mathbb{R})$ de \mathbb{R} par l'application f .

Exercice n°8

Soit f l'application de \mathbb{Z} dans lui-même définie par $f(x) = x^2 - x$.

1-a) Montrer que f n'est pas injective.

b) Calculer les valeurs de $f(n)/2$ pour $n \in \{n \in \mathbb{N}^* \mid n \leq 6\}$. Que remarquez-vous ?

c) Montrer que la restriction de f à \mathbb{N}^* est injective.

2) Soit h l'application de $\mathbb{Z} \times \mathbb{Z}$ dans \mathbb{Z} définie par $h(x, y) = f(x) + f(y)$ pour tout (x, y) de $\mathbb{Z} \times \mathbb{Z}$.

a) Montrer que l'image de h est un sous-ensemble de l'ensemble $2\mathbb{Z}$ des entiers pairs. L'application h est-elle surjective ?

b) La restriction de h à $\mathbb{N}^* \times \mathbb{N}^*$ est-elle injective ?

Exercice n°9

Soient A et B deux parties non vides d'un ensemble E et f l'application de $\mathcal{P}(E)$ dans $\mathcal{P}(A) \times \mathcal{P}(B)$ définie par $f(X) = (A \cap X, B \cap X)$. Donner des conditions nécessaires et suffisantes sur A et B pour que f soit injective, surjective, bijective. Expliciter f^{-1} lorsque f est bijective.

Exercice n°10

Soient f une application de E dans F , g une application de F dans G et $h = g \circ f$.

1) Montrer que si h est injective, f l'est aussi et que si h est surjective, g l'est aussi.

2) Montrer que si h est surjective et g injective, alors f est surjective.

3) Montrer que si h est injective et f surjective alors g est injective.

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°1

Il faut $h(n) = nh(1)$ pour tout $n \in \{0, 1, 2, 3, 4\}$. Les solutions sont $h = 0$ et $h = Id$.

Exercice n°2

$(f \circ g)(x) = 1/2$ si $x \in [0, 1/2[$, $(f \circ g)(x) = 1 - x$ sinon, $g \circ f = 0$.

Les deux applications sont distinctes.

Exercice n°3

Il faut $E = F$ et dans ce cas, il existe une et une seule solution $h = Id_E$.

Exercice n°4

$E =]0, 1[$.

Exercice n°5

Si $a \neq 0$, f est bijective. Sinon, f n'est ni injective, ni surjective.

Exercice n°6

Pour montrer que f est bien définie, vérifier que $(\forall x \in \mathbb{R}, f(x) \in]-1, 1[)$. Remarquer que x et $f(x)$ ont même signe. Si $y \in]-1, 1[$, l'équation $y = f(x)$ admet une et une seule solution $y/(1 - |y|)$. Donc f est bijective et $f^{-1}(y) = y/(1 - |y|)$.

Exercice n°7

Soit $u \in \mathbb{C}$. L'équation $u = f(z)$ a deux solutions complexes distinctes si $u \neq 1$ et une seule si $u = 1$.

- 1) Donc f est surjective,
- 2) et f n'est pas injective
- 3) $f(\mathbb{R}) = \{u \in \mathbb{R} \mid u \geq 1\}$.

Exercice n°8

1-a) $f(0) = f(1) = 0$ et $0 \neq 1$.

b) On trouve 0, 1, 3, 6, 10, 15. On voit que $f(n)/2$ est la somme des $n - 1$ premiers nombres entiers.

c) La restriction de f à \mathbb{N}^* est strictement croissante, donc injective.

2) Pour n entier, n ou $n - 1$ est pair, donc $f(n) = n(n - 1)$ est pair, donc h prend ses valeurs dans $2\mathbb{Z}$. Mais par exemple, 10 n'a aucun antécédent (voir que les valeurs prises par f sont 0, 2, 6, 12, ...); donc h n'est pas surjective.

3) non : $h(1, 4) = h(3, 3) = 12$ et $(1, 4) \neq (3, 3)$.

Exercice n°9

L'application f est injective ssi $A \cup B = E$, surjective ssi $A \cap B = \emptyset$, f bijective ssi A et B forment une partition de E . Dans ce cas, $f^{-1}(C, D) = C \cup D$.

Exercice n°10

- 1) Appliquer les définitions.
- 2) Dédire de la question 1 que g est bijective et écrire $f = g^{-1} \circ h$.
- 3) Dédire de la question 1 que f est bijective et écrire $g = h \circ f^{-1}$.

Chapitre 5

Lois de composition internes - Relations

1. Lois de composition internes

1.1. Définition et exemples

Définition 5.1 – Soit E un ensemble. Une loi de composition interne sur E est une application de $E \times E$ dans E . Si on la note $E \times E \longrightarrow E$
 $(a, b) \longmapsto a * b$, on parle de la loi $*$ et on dit que $a * b$ est le composé de a et b pour la loi $*$.

Exemples -

- Sur $E = \mathbb{Z}$, l'addition définie par $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
 $(a, b) \longmapsto a + b$, la multiplication $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
 $(a, b) \longmapsto a \times b$ et la soustraction $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
 $(a, b) \longmapsto a - b$ sont des lois de composition internes. Ce n'est pas le cas de la division car a/b n'est pas défini pour tous les couples (a, b) d'entiers.
- Soit X un ensemble. Sur $\mathcal{P}(X)$, la réunion $\mathcal{P}(X)^2 \rightarrow \mathcal{P}(X)$
 $(A, B) \mapsto A \cup B$ est une loi de composition interne. De même, pour l'intersection \cap et la différence symétrique Δ .
- Soit X un ensemble. On note $E = \mathcal{F}(X)$ l'ensemble des applications de X dans X . La composition des applications $E \times E \longrightarrow E$
 $(f, g) \longmapsto f \circ g$ est une loi interne sur E .
- Sur $E = \mathbb{R}^2$, l'addition $E \times E \rightarrow E$
 $((x, y), (x', y')) \mapsto (x + x', y + y')$ est une loi interne. La multiplication par un scalaire $\mathbb{R} \times E \rightarrow E$
 $(\lambda, (x, y)) \mapsto (\lambda x, \lambda y)$ n'est pas une loi interne, car son ensemble de départ n'est pas $E \times E$.

1.2. Propriétés usuelles des lois internes

Définition 5.2 – Soit $*$ une loi interne sur un ensemble E . On dit que

1 – la loi $*$ est **commutative** si $\forall (x, y) \in E^2, x * y = y * x$.

2 – la loi $*$ est **associative** si $\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$.

- Exemples -**
- L'addition et la multiplication dans \mathbb{Z} sont commutatives et associatives. Ce n'est pas le cas de la soustraction (montrez le).
 - La composition des applications dans $\mathcal{F}(X, X)$ est associative, mais n'est en général pas commutative (trouvez un contre-exemple).
 - Que pensez-vous des autres exemples du paragraphe précédent ?

Définition 5.3 – Soit $*$ une loi interne sur un ensemble E . Un élément e de E est un **élément neutre** pour la loi $*$ si $\boxed{\forall a \in E, a * e = e * a = a.}$

- Exemples -**
- Dans \mathbb{Z} , 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication.
 - La composition des applications dans $\mathcal{F}(X, X)$ admet Id_X pour élément neutre.
 - Etudiez les autres exemples.

Proposition 5.4 – Soit $*$ une loi interne sur un ensemble E , si $*$ possède un élément neutre, il est unique.

Preuve : supposons que $*$ ait deux éléments neutres e et e' , alors on a $e * e' = e$ car e' est élément neutre et $e * e' = e'$ car e est élément neutre. On en déduit que $e = e'$. \square

Définition 5.5 – Soit $*$ une loi interne sur un ensemble E , possédant un élément neutre e et soit a un élément de E . On dit que a admet un **symétrique** b pour la loi $*$, si l'on a $(a * b = b * a = e)$.

- Exemples -**
- Dans \mathbb{R} , chaque élément a possède un symétrique pour l'addition qui est son opposé $-a$. Mais a n'a un symétrique pour la multiplication que s'il est non nul ; son symétrique est alors l'inverse $1/a$ de a .
 - Dans $\mathcal{F}(X, X)$, un élément f a un symétrique (pour la composition \circ) si et seulement si f est bijective et alors son symétrique est l'application réciproque f^{-1} .

Définition 5.6 – Soit E un ensemble muni de deux lois de composition internes, notées $+$ et $*$. On dit que $*$ est **distributive** par rapport à $+$ si

$$\boxed{\forall (x, y, z) \in E^3, x * (y + z) = (x * y) + (x * z) \text{ et } (x + y) * z = (x * z) + (y * z).}$$

- Exemples -**
- Dans \mathbb{R} , la multiplication est distributive par rapport à l'addition. L'addition est-elle distributive par rapport à la multiplication ?

- Dans l'ensemble $\mathcal{P}(X)$ des parties d'un ensemble X , la réunion est distributive par rapport à l'intersection et l'intersection est distributive par rapport à la réunion.

1.3. Exemples de structures algébriques (culture générale)

Définition 5.7 – Soit E un ensemble muni d'une loi de composition interne $*$. On dit que $(E, *)$ est un **groupe** si la loi $*$ satisfait aux trois conditions suivantes :

- 1 – Elle est associative.
- 2 – Elle admet un élément neutre.
- 3 – Chaque élément de E admet un symétrique pour $*$.

Si de plus, la loi est commutative, on dit que le groupe est commutatif ou abélien (du nom du mathématicien Abel).

- Exemples** -
- L'ensemble des entiers relatifs muni de l'addition $(\mathbb{Z}, +)$ est un groupe commutatif.
 - De même $(\mathbb{R}, +)$ et (\mathbb{R}^*, \times) sont des groupes commutatifs.
 - Dans l'ensemble des applications $\mathcal{F}(X, X)$ d'un ensemble X dans lui-même, considérons le sous-ensemble BIJ des bijections. Vérifier que la composition des applications définit une loi interne sur BIJ et que (BIJ, \circ) est un groupe, en général non commutatif.
 - Soient n un entier non nul et $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ l'ensemble des racines $n^{\text{ièmes}}$ de l'unité. Alors (U_n, \times) est un groupe commutatif.

Définition 5.8 – Soit E un ensemble muni de deux lois de composition internes que nous noterons $+$ et $*$. On dit que $(E, +, *)$ est un **anneau** si les conditions suivantes sont remplies :

- 1 – $(E, +)$ est un groupe commutatif.
- 2 – La loi $*$ est associative.
- 3 – La loi $*$ est distributive par rapport à la loi $+$.

Si de plus la loi $*$ est commutative, on dit que l'anneau est commutatif ; si elle admet un élément neutre, on dit que l'anneau est **unitaire**. On note en général 0 l'élément neutre de la loi $+$ et 1 celui de la loi $*$ lorsqu'il existe.

- Exemples** -
- L'ensemble des entiers muni de l'addition et de la multiplication $(\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire.
 - De même pour $(\mathbb{R}, +, \times)$ et pour $(\mathbb{R}[X], +, \times)$ où $\mathbb{R}[X]$ désigne l'ensemble des polynômes à coefficients réels.
 - De même pour $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, où $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers modulo n (voir le chapitre 6).

Dans un anneau commutatif et unitaire $(E, +, *)$ les règles de calcul qui ne font intervenir que l'addition, la soustraction et la multiplication sont les

mêmes que dans $(\mathbb{Z}, +, \times)$. Par contre, il faut être prudent avec les divisions : l'équation $(x * y = x * z)$ n'est pas toujours équivalente à $(y = z \text{ ou } x = 0)$, $n \cdot x = 0$ n'implique pas toujours $(x = 0 \text{ ou } n = 0)$ (pour des exemples, voir le cours d'arithmétique sur les congruences).

Définition 5.9 – Soit E un ensemble muni de deux lois de composition internes toujours notées $+$ et $*$. On dit que $(E, +, *)$ est un **corps commutatif** si les conditions suivantes sont remplies :

- 1 – $(E, +, *)$ est un anneau commutatif et unitaire.
- 2 – Chaque élément de $E \setminus \{0\}$ a un symétrique pour la loi $*$. Si $(E, +, *)$ est un corps commutatif, et si on note $E^* = E \setminus \{0\}$, alors $(E^*, *)$ a une structure de groupe commutatif, dont l'élément neutre est 1.

Exemples - • $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps commutatifs.
 • On note $\mathbb{R}(X)$ l'ensemble des fractions rationnelles à coefficients réels. Alors, $(\mathbb{R}(X), +, \times)$ est un corps commutatif.
 • L'anneau $(\mathbb{Z}, +, \times)$ n'est pas un corps. (Quels sont les éléments inversibles ?)

2. Relations

2.1. Définitions et exemples

Définition 5.10 – Soit E un ensemble. Une relation dans E est une propriété concernant les couples (x, y) d'éléments de E . Notons \mathcal{R} une telle relation ; on écrit en général $x\mathcal{R}y$ pour signifier que le couple (x, y) vérifie la relation \mathcal{R} .

Exemples - • Dans $E = \mathbb{C}$, la relation d'égalité : $x = y$.
 • Dans $E = \mathbb{R}$, la relation : $x = y^2$.
 • Dans $E = \mathbb{R}$, la relation d'inégalité : $x \leq y$.
 • Dans l'ensemble des droites du plan (affine) la relation de parallélisme : D est parallèle à D' .
 • Soit X un ensemble et $E = \mathcal{P}(X)$; dans E , on a la relation d'inclusion : $A \subset B$.
 • Sur $E = \mathbb{Z}$, la relation : x et y sont de même parité, appelée relation de congruence modulo 2 et notée : $x \equiv y \pmod{2}$.
 • Si f est une application de E dans un ensemble F , on peut lui associer la relation \mathcal{R} définie par $(x\mathcal{R}y \Leftrightarrow f(x) = f(y))$.

2.2. Propriétés usuelles des relations

Définition 5.11 – Soit \mathcal{R} une relation sur un ensemble E . On dit que :

1 – La relation \mathcal{R} est **réflexive** si

$$\boxed{\forall x \in E, x\mathcal{R}x.}$$

2 – La relation \mathcal{R} est **symétrique** si

$$\boxed{\forall (x, y) \in E^2, (x\mathcal{R}y \Rightarrow y\mathcal{R}x).}$$

3 – La relation \mathcal{R} est **antisymétrique** si

$$\boxed{\forall (x, y) \in E^2, ((x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y).}$$

4 – La relation \mathcal{R} est **transitive** si

$$\boxed{\forall (x, y, z) \in E^3, ((x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z).}$$

Définition 5.12 – Soit \mathcal{R} une relation. Si \mathcal{R} est réflexive, symétrique et transitive, on dit que \mathcal{R} est une **relation d'équivalence**. Si \mathcal{R} est réflexive, antisymétrique et transitive, on dit que \mathcal{R} est une **relation d'ordre**.

Exemple - Reprenons les exemples ci-dessus. On voit facilement que les relations d'égalité (ex.1), de parallélisme (ex.4) ou de congruence modulo 2 (ex.6) sont des relations d'équivalence et que les relations d'inégalité (ex.3) ou d'inclusion (ex.5) sont des relations d'ordre. Que pensez-vous de l'exemple 2 ?

Définition 5.13 – Soit \mathcal{R} une relation d'ordre dans un ensemble E . On dit que \mathcal{R} est une **relation d'ordre total** si

$$\boxed{\forall (x, y) \in E^2, x\mathcal{R}y \text{ ou } y\mathcal{R}x.}$$

C'est une **relation d'ordre partiel** sinon.

Exemples - • La relation \leq dans \mathbb{R} est une relation d'ordre total.
 • Soit $X = \{0, 1, 2\}$, la relation \subset dans l'ensemble $E = \mathcal{P}(X)$ est une relation d'ordre partiel. En effet, si on considère les éléments $A = \{0\}$ et $B = \{1\}$ de $\mathcal{P}(X)$, on n'a ni $A \subset B$ ni $B \subset A$.

2.3. Etude des relations d'équivalence

Fixons une relation d'équivalence \mathcal{R} dans un ensemble E . La notation $x\mathcal{R}y$ se lit souvent “ x et y sont équivalents pour \mathcal{R} ”.

Définition 5.14 – Soit x un élément de E . On appelle **classe d'équivalence de x** l'ensemble qu'on notera ici \bar{x} :

$$\boxed{\bar{x} = \{y \in E \mid y\mathcal{R}x\}.}$$

L'ensemble des classes d'équivalence est appelé **l'ensemble quotient** de E par la relation \mathcal{R} . On le note E/\mathcal{R} .

Exemples - • Dans l'exemple 1 ci-dessus, on a $\bar{x} = \{x\}$
 • Dans l'exemple 6, si x est pair, on a $\bar{x} = 2\mathbb{Z}$ et si x est impair, on a $\bar{x} = 2\mathbb{Z} + 1$. On a $\mathbb{Z}/\mathcal{R} = \{\bar{0}, \bar{1}\}$. On voit que $x \equiv y$ est équivalent à $\bar{x} = \bar{y}$ et que les deux classes distinctes forment une partition de \mathbb{Z} .

Exercice - Soit $E = \mathbb{R}$. Montrer qu'on définit une relation d'équivalence sur E par : pour $(x, y) \in E^2$, $x \mathcal{R} y$ si $x^2 = y^2$. Déterminer E/\mathcal{R} .

Ceci se généralise par le théorème suivant :

Théorème 5.15 – 1 – Soit x un élément de E , on a : $x \in \bar{x}$.
 2 – Soient x et y des éléments de E . On a l'équivalence :

$$\boxed{x \mathcal{R} y \Leftrightarrow \bar{x} = \bar{y}.}$$

3 – Les classes d'équivalence distinctes forment une partition de E .

Preuve :

- 1) Puisque \mathcal{R} est réflexive, on a $x \mathcal{R} x$ pour tout élément x de E , donc $x \in \bar{x}$.
- 2) Supposons $x \mathcal{R} y$. Montrons que l'on a $\bar{y} \subset \bar{x}$. Soit z un élément de \bar{y} ; on a donc $y \mathcal{R} z$; comme \mathcal{R} est transitive et que l'on a ($x \mathcal{R} y$ et $y \mathcal{R} z$), on obtient $x \mathcal{R} z$; donc $z \in \bar{x}$. On a montré que $\bar{y} \subset \bar{x}$. Comme \mathcal{R} est symétrique et $x \mathcal{R} y$, on a aussi $y \mathcal{R} x$. En échangeant les rôles de x et y , on obtient de même $\bar{x} \subset \bar{y}$. On a montré que l'on a $\bar{x} \subset \bar{y}$ et $\bar{y} \subset \bar{x}$; on a donc $\bar{x} = \bar{y}$.
 Supposons $\bar{x} = \bar{y}$; on a $x \in \bar{x}$ donc $x \in \bar{y}$, c'est à dire $y \mathcal{R} x$; comme \mathcal{R} est symétrique, on a aussi $x \mathcal{R} y$.
 On a montré l'équivalence ($x \mathcal{R} y \Leftrightarrow \bar{x} = \bar{y}$).
- 3) La classe \bar{x} d'un élément x de E contient x d'après 1; elle est donc non vide.

Montrons que deux classes distinctes sont disjointes, et pour cela supposons $\bar{x} \cap \bar{y} \neq \emptyset$ et

montrons $\bar{x} = \bar{y}$. Soit z un élément de l'ensemble $\bar{x} \cap \bar{y}$; on a ($x \mathcal{R} z$ et $y \mathcal{R} z$) donc

$\bar{x} = \bar{z} = \bar{y}$; d'où le résultat.

Notons E' la réunion des classes : $E' = \bigcup_{x \in E} \bar{x}$ et montrons que $E = E'$. Soit x

un élément de E . On a $x \in \bar{x}$, donc $x \in E'$; on obtient $E \subset E'$. Comme on a évidemment

$E' \subset E$, on obtient $E = E'$.

De tout ceci, on déduit le résultat 3.

D'après la deuxième partie de la proposition, l'équivalence se ramène à l'égalité des classes. Pour illustrer ceci, considérons l'exemple 4 : si on appelle *direction* d'une droite D la classe d'équivalence de D , dire que deux droites sont parallèles revient à dire qu'elles ont même direction et l'ensemble quotient est l'ensemble des directions du plan.

Plus généralement si \mathcal{R} est une relation d'équivalence sur un ensemble E , on peut construire l'application $f : \begin{matrix} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & \bar{x} \end{matrix}$. Dire que $x\mathcal{R}y$ équivaut à dire que $f(x) = f(y)$. Les classes d'équivalence sont exactement les ensembles $f^{-1}(\{y\})$ où y décrit E/\mathcal{R} .

Inversement, si f est une application d'un ensemble E dans un ensemble F , on peut considérer la relation d'équivalence ($x\mathcal{R}y \Leftrightarrow f(x) = f(y)$) sur E . Ses classes d'équivalence sont les ensembles $f^{-1}(\{y\})$ où y décrit l'image de f . D'après ce qui précède, toutes les relations d'équivalence sont obtenues ainsi.

2.4. Relations d'ordre

Dans la suite, on se contentera d'étudier les relations \leq dans $E = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou \mathbb{R} .

Définition 5.16 – Soient A un sous-ensemble de E et M un élément de E .

1 – On dit que M est un **majorant** de A si pour tout élément a de A , on a : $a \leq M$.

2 – On dit que M est un **plus grand élément** de A si M est un majorant de A et si M **appartient à** A . On le note $\max A$.

3 – On définit de même la notion de **minorant** et celle de **plus petit élément** (noté $\min A$).

Proposition 5.17 – S'il existe un plus grand élément de A , il est **unique**.

Preuve : si a et a' sont deux plus grands éléments de A , a est un élément de A et a' majore A , donc $a \leq a'$; de même en échangeant les rôles de a et a' , on obtient $a' \leq a$. Comme la relation \leq est antisymétrique, on obtient $a = a'$. On peut donc dire qu'un élément a est le plus grand (ou le plus petit) élément de A . \square

Exemples -

- Considérons la relation d'ordre \leq dans $E = \mathbb{R}$ et soit $A = [0, 1[$. Alors, les majorants de A sont les réels M tels que $1 \leq M$, les minorants de A sont les réels m tels que $m \leq 0$, A a 0 pour plus petit élément, mais A n'a pas de plus grand élément.

- Considérons la relation d'ordre \leq dans $E = \mathbb{N}$ et soit $A = \{x \in \mathbb{N} \mid x^2 \leq 2\}$. Alors, $A = \{0, 1\}$, 0 est le seul minorant de A et c'est le plus petit élément de A ; les majorants de A sont les entiers naturels non nuls et 1 est le plus grand élément de A .

Définition 5.18 – Soient A un sous-ensemble de E et M un élément de E . On dit que M est une **borne supérieure** de A si M est un plus petit élément de l'ensemble des majorants de A , c'est à dire si les deux conditions suivantes sont vérifiées :

- 1) M est un majorant de A
- 2) Si M' est un autre majorant de A , alors $M \leq M'$.

ou de façon équivalente si :

- 1) M est un majorant de A .
- 2) Si $M' < M$, il existe un élément a de A tel que $M' < a \leq M$.

On définit de même une borne inférieure.

Exercice - Ecrire avec des quantificateurs la définition d'une borne supérieure et d'une borne inférieure.

Exemples et remarques

- 1) Reprenons le premier exemple ci-dessus. L'ensemble $A = [0, 1[$ admet 0 comme borne inférieure et 1 comme borne supérieure.
- 2) S'il existe une borne supérieure de A , elle est unique. On peut donc dire qu'un élément M est la borne supérieure de A et noter $M = \sup A$. De même, on parle de la borne inférieure de A et on note $m = \inf A$.
- 3) Si A a une borne supérieure et si elle appartient à A , c'est le plus grand élément de A et inversement, un plus grand élément est une borne supérieure. Le premier exemple montre cependant que $\sup A$ n'est pas forcément un plus grand élément.
- 4) Pour que la borne supérieure existe, il est évidemment nécessaire que l'ensemble soit majoré. Mais ce n'est pas toujours suffisant. Par exemple, dans l'ensemble \mathbb{Q} muni de la relation \leq , considérons le sous-ensemble $A = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$. Il est majoré (par 3 par exemple). Mais A n'a pas de borne supérieure ; en effet, s'il existe une borne supérieure M , on peut montrer qu'elle vérifie $M^2 = 2$; mais il est facile de montrer qu'il n'existe pas de rationnel M tel que $M^2 = 2$ (essayez) ; on aboutit donc à une contradiction.
- 5) Par contre l'ensemble \mathbb{R} muni de la relation \leq possède la propriété fondamentale suivante :

Tout sous-ensemble non vide et majoré de \mathbb{R} admet une borne supérieure.

et de même :

Tout sous-ensemble non vide et minoré de \mathbb{R} admet une borne inférieure.

Cette propriété est à la base de nombreux théorèmes d'analyse. Nous y reviendrons au cours du chapitre sur les suites réelles. Elle permet par exemple de démontrer l'existence de $\sqrt{2}$: en effet, le sous-ensemble de \mathbb{R} égal à $\{x \in \mathbb{R} \mid x^2 \leq 2\}$ a une borne supérieure a , et on peut montrer que l'on a $a^2 = 2$.

Chapitre 6

Arithmétique

1. Divisibilité

1.1. Entiers naturels

On note \mathbb{N} l'ensemble des *entiers naturels*.

Le raisonnement par récurrence s'applique aux propositions dont l'énoncé dépend d'un entier naturel n . Il est une conséquence de la construction de l'ensemble des entiers naturels \mathbb{N} (basée sur les axiomes de Peano). Ce raisonnement a été vu dans le chapitre sur les démonstrations.

Voici deux autres propriétés des entiers naturels qui nous seront utiles :

- *Un ensemble non vide d'entiers naturels a un plus petit élément.*
Soit B un sous-ensemble de \mathbb{N} , et supposons qu'il n'a pas de plus petit élément. Soit A l'ensemble des entiers naturels n tels qu'aucun entier naturel inférieur ou égal à n n'appartienne à B . Alors
 - 1) 0 appartient à A , sinon 0 serait le plus petit élément de B ,
 - 2) si n appartient à A , alors $n + 1$ appartient à A , sinon $n + 1$ serait le plus petit élément de B .

Donc A est égal à \mathbb{N} , et B est vide. Le raisonnement qu'on vient de faire est un raisonnement par récurrence.

- *Une suite strictement décroissante d'entiers naturels est toujours finie (il n'y a pas de suite infinie strictement décroissante).*
Supposons qu'il y ait une suite (a_n) strictement décroissante d'entiers naturels. Alors, d'après la propriété précédente, l'ensemble des a_n , qui est non vide, a un plus petit élément, disons a_N . On devrait avoir $a_{N+1} < a_N$, ce qui contredit le fait que a_N est le plus petit élément.

1.2. Entiers relatifs

On note \mathbb{Z} l'ensemble des *entiers relatifs*. On rappelle quelques propriétés algébriques de \mathbb{Z} , pour l'addition et la multiplication.

Addition

- 1) (*associativité*) Quels que soient les entiers relatifs m, n, p ,

$$(m + n) + p = m + (n + p).$$

- 2) (*commutativité*) Quels que soient les entiers relatifs m, n ,

$$m + n = n + m.$$

DIVISIBILITÉ

3) (*0 est élément neutre*) Quel que soit l'entier relatif m ,

$$0 + m = m + 0 = m.$$

4) (*existence d'un opposé*) Quel que soit l'entier relatif m , il existe un entier relatif n tel que

$$m + n = n + m = 0.$$

Multiplication

5) (*associativité*) Quels que soient les entiers relatifs m, n, p ,

$$(m n) p = m (n p).$$

6) (*commutativité*) Quels que soient les entiers relatifs m, n ,

$$m n = n m.$$

7) (*1 est élément neutre*) Quel que soit l'entier relatif m ,

$$1 m = m 1 = m.$$

8) (*distributivité par rapport à l'addition*) Quels que soient les entiers relatifs m, n, p ,

$$m(n + p) = m n + m p \quad (n + p) m = n m + p m.$$

Les quatre propriétés pour l'addition font de \mathbb{Z} un *groupe commutatif*. Quelle propriété manque-t-il à \mathbb{N} , muni de l'addition, pour être un groupe commutatif ?

Les propriétés de groupe commutatif pour l'addition, plus les quatre propriétés pour la multiplication, font de \mathbb{Z} un *anneau commutatif*.

En plus de ces propriétés d'anneau commutatif, on peut "faire des simplifications" dans \mathbb{Z} . Si $a \neq 0$ et $ab = 0$, alors $b = 0$. Aussi, si $a \neq 0$ et $ab = ac$, alors $b = c$; ceci est une conséquence de la propriété précédente, car $ab = ac$ peut se réécrire $a(b - c) = 0$, d'où il vient $b - c = 0$. Tous les anneaux commutatifs n'ont pas cette propriété de simplification : nous verrons des exemples plus loin, à propos des congruences.

1.3. La division euclidienne, relation de divisibilité

La *division euclidienne* est la “division avec reste” des entiers naturels. On rappelle ce qui la caractérise.

Proposition 6.1 – Soient a et b deux entiers naturels avec $b \neq 0$. Alors il existe deux entiers naturels q (*quotient*) et r (*reste*) tels que

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

De plus il y a **unicité** du couple d’entiers (q, r) vérifiant cette propriété.

Exemple - La division euclidienne de 223 par 12 est $223 = 12 \times 18 + 7$. 7 est le reste et 18 le quotient.

Remarque - La condition $0 \leq r < b$ est équivalente à $0 \leq r \leq b - 1$ car r et b sont des entiers naturels.

Preuve : soit b un entier strictement positif, et soit A l’ensemble des entiers naturels n tels qu’il existe un entier naturel s vérifiant $n < bs$. Alors

- 0 appartient à A car $0 < b$,
- si n appartient à A , il existe s dans \mathbb{N} tel que $n < bs$ et alors $n + 1 < bs + b = b(s + 1)$, donc $n + 1$ appartient à A .

On en déduit que $A = \mathbb{N}$. Si a est un entier naturel quelconque, il existe s dans \mathbb{N} tel que $a < bs$. Soit t le plus petit de ces entiers. Forcément on a $t > 0$ car $b0 = 0 \leq a$. Posons $q = t - 1$ et $r = a - bq$; comme $bq \leq a < b(q + 1)$, on a bien $0 \leq r < b$ et $a = bq + r$.

S’il y a un autre couple (q_1, r_1) tel que $a = bq_1 + r_1$ et $0 \leq r_1 < b$, alors $0 = b(q - q_1) + (r - r_1)$, d’où $b|q - q_1| = |r - r_1| < b$, ce qui n’est possible que si $q_1 = q$, et alors $r_1 = r$. Le couple (q, r) est défini de manière unique. \square

Division euclidienne dans \mathbb{Z} .

Nous aurons aussi besoin de la division euclidienne de a par b quand a est un entier relatif. Le quotient q est alors un entier relatif, et on demande toujours que le reste r vérifie $0 \leq r < b$. Il faut examiner le cas où $a < 0$. On a par la division euclidienne des entiers naturels

$$-a = bq_1 + r_1 \quad \text{avec} \quad 0 \leq r_1 < b.$$

Si $r_1 = 0$, alors $a = b(-q_1)$ convient. Sinon, on a

$$a = b(-q_1) - r_1 = b(-1 - q_1) + (b - r_1)$$

et on prend $q = -1 - q_1$, et $r = b - r_1$ qui vérifie $0 < r < b$. Le couple (q, r) est également défini de manière unique.

Définition 6.2 – Soient a et b deux entiers naturels. Par définition, on dit que a **divise** b quand il existe un entier naturel q tel que $b = aq$ (la division

“tombe juste”, son reste est nul). On dit aussi que a est un **diviseur** de b , ou que b est un **multiple** de a . On notera $a \mid b$ pour “ a divise b ”.

Remarque - Ne pas confondre $a \mid b$ qui signifie “ a divise b ” et a/b qui est la fraction de a par b .

Voici quelques propriétés de la relation de divisibilité sur l’ensemble des entiers naturels.

- 1) (*réflexivité*) Quel que soit l’entier naturel a ,

$$a \mid a.$$
- 2) (*antisymétrie*) Quels que soient les entiers **naturels** a, b ,

$$(a \mid b \text{ et } b \mid a) \implies a = b.$$
- 3) (*transitivité*) Quels que soient les entiers naturels a, b, c ,

$$(a \mid b \text{ et } b \mid c) \implies a \mid c.$$

L’ordre usuel \leq sur les entiers naturels est bien sûr une relation d’ordre sur \mathbb{N} . **La divisibilité est aussi une relation d’ordre sur \mathbb{N} .** L’ordre usuel est un *ordre total*, ce qui signifie que quels que soient les entiers naturels a et b , on a $a \leq b$ ou $b \leq a$. Cette propriété n’est pas vraie pour la divisibilité : 2 ne divise pas 3, et 3 ne divise pas 2. La relation de divisibilité n’est pas un ordre total.

On remarque que si $a \mid b$ et $b \neq 0$, alors $a \leq b$. Ceci montre qu’un entier naturel non nul a un nombre fini de diviseurs.

On étend la relation de divisibilité aux entiers relatifs : l’entier relatif a divise l’entier relatif b quand il existe un entier relatif q tel que $b = qa$ (on dit aussi que a est un diviseur de b , ou que b est un multiple de a). La relation de divisibilité n’est plus une relation d’ordre sur les entiers relatifs ; quelle est la propriété qui est prise en défaut dans ce cas ? Les questions de divisibilité sur les entiers relatifs se ramènent à celles sur les entiers naturels : l’entier relatif a divise l’entier relatif b si et seulement si l’entier naturel $|a|$ divise l’entier naturel $|b|$.

On remarque que 1 (et -1) divisent tous les entiers, et que tous les entiers divisent 0. Si a divise b et c , alors il divise $b + c$. Si a divise b , alors ac divise bc (et réciproquement pour $c \neq 0$).

2. Congruences

2.1. Relation de congruence. Classes de congruence

Définition 6.3 – Soit n un entier supérieur ou égal à 2. On dit que deux entiers relatifs a et b sont **congrus modulo n** quand n divise $a - b$. On note $a \equiv b \pmod{n}$.

$$a \equiv b \pmod{n} \iff [\exists k \in \mathbb{Z}, a - b = kn]$$

Exemple - $12 \equiv 2 \pmod{5}$.

La relation de congruence modulo n vérifie les propriétés suivantes :

1) (*réflexivité*) Quel que soit l'entier relatif a ,

$$a \equiv a \pmod{n}.$$

2) (*symétrie*) Quels que soient les entiers relatifs a et b ,

$$a \equiv b \pmod{n} \iff b \equiv a \pmod{n}.$$

3) (*transitivité*) Quels que soient les entiers relatifs a , b et c ,

$$[a \equiv b \pmod{n} \text{ et } b \equiv c \pmod{n}] \implies a \equiv c \pmod{n}.$$

La vérification de la réflexivité et de la symétrie est immédiate.

Pour la transitivité, si n divise $(a - b)$ et n divise $(b - c)$, alors n divise $(a - b) + (b - c) = a - c$.

Proposition 6.4 – La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} .

Les classes d'équivalence de la relation de congruence modulo n s'appellent des classes de congruence modulo n .

Soit a un entier relatif, et r le reste de la division euclidienne de a par n . Alors $a \equiv r \pmod{n}$. **Deux entiers relatifs sont congrus modulo n si et seulement si ils ont même reste dans la division euclidienne par n** (vérifier!).

Proposition 6.5 – La **classe de congruence modulo n** d'un entier relatif a est l'ensemble de tous les entiers relatifs qui sont congrus à a modulo n .

Autrement dit, c'est l'ensemble des entiers relatifs de la forme $a + nq$ où q est un entier relatif quelconque. Cette description montre que la notation naturelle pour la classe de congruence de a modulo n serait $a + n\mathbb{Z}$. Cependant on utilisera la notation \bar{a} qui est moins précise (car elle ne fait pas référence à n), mais qui a l'avantage d'être courte. Dire que la classe de congruence de a modulo n est égale à la classe de congruence de b modulo n revient à dire que a est congru à b modulo n . Voici par exemple la liste des classes de congruence modulo 5 : sur chaque ligne figure une classe de congruence.

$$\begin{aligned} \bar{0} &= \{ \dots -15 \ -10 \ -5 \ 0 \ 5 \ 10 \ 15 \ \dots \} \\ \bar{1} &= \{ \dots -14 \ -9 \ -4 \ 1 \ 6 \ 11 \ 16 \ \dots \} \\ \bar{2} &= \{ \dots -13 \ -8 \ -3 \ 2 \ 7 \ 12 \ 17 \ \dots \} \\ \bar{3} &= \{ \dots -12 \ -7 \ -2 \ 3 \ 8 \ 13 \ 18 \ \dots \} \\ \bar{4} &= \{ \dots -11 \ -6 \ -1 \ 4 \ 9 \ 14 \ 19 \ \dots \} \end{aligned}$$

Sur la troisième ligne, on a $\bar{2}$, qui est la même chose que $\bar{17}$, ou que $\overline{-13}$. Cet exemple est une illustration de la proposition suivante.

Proposition 6.6 – Il y a n classes de congruence modulo n , qui sont $\bar{0}$, $\bar{1}, \dots, \overline{n-1}$.

Preuve : tout d'abord, ces classes de congruence sont bien distinctes. Si k et l sont deux entiers différents avec $0 \leq k < n$ et $0 \leq l < n$,

alors n ne divise pas $k - l$ et donc les classes de congruence \bar{k} et \bar{l} sont différentes. Ensuite, on obtient bien ainsi toutes les classes de congruence. Si a est un entier relatif quelconque, sa classe de congruence modulo n est égale à celle de son reste dans la division euclidienne par n . Donc \bar{a} est égale à l'une des classes $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

□

En fait, dans cette démonstration, on a répété ce qu'on a dit plus haut : a et b sont congrus modulo n si et seulement s'ils ont même reste dans la division par n .

Définition 6.7 – L'ensemble des n classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

2.2. Opérations sur les congruences

Théorème 6.8 – Soient a, b, c et d quatre entiers relatifs qui vérifient $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors

$$\begin{cases} -a \equiv -b \pmod{n}, \\ a + c \equiv b + d \pmod{n}, \\ ac \equiv bd \pmod{n}. \end{cases}$$

Preuve : par hypothèse, n divise $a - b$ et $c - d$. L'item 1 est très facile à démontrer.

Vérifions l'item 2. On a $(a + c) - (b + d) = (a - b) + (c - d)$, donc n divise $(a + c) - (b + d)$.

Vérifions l'item 3. On a $ac - bd = c(a - b) + b(c - d)$, donc n divise $ac - bd$. □

Les règles qui figurent dans le théorème permettent de faire rapidement des "calculs modulo n ". Par exemple, calculons $1! + 2! + 3! + 4! + 5! + 6!$ modulo 7. On a (toutes les congruences sont modulo 7) :

$$4! \equiv 3 \quad 5! \equiv 3 \times 5 \equiv 1 \quad 6! \equiv 5! \times 6 \equiv 6,$$

d'où $1! + 2! + 3! + 4! + 5! + 6! \equiv 1 + 2 + 6 + 3 + 1 + 6 \equiv 5$, autrement dit le reste de la division euclidienne de $1! + 2! + 3! + 4! + 5! + 6!$ par 7 est 5.

Les résultats du théorème permettent de définir l'addition et la multiplication de classes de congruence modulo n . Le deuxième résultat nous dit par exemple que, pour $\bar{a} = \bar{b}$ et $\bar{c} = \bar{d}$, alors $\overline{a + b} = \overline{c + d}$. On peut donc poser

$$\bar{a} + \bar{c} = \overline{a + c}$$

sans risquer de problème : si on remplace a par b et c par d , on trouve bien le même résultat. Prenons l'exemple des classes de congruence modulo 5 que

nous avons décrites ci-dessus. On pose $\bar{1} + \bar{2} = \bar{3}$. On pose aussi $\overline{-4} + \overline{12} = \bar{8}$. A gauche on a $\bar{1} = \overline{-4}$ et $\bar{2} = \overline{12}$, donc les deux résultats à droite doivent être égaux. C'est bien le cas, $\bar{3} = \bar{8}$. Dressons les tables d'addition et de multiplication dans $\mathbb{Z}/5\mathbb{Z}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Quelles sont les propriétés vérifiées par l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$? On a par exemple

$$\bar{a} \times \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \times \bar{a}$$

qui montre la commutativité de la multiplication des classes de congruence. Ainsi, on a des propriétés qui sont "héritées" de celles de l'addition et de la multiplication sur \mathbb{Z} . L'addition des classes de congruence modulo n est associative, commutative, a un élément neutre $\bar{0}$ et toute classe \bar{a} a un opposé $\overline{-a}$. La multiplication est associative, commutative, a un élément neutre $\bar{1}$ et est distributive par rapport à l'addition. Au total, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

⚠ Un élément de $\mathbb{Z}/n\mathbb{Z}$ n'admet pas toujours un inverse pour la multiplication. Ce fait oblige à changer ses habitudes de calcul, en particulier pour la simplification dans la multiplication des classes de congruence

$$\bar{a} \times \bar{b} = \bar{a} \times \bar{c} \text{ et } \bar{a} \neq \bar{0} \text{ n'entraînent pas toujours } \bar{b} = \bar{c}.$$

Par exemple $\bar{9} \times \bar{1} = \bar{9} \times \bar{5}$ et $\bar{9} \neq \bar{0}$, mais $\bar{1} \neq \bar{5}$ dans $\mathbb{Z}/12\mathbb{Z}$.

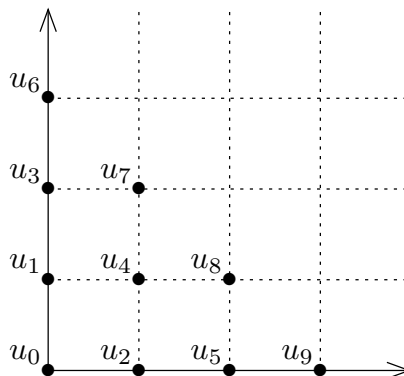
⚠ De même, si $\bar{ac} = \bar{0}$, cela ne veut pas dire $\bar{a} = \bar{0}$ ou $\bar{c} = \bar{0}$. Par exemple, $\bar{2} \times \bar{3} = \bar{0}$ dans $\mathbb{Z}/6\mathbb{Z}$.

3. Ensembles finis ou dénombrables (pour votre culture générale)

Théorème 6.9 – Un ensemble E non vide est **fini** s'il existe un entier $n \in \mathbb{N}^*$ et une bijection $f : \{1, 2, \dots, n\} \rightarrow E$. Le nombre n est alors unique et on l'appelle le **cardinal** ou le nombre d'éléments de E . On convient que \emptyset est fini et de cardinal 0. Un ensemble qui n'est pas fini est dit infini.

Définition 6.10 – Un ensemble E est **dénombrable** s'il existe une surjection u de \mathbb{N} sur E .

Exemples - • L'ensemble \mathbb{N} est infini et dénombrable.
 • $\mathbb{N} \times \mathbb{N}$ est dénombrable : pour le voir, on numérote ses éléments comme sur le dessin ci-dessous :



• On peut montrer qu'un produit fini d'ensembles dénombrables est dénombrable, qu'un sous-ensemble d'un ensemble dénombrable est dénombrable et qu'une réunion finie d'ensembles dénombrables est dénombrable. On déduit de ce qui précède que \mathbb{Z} et \mathbb{Q} sont dénombrables.

• Mais $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable. Raisonnons par l'absurde. Si $\mathcal{P}(\mathbb{N})$ est dénombrable, il existe une surjection de \mathbb{N} sur $\mathcal{P}(\mathbb{N})$. Soit u une telle surjection. Alors $\forall n \in \mathbb{N}$, $u(n)$ est un sous-ensemble de \mathbb{N} . Soit $E = \{n \in \mathbb{N} \mid n \notin u(n)\}$. On a $E \subset \mathbb{N}$ donc $E \in \mathcal{P}(\mathbb{N})$; comme u est surjective, E a au moins un antécédent par u ; soit $n \in \mathbb{N}$ un antécédent de E ; on a donc $E = u(n)$. Pour un tel n , il y a deux possibilités : $n \in E$ ou $n \notin E$. Si $n \in E$, par définition $n \notin u(n)$, c'est-à-dire $n \notin E$ et on a une contradiction. De même, si $n \notin E$, on a $n \in u(n)$, c'est-à-dire $n \in E$ et on aboutit encore à une contradiction. L'hypothèse de départ est donc absurde et on en déduit le résultat.

• On en déduit que l'ensemble des suites d'entiers n'est pas dénombrable, non plus que \mathbb{R} .

EXERCICES D'APPLICATION

Exercice n°1

Quel est le reste de la division par 7 de 247^{349} , de la division par 13 de 100^{1000} ?

Exercice n°2

Montrer que le produit de trois entiers consécutifs est divisible par 3.

Exercice n°3

Résoudre dans \mathbb{Z} le système suivant

$$\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 2 \pmod{15} \end{cases}$$

Exercice n°4

- 1) Calculer les carrés des éléments de $\mathbb{Z}/5\mathbb{Z}$.
- 2) Résoudre, dans $\mathbb{Z}/5\mathbb{Z}$, l'équation $\bar{x}^2 + 2\bar{y}^2 = \bar{0}$.

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°1

On obtient $247^{349} \equiv 2 \pmod{7}$ en utilisant $247 \equiv 2 \pmod{7}$ et $2^3 \equiv 1 \pmod{7}$.
On obtient $100^{1000} \equiv 9 \pmod{13}$ en utilisant $100 \equiv 9 \pmod{13}$ et $9^6 \equiv 1 \pmod{13}$.

Exercice n°2

Soit $n, n+1$ et $n+2$ trois entiers consécutifs. On a $n \equiv 0 \pmod{3}$ ou $n \equiv 1 \pmod{3}$ ou $n \equiv 2 \pmod{3}$. Etudier chacun de ces cas.

Exercice n°3

On écrit : $x \equiv 7 \pmod{10} \iff (\exists k \in \mathbb{Z}, x = 7 + 10k)$. On en déduit que

$$\begin{aligned} x \equiv 2 \pmod{15} &\iff 7 + 10k \equiv 2 \pmod{15} \iff 10k \equiv -5 \pmod{15} \\ &\iff 2k \equiv -1 \pmod{3} \iff 2k \equiv 2 \pmod{3} \\ &\iff k \equiv 1 \pmod{3} \text{ en multipliant par } \bar{2}. \end{aligned}$$

On en déduit qu'il existe $p \in \mathbb{Z}$ tel que $k = 1 + 3p$ et $x = 7 + 10(1 + 3p) = 17 + 30p$, donc $x \equiv 17 \pmod{30}$.

Exercice n°4

- 1) $\bar{x}^2 \in \{\bar{0}, \bar{1}, \bar{4}\}$
- 2) Faire un tableau à deux entrées en utilisant la première question.

Chapitre 7

Nombres réels et suites réelles

1. Les nombres réels

La démarche que nous allons suivre est de partir d'une liste (aussi restreinte que possible) de propriétés des nombres réels (les *axiomes*) que nous admettrons. Le premier axiome est que \mathbb{R} est un corps ordonné contenant \mathbb{Q} et le second est celui de la borne supérieure. Nous redémontrerons toutes les autres propriétés que nous utiliserons à partir de ces axiomes. En fait nous ne nous donnerons pas la peine de redémontrer à partir des axiomes les propriétés classiques sur les manipulations d'identités algébriques ou d'inégalités. Nous nous attacherons surtout à *démontrer* les propriétés concernant les limites de suites. Pour démontrer ces propriétés, il faut avoir une définition précise de la notion de limite de suite.

Nous donnerons plus loin des indications sur la manière de construire, à partir des nombres rationnels, un ensemble des nombres réels qui vérifie les axiomes que l'on a posés.

1.1. \mathbb{R} est un corps commutatif totalement ordonné

On note \mathbb{R} l'ensemble des nombres réels. Il contient l'ensemble des nombres rationnels \mathbb{Q} , et est muni de deux opérations (addition et multiplication) qui vérifient les propriétés suivantes.

1) L'addition est associative :

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

2) L'addition a un élément neutre 0 :

$$\forall x \in \mathbb{R}, \quad x + 0 = 0 + x = x.$$

3) Tout nombre réel a un opposé pour l'addition :

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \quad x + y = y + x = 0.$$

L'opposé d'un nombre réel x est unique : si y et z vérifient tous les deux $x + y = y + x = 0$ et $x + z = z + x = 0$, alors

$$y = y + 0 = y + (x + z) = (y + x) + z = 0 + z = z.$$

On désigne par $-x$ l'opposé de x .

4) L'addition est commutative :

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

\mathbb{R} est donc un *groupe commutatif*.

5) La multiplication est associative :

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

6) La multiplication a un élément neutre 1 :

\mathbb{R} EST UN CORPS COMMUTATIF TOTALEMENT ORDONNÉ

$$\forall x \in \mathbb{R}, \quad x \times 1 = 1 \times x = x.$$

7) La multiplication est distributive par rapport à l'addition :

$$\begin{aligned} \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \forall z \in \mathbb{R}, \quad x \times (y + z) &= (x \times y) + (x \times z) \\ (y + z) \times x &= (y \times x) + (z \times x). \end{aligned}$$

8) La multiplication est commutative :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad x \times y = y \times x.$$

\mathbb{R} est un *anneau commutatif*.

9) 0 est différent de 1 et tout nombre réel x différent de 0 a un inverse pour la multiplication :

$$\forall x \in \mathbb{R}, \quad (x \neq 0 \implies (\exists y \in \mathbb{R}, \quad x \times y = y \times x = 1)).$$

Un tel inverse est unique (même démonstration que pour l'opposé pour l'addition) et on le note x^{-1} .

\mathbb{R} est un *corps*. Comme autre corps, on connaît le corps \mathbb{Q} des rationnels (les fractions), le corps \mathbb{C} des nombres complexes.

On utilise les notations habituelles pour la soustraction et la division : $x - y$ désigne $x + (-y)$ et x/y désigne $x \times y^{-1}$. On omet le plus souvent le symbole \times pour écrire les multiplications.

10) \mathbb{R} est muni d'une relation d'ordre \leq :

$$\begin{array}{lll} \forall x \in \mathbb{R}, & x \leq x & \text{(réflexivité),} \\ \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \forall z \in \mathbb{R}, & ((x \leq y \text{ et } y \leq z) \implies x \leq z) & \text{(transitivité),} \\ \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, & ((x \leq y \text{ et } y \leq x) \implies x = y) & \text{(antisymétrie).} \end{array}$$

11) L'ordre \leq est total :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad (x \leq y \text{ ou } y \leq x).$$

12) L'ordre \leq est compatible avec l'addition :

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

13) Le produit de deux réels positifs ou nuls est positif ou nul :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad ((0 \leq x \text{ et } 0 \leq y) \implies 0 \leq xy).$$

Un corps muni en plus d'une relation d'ordre vérifiant les propriétés 10–13 est appelé un *corps totalement ordonné*. Les corps \mathbb{Q} et \mathbb{R} sont des corps totalement ordonnés.

A titre d'exemple, montrons en utilisant ces propriétés 12 et 13 que si $0 \leq c$ et $a \leq b$, alors $ac \leq bc$. En utilisant 12, on a $0 = a + (-a) \leq b - a$. En utilisant 13, on a $0 \leq c(b - a) = cb - ca$. Enfin, en utilisant de nouveau 12, $ca = 0 + ca \leq (cb - ca) + ca = cb$.

Exercice - 1°) Montrer que si un élément x d'un corps ordonné vérifie $x \leq 0$, alors $-x \geq 0$.

2°) Montrer que dans un corps ordonné un carré est positif ou nul. (Ecrire $x^2 = x \times x$ si $x \geq 0$ et $x^2 = (-x) \times (-x)$ si $x \leq 0$).

3°) Montrer qu'on ne peut pas définir d'ordre sur \mathbb{C} qui en fasse un corps ordonné. (En utilisant la question précédente montrer qu'on devrait avoir $0 \leq 1$ et $0 \leq -1$, et en déduire $0 = 1$).

On définit bien sûr la valeur absolue $|x|$ d'un élément x de \mathbb{R} par $|x| = x$ si $x \geq 0$ et $|x| = -x$ si $x \leq 0$. On rappelle la première inégalité triangulaire, très importante :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad |x + y| \leq |x| + |y|.$$

Cette inégalité peut se démontrer à partir des axiomes de corps ordonnés.

Exercice - 1°) Démontrer (en utilisant les axiomes de corps ordonnés et les résultats déjà vus) l'inégalité dans le cas $x \geq 0$ et $y \leq 0$, en distinguant suivant les possibilités $x + y \geq 0$ ou $x + y \leq 0$.

2°) Dans quels cas la première inégalité triangulaire est-elle une égalité?

A partir de la première inégalité triangulaire, on démontre la deuxième inégalité triangulaire :

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad \left| |x| - |y| \right| \leq |x - y|.$$

La démonstration se fait ainsi : on a $|x| = |(x - y) + y| \leq |x - y| + |y|$ par la première inégalité triangulaire, d'où $|x| - |y| \leq |x - y|$; de même $|y| \leq |y - x| + |x|$, d'où $|y| - |x| \leq |y - x|$. On en déduit la deuxième inégalité triangulaire.

Le plus gros du travail en analyse consiste à majorer, minorer, encadrer. Il est donc indispensable de savoir manipuler les inégalités.

Exercice - On suppose que $|x - 1| \leq 2$ et que $-5 \leq y \leq -4$. Encadrer les quantités suivantes :

$$1) x + y \quad 2) x - y \quad 3) xy \quad 4) \frac{x}{y} \quad 5) |x| - |y|.$$

1.2. Axiome de la borne supérieure

Définition 7.1 – Soient A une partie de \mathbb{R} et a un élément de \mathbb{R} . 1 – On dit que a est un majorant (respectivement un minorant) de A si, pour tout $x \in A$, $x \leq a$ (respectivement $x \geq a$).

2 – On dit que A est majorée (respectivement minorée) si elle possède un majorant (respectivement un minorant).

3 – On dit que A est bornée si elle est à la fois majorée et minorée.

Définition 7.2 – Soit A une partie de \mathbb{R} , on dit que A possède un plus grand (respectivement plus petit) élément s'il existe un élément **appartenant** à A qui majore (respectivement minore) A .

Proposition 7.3 – Si A possède un plus grand (respectivement plus petit) élément, celui-ci est unique.

Exercice - 1°) Démontrer la proposition.

2°) Trouver des parties de \mathbb{R} illustrant la définition de 'plus grand élément'.

Définition 7.4 – Soit A une partie majorée de \mathbb{R} . Si l'ensemble des majorants de A admet un plus petit élément, celui-ci est appelé borne supérieure de A et est noté $\sup A$.

Exemple - 1 est la borne supérieure de $[0, 1[$.

Proposition 7.5 – Soit A une partie majorée de \mathbb{R} . $M = \sup A$ si, et seulement si,

- 1) $\forall a \in A, \quad a \leq M$
- 2) $\forall \varepsilon > 0, \exists b \in A, \quad M - \varepsilon < b \leq M.$

On définit de manière analogue la borne inférieure d'une partie A de \mathbb{R} :

Définition 7.6 – Soit A une partie minorée de \mathbb{R} . Si l'ensemble des minorants admet un plus grand élément, celui-ci est appelé borne inférieure de A et est noté $\inf A$.

Exemple - 0 est la borne inférieure de $]0, 1]$.

Proposition 7.7 – Soit A une partie minorée de \mathbb{R} . $m = \inf A$ si, et seulement si,

- 1) $\forall a \in A, \quad m \leq a$
- 2) $\forall \varepsilon > 0, \exists b \in A, \quad m \leq b < m + \varepsilon.$

On voit que, si A possède un plus grand élément, celui-ci est sa borne supérieure et, s'il possède un plus petit élément, celui-ci est sa borne inférieure. Les exemples donnés montrent que les bornes supérieure et inférieure **n'appartiennent pas forcément** à A .

Nous admettrons comme propriété essentielle de \mathbb{R} , l'énoncé suivant, appelé **axiome de la borne supérieure**

Tout partie majorée non vide de \mathbb{R} admet une borne supérieure.

Remarque - Dans l'énoncé la précision "non vide" est nécessaire, car pour tout réel M la proposition " $\forall x \in \emptyset, x \leq M$ " est vraie. Donc \emptyset est majoré et pourtant l'ensemble des majorants, à savoir \mathbb{R} n'admet pas de plus petit élément.

De cette propriété, on déduit aussitôt :

Tout partie minorée non vide de \mathbb{R} admet une borne inférieure.

La démonstration est laissée en exercice.

Exercice - Pour chacun des sous-ensembles suivants de \mathbb{R} , dire s'il a un plus grand élément, un plus petit élément, une borne inférieure, une borne supérieure :

- 1) \mathbb{N} , 2) $[0, 1[$, 3) $\{1 + (1/n) ; n \in \mathbb{N}, n > 0\}$.

De l'axiome de la borne supérieure, on déduit le fait que \mathbb{R} est un corps archimédien, c'est-à-dire qu'il vérifie la propriété suivante :

$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists n \in \mathbb{N}, \quad n\varepsilon > x.$$

Démonstration : soit $x \in \mathbb{R}$ et $\varepsilon \in \mathbb{R}_+^* =]0, +\infty[$.

Supposons la proposition " $\exists n \in \mathbb{N}, n\varepsilon > x$ " fautive ; cela signifie que sa négation est vraie donc que : " $\forall n \in \mathbb{N}, n\varepsilon \leq x$ ".

Notons $A_\varepsilon = \{n\varepsilon ; n \in \mathbb{N}\}$; c'est une partie de \mathbb{R} non vide et majorée par x ; Elle admet donc une borne supérieure M . Puisque $M - \varepsilon < M$, il existe $n_0\varepsilon \in A_\varepsilon$ tel que $M - \varepsilon < n_0\varepsilon \leq M$. Il en résulte que $M < (n_0 + 1)\varepsilon$. Or $n_0 + 1 \in \mathbb{N}$, donc on obtient une contradiction car $(n_0 + 1)\varepsilon \in A_\varepsilon$. \square

Remarque - Le corps \mathbb{Q} des nombres rationnels est également archimédien.

Exercice - 1°) Soit $x \in \mathbb{R}$. Montrer :

- a) $(\forall \varepsilon > 0, 0 \leq x \leq \varepsilon) \implies x = 0$;
 b) $(\forall n \in \mathbb{N}^*, 0 \leq x \leq \frac{1}{n}) \implies x = 0$.
 2°) Soit $x \in \mathbb{R}$ et $y \in \mathbb{R}$. Montrer que :
 a) $(\forall \varepsilon > 0, 0 \leq |x - y| \leq \varepsilon) \implies x = y$;
 b) $(\forall n \in \mathbb{N}^*, 0 \leq |x - y| \leq \frac{1}{n}) \implies x = y$.

1.3. \mathbb{Q} est dense dans \mathbb{R} (pour votre culture générale)

Définition 7.8 - L'ensemble des nombres rationnels \mathbb{Q} , est égal au sous-ensemble de \mathbb{R} défini par

$$\left\{ r \in \mathbb{R} / \exists n \in \mathbb{Z} \quad \text{et} \quad \exists m \in \mathbb{Z}^*, \quad r = \frac{n}{m} \right\}.$$

Les éléments de \mathbb{Q} sont appelés les nombres rationnels et ceux de $\mathbb{R} \setminus \mathbb{Q}$ les nombres irrationnels.

Exercice - Montrer que \mathbb{Q} muni de l'addition et de la multiplication est un corps commutatif totalement ordonné.

Définition 7.9 – Un sous-ensemble A de \mathbb{R} est *dense* dans \mathbb{R} si et seulement si

$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists a \in A, \quad |x - a| < \varepsilon$$

Remarque - Cette condition peut s'écrire :

$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \quad]x - \varepsilon, x + \varepsilon[\cap A \neq \emptyset$$

Proposition 7.10 – Soient a et b deux nombres réels, avec $a < b$. Alors il existe un nombre rationnel r tel que $a < r < b$.

Autrement dit, entre deux nombres réels il y a toujours un nombre rationnel.
Démonstration : si $a < 0 < b$, on fait $r = 0$. Si $a < b \leq 0$, on travaille avec les opposés : $0 \leq -b < -a$. On peut donc supposer $0 \leq a < b$. On choisit un entier $h > 0$ tel que $1/h < b - a$ (c'est possible car \mathbb{R} est archimédien). Soit d le plus petit entier naturel d tel que $d/h > a$ (il y en a bien un, toujours grâce à l'archimédianité). Alors $(d - 1)/h \leq a$ et donc

$$\frac{d}{h} = \frac{d-1}{h} + \frac{1}{h} \leq a + \frac{1}{h} < b.$$

Donc le nombre rationnel d/h vérifie bien $a < d/h < b$. □

Théorème 7.11 – \mathbb{Q} est dense dans \mathbb{R} .

Démonstration : il suffit d'appliquer la proposition précédente aux réels distincts $x - \varepsilon$ et $x + \varepsilon$ □

Exercice - Montrer que $\sqrt{2}$ n'est pas rationnel.

On raisonne par l'absurde en posant $(p/q)^2 = 2$ où p et q sont des entiers, et en comparant les puissances de 2 dans les diviseurs de p^2 et de $2q^2$.

2. Suites de nombres réels

2.1. Suites convergentes

2.1.1. Définition d'une suite convergente

Définition 7.12 – Soit $(a_n)_{n \in \mathbb{N}}$ une suite de nombres réels. On dit que le nombre réel ℓ est *limite de la suite* (a_n) quand, pour tout nombre réel ε strictement positif, il existe un entier naturel N , tel que pour tout entier naturel n supérieur ou égal

à N on a $|a_n - \ell| < \varepsilon$.

La suite $(a_n)_{n \in \mathbb{N}}$ converge vers ℓ si et seulement si

$$[\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \quad (n \geq N \implies |a_n - \ell| < \varepsilon.)]$$

On dit qu'une suite de nombres réels est *convergente* quand elle a une limite dans \mathbb{R} . On remarque que dans la définition de limite, seul compte ce qui se passe "à la fin" : si dans la suite (a_n) on modifie les k premiers termes, en remplaçant a_0, \dots, a_{k-1} par des réels quelconques b_0, \dots, b_{k-1} , alors on ne change pas la nature de la suite (convergente ou non convergente), et si elle est convergente on ne change pas sa limite. En effet, on peut toujours prendre le N de la définition supérieur ou égal à k .

On s'autorisera donc de considérer des suites de nombres réels (a_n) qui ne sont bien définies que pour n supérieur à un certain entier. Par exemple, on parlera de la suite $(1/n)$ qui n'est définie que pour $n \geq 1$.

On dira qu'une suite (a_n) vérifie une propriété *à partir d'un certain rang* s'il existe un entier N tel que la propriété soit vérifiée pour tout entier $n \geq N$.

Exercice - 1°) Montrer que l'on peut aussi exprimer $\lim_{n \rightarrow \infty} a_n = \ell$ de la manière suivante :

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \quad (n \geq N \implies |a_n - \ell| \leq \varepsilon)$$

(on remplace $< \varepsilon$ par $\leq \varepsilon$). Indication : si $|a_n - \ell| \leq \varepsilon/2$ à partir du rang N , alors certainement $|a_n - \ell| < \varepsilon$ à partir du rang N .

2°) Montrer, en utilisant la définition, que les suites suivantes convergent vers 0

$$a_n = \frac{1}{n}, \quad a_n = \frac{1}{2^n}, \quad a_n = a^n \quad (\text{où } 0 < a < 1).$$

3°) Donner la définition d'une suite divergente.

2.1.2. Unicité de la limite

Proposition 7.13 – Soit (a_n) une suite réelle, $\ell \in \mathbb{R}$ et $\ell' \in \mathbb{R}$.

Si (a_n) converge vers ℓ et (a_n) converge vers ℓ' , alors $\ell = \ell'$.

Démonstration : supposons $\ell \neq \ell'$. Soit $\varepsilon = |\ell - \ell'|/2$. On devrait avoir d'une part un entier naturel N_1 tel que pour tout entier naturel $n \geq N_1$, $|a_n - \ell| < \varepsilon$, et d'autre part un entier naturel N_2 tel que pour tout entier

$n \geq N_2$, $|a_n - \ell'| < \varepsilon$. Si l'on prend n supérieur à la fois à N_1 et à N_2 , on devrait avoir

$$|\ell - \ell'| \leq |\ell - a_n| + |a_n - \ell'| < 2\varepsilon = |\ell - \ell'|.$$

On aboutit à une contradiction, donc une suite de nombres réels ne peut pas avoir plus d'une limite. \square

On note alors $\ell = \lim_{n \rightarrow \infty} a_n$ ou simplement $\ell = \lim a_n$. On dit aussi que (a_n) tend vers ℓ (quand n tend vers l'infini).

Exercice - 1°) Montrer l'équivalence des trois propriétés suivantes :

$$\text{a) } \lim a_n = \ell \quad \text{b) } \lim(a_n - \ell) = 0 \quad \text{c) } \lim |a_n - \ell| = 0.$$

2°) Montrer que si $\lim a_n = \ell$, alors $\lim |a_n| = |\ell|$. (La deuxième inégalité triangulaire sert !)

Pour étudier une suite, on se ramène souvent à une suite tendant vers 0. Le critère suivant est très utile.

Proposition 7.14 – Soit (a_n) une suite de nombres réels et $\ell \in \mathbb{R}$. S'il existe une suite (u_n) de nombres réels positifs tels que $|a_n - \ell| \leq u_n$ à partir d'un certain rang et $\lim_{n \rightarrow \infty} u_n = 0$, alors $\lim_{n \rightarrow \infty} a_n = \ell$.

Démonstration : donnons nous un réel $\varepsilon > 0$. Puisque $\lim_{n \rightarrow \infty} u_n = 0$, on a $u_n = |u_n - 0| < \varepsilon$ à partir d'un certain rang. Comme $|a_n - \ell| \leq u_n$ à partir d'un certain rang, on a aussi $|a_n - \ell| < \varepsilon$ à partir d'un certain rang et ceci montre que $\lim_{n \rightarrow \infty} a_n = \ell$. \square

Pour utiliser le critère précédent, il faut avoir à sa disposition un certain nombre de suites tendant vers 0 (des "suites de référence"). Nous allons pouvoir construire de telles suites en utilisant le fait que \mathbb{R} est archimédien .

Proposition 7.15 – Soit a un nombre réel positif.

- i) La suite $(a/n)_{n \geq 1}$ tend vers 0.
- ii) Si k est un entier positif, la suite $(a/n^k)_{n \geq 1}$ tend vers 0.
- iii) Si r est un nombre réel positif strictement plus petit que 1, la suite $(a r^n)_{n \in \mathbb{N}}$ tend vers 0.

Démonstration : (i) Donnons nous $\varepsilon > 0$. Comme \mathbb{R} est archimédien, il existe un entier naturel N tel que $N\varepsilon > a$. Donc pour tout entier $n \geq N$, on a $|a/n - 0| = a/n < \varepsilon$.

(ii) Si k est un entier positif et $n \geq 1$, on a $n^{k-1} \geq 1$ et donc $n^k = n \times n^{k-1} \geq n$. On a donc $|a/n^k - 0| = a/n^k \leq a/n$ pour $n \geq 1$, et donc d'après (i) et la proposition 7.14 la limite de (a/n^k) est 0.

(iii) Si $r < 1$, alors $1/r > 1$ et on a pour $n \geq 1$

$$\begin{aligned} \left(\frac{1}{r}\right)^n &= \left(1 + \left(\frac{1}{r} - 1\right)\right)^n \\ &= 1 + n\left(\frac{1}{r} - 1\right) + \mathbf{C}_n^2\left(\frac{1}{r} - 1\right)^2 + \cdots + \mathbf{C}_n^{n-1}\left(\frac{1}{r} - 1\right)^{n-1} + \left(\frac{1}{r} - 1\right)^n \\ &\geq n\left(\frac{1}{r} - 1\right) \text{ car tous les termes de la somme sont positifs.} \end{aligned}$$

Donc pour $n \geq 1$ on a $|ar^n - 0| = ar^n \leq a \frac{r}{n(1-r)}$. D'après (i) et la proposition 7.14 on en déduit que la limite de (ar^n) est 0. \square

2.1.3. Limites et inégalités

Définition 7.16 – Soit (a_n) une suite de nombres réels.

On dit que M est un *majorant* de la suite (a_n) si $a_n \leq M$ pour tout $n \in \mathbb{N}$.

On dit que m est un *minorant* de la suite (a_n) si $m \leq a_n$ pour tout $n \in \mathbb{N}$.

On dit que la suite (a_n) est *majorée* (resp. est *minorée*) si elle a un majorant (resp. un minorant). On dit qu'elle est *bornée* si elle a à la fois un majorant et un minorant.

Exercice - Montrer que la suite (a_n) est bornée si et seulement s'il existe un réel $A > 0$ tel que $|a_n| \leq A$ pour tout n .

Proposition 7.17 – Soit (a_n) une suite convergente de nombres réels. Alors il existe un réel $A > 0$ tel que $|a_n| \leq A$ pour tout $n \in \mathbb{N}$. Autrement dit, une suite convergente de nombres réels est bornée.

Démonstration : posons $\lim a_n = \ell$. Il existe un rang N tel que pour tout $n \geq N$, on a $|a_n - \ell| < 1$. On en déduit, pour tout $n \geq N$, $|a_n| < 1 + |\ell|$. Si l'on pose

$$A = \max(|a_0|, |a_1|, \dots, |a_{N-1}|, 1 + |\ell|),$$

on a bien $|a_n| \leq A$ pour tout n . \square

Proposition 7.18 – Soit (a_n) une suite convergente vers ℓ , et b un nombre réel. Si $\ell > b$ (respectivement $\ell < b$), alors il existe un entier naturel N tel que pour tout $n \geq N$, on a $a_n > b$ (resp. $a_n < b$).

On dit aussi que, même pour un ε petit, a_n sera plus grand que $\ell - \varepsilon$ à partir d'un certain rang.

Démonstration : soit $\ell = \lim a_n$, et $\varepsilon = \ell - b > 0$. Il existe un entier naturel N tel que pour tout $n \geq N$, on a $|a_n - \ell| < \varepsilon$, et donc $a_n > b$. \square

Théorème 7.19 – [Passage à la limite dans les inégalités] Soit (a_n) une suite convergente, et b un nombre réel. Si pour tout

entier naturel N il existe un entier $n \geq N$ tel que $a_n \leq b$ (respectivement $a_n \geq b$), alors $\lim a_n \leq b$ (resp. $\lim a_n \geq b$). En particulier si on a $a_n \leq b$ (resp. $a_n \geq b$) à partir d'un certain rang, alors $\lim a_n \leq b$ (resp. $\lim a_n \geq b$).

Démonstration : c'est la contraposée de la proposition 7.18. En formule, cette proposition s'écrit

$$(\lim a_n > b) \implies (\exists N \in \mathbb{N}, \forall n \geq N, a_n > b).$$

La contraposée, qui lui est équivalente, s'écrit

$$\text{non } (\exists N \in \mathbb{N}, \forall n \geq N, a_n > b) \implies \text{non } (\lim a_n > b).$$

Ceci équivaut à

$$(\forall N \in \mathbb{N}, \exists n \geq N, a_n \leq b) \implies (\lim a_n \leq b),$$

qui est bien la formulation du théorème. □

2.1.4. Opérations sur les suites

Théorème 7.20 – Soient (a_n) et (b_n) deux suites convergentes de nombres réels. Alors

- 1) La suite $(a_n + b_n)$ est convergente et $\lim(a_n + b_n) = \lim a_n + \lim b_n$.
- 2) Soit λ un nombre réel quelconque. La suite (λa_n) est convergente et $\lim(\lambda a_n) = \lambda \lim a_n$.
- 3) La suite $(a_n b_n)$ est convergente et $\lim(a_n b_n) = \lim a_n \times \lim b_n$.

Démonstration : on pose $\ell = \lim a_n$ et $m = \lim b_n$.

Pour 1, on veut rendre $|(a_n + b_n) - (\ell + m)|$ plus petit qu'un nombre réel $\varepsilon > 0$ donné. Or on a $|(a_n + b_n) - (\ell + m)| \leq |a_n - \ell| + |b_n - m|$. On sait que $|a_n - \ell| < \varepsilon/2$ à partir d'un certain rang et que $|b_n - m| < \varepsilon/2$ à partir d'un certain rang. Donc $|(a_n + b_n) - (\ell + m)| < \varepsilon$ à partir d'un certain rang. Ceci montre que $\lim(a_n + b_n) = \ell + m$.

Le 2 est facile (le traiter en exercice).

Voyons maintenant 3. On suppose d'abord que $\ell = 0$. On veut montrer que $\lim(a_n b_n) = 0 \times m = 0$. Puisque la suite (b_n) est convergente, elle est bornée (Proposition 7.17) et il existe un nombre réel $B > 0$ tel que, pour tout n , on a $|b_n| \leq B$. On obtient $|a_n b_n| \leq B|a_n|$. Puisque $\lim a_n = 0$ on a $\lim |a_n| = 0$ et, d'après 2, $\lim(B|a_n|) = 0$. Par la proposition 7.14 on en déduit $\lim(a_n b_n) = 0$.

Il nous reste à voir ce qui se passe dans le cas général. On a alors $a_n b_n = \ell b_n + (a_n - \ell)b_n$. Comme $\lim(a_n - \ell) = 0$, on sait d'après le cas particulier que

l'on vient de traiter que $\lim((a_n - \ell)b_n) = 0$. D'après 2 on a $\lim(\ell b_n) = \ell m$. En appliquant 1, il vient $\lim(a_n b_n) = \ell m + 0 = \ell m$. \square

Proposition 7.21 – Soit (u_n) , (a_n) et (b_n) trois suites de nombres réels. Si $\lim a_n = \lim b_n = \ell$ et si on a $a_n \leq u_n \leq b_n$ à partir d'un certain rang (u_n est encadré par les deux gendarmes a_n et b_n), alors $\lim u_n = \ell$.

Exercice - Démontrer la "propriété des gendarmes" énoncée ci-dessus. On utilisera l'inégalité $|u_n - a_n| \leq (b_n - a_n)$ valide à partir d'un certain rang, le théorème 7.20 et la proposition 7.14.

Proposition 7.22 – [Limite d'un quotient] Soit (a_n) une suite convergente de nombres réels, et supposons que $\ell = \lim a_n$ est non nul. Alors à partir d'un certain rang on a $a_n \neq 0$, et $\lim(1/a_n) = 1/\ell$.

Démonstration : on sait que $\lim |a_n| = |\ell| > 0$. D'après la proposition 7.18, on a $|a_n| > |\ell|/2$ à partir d'un certain rang, et a fortiori $a_n \neq 0$. Etant donné $\varepsilon > 0$, on veut rendre $|1/a_n - 1/\ell|$ plus petit que ε . On a

$$\left| \frac{1}{a_n} - \frac{1}{\ell} \right| = \left| \frac{\ell - a_n}{a_n \ell} \right| = \frac{|a_n - \ell|}{|a_n| |\ell|}.$$

On sait déjà que $|a_n| > |\ell|/2$ à partir d'un certain rang. On sait aussi que $|a_n - \ell| < \varepsilon \ell^2/2$ à partir d'un certain rang. Donc

$$\left| \frac{1}{a_n} - \frac{1}{\ell} \right| < \frac{\varepsilon \ell^2/2}{(|\ell|/2)|\ell|} = \varepsilon$$

à partir d'un certain rang. C'est ce que l'on voulait. \square

En combinant le 3 du théorème 7.20 et la proposition 7.22, on obtient que si $\lim u_n = \ell$ et $\lim v_n = m \neq 0$, alors $\lim(u_n/v_n) = \ell/m$.

2.2. Suites croissantes

Une suite (a_n) est croissante si et seulement si

$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, \quad (n \leq m \implies u_n \leq u_m).$$

Une suite (a_n) est majorée si et seulement si

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

Théorème 7.23 – Toute suite de nombres réels croissante et majorée est convergente.

Démonstration : soit (a_n) une suite de nombres réels croissante et majorée. Posons $A = \{a_n; n \in \mathbb{N}\}$. Comme la suite (a_n) est majorée, le sous-ensemble (non vide) A est aussi majoré et admet donc une borne supérieure que nous noterons ℓ . Montrons que $\ell = \lim a_n$.

Soit $\varepsilon > 0$; il existe un entier naturel n tel que $\ell - \varepsilon < a_n < \ell$. Comme a_n est croissante pour tout entier m tel que $m \geq n$ on a $a_n \leq a_m$ et par définition de ℓ on a $a_m \leq \ell$. On a donc $\ell - \varepsilon < a_n \leq a_m \leq \ell < \ell + \varepsilon$. On a bien montré que :

$$\forall \varepsilon > 0, \exists n \in \mathbb{N}, \forall m \in \mathbb{N}, \quad (m \geq n \implies |a_m - \ell| < \varepsilon). \quad \square$$

Corollaire 7.24 – Si (a_n) est une suite de nombres réels croissante et majorée, alors

$$\lim a_n = \sup\{a_n; n \in \mathbb{N}\} = \sup_{n \in \mathbb{N}} a_n$$

Corollaire 7.25 – Si (a_n) est une suite de nombres réels décroissante et minorée, alors (a_n) converge et

$$\lim a_n = \inf\{a_n; n \in \mathbb{N}\} = \inf_{n \in \mathbb{N}} a_n$$

Exercice - Démontrer les corollaires.

Remarque - Ce théorème est faux si l'on remplace réel par rationnel. (Donner un contre-exemple)

Exercice - (difficile) Soit (u_n) une suite de nombres réels. On définit les suites (v_n) et (w_n) par

$$\begin{aligned} v_n &= \sup\{u_m; m \geq n\} \\ w_n &= \inf\{u_m; m \geq n\} \end{aligned}$$

- 1°) Montrer que (v_n) est décroissante et que (w_n) est croissante.
 2°) Montrer que (v_n) et (w_n) sont convergentes et que $\lim v_n \geq \lim w_n$.

On appelle **limite supérieure** de (u_n) et on note $\limsup u_n$ la limite de (v_n) , de même on appelle **limite inférieure** et on note $\liminf u_n$ la limite de (w_n) .

- 3°) Montrer que si $\limsup u_n = \liminf u_n$, alors (u_n) converge et $\lim u_n = \limsup u_n = \liminf u_n$.

2.3. Suites adjacentes

Définition 7.26 – Deux suites (a_n) et (b_n) de nombres réels sont dites *adjacentes* si elles vérifient les propriétés suivantes :

- 1) $\forall n \in \mathbb{N}, a_n \leq b_n,$
- 2) $\forall n \in \mathbb{N}, a_n \leq a_{n+1}$ (la suite (a_n) est croissante),
- 3) $\forall n \in \mathbb{N}, b_n \geq b_{n+1}$ (la suite (b_n) est décroissante),
- 4) $\lim_{n \rightarrow \infty} (b_n - a_n) = 0.$

Exemple - Les suites de décimaux à 10^{-n} près par défaut et par excès d'un nombre réel x , $a_n = E(10^n x)$ et $b_n = E(1 + 10^n x)$, sont des suites adjacentes et convergent vers x .

Remarque - Le premier item est en fait une conséquence des trois autres : posons $c_n = a_n - b_n$. La suite (c_n) converge vers 0 d'après l'item 3 ; elle est croissante car $a_{n+1} - b_{n+1} \geq a_n - b_n$ car (a_n) croît et (b_n) décroît. On en déduit qu'elle est négative donc, pour tout entier n , $a_n \leq b_n$.

Proposition 7.27 – Soient (a_n) et (b_n) deux suites adjacentes de nombres réels. Alors il existe un unique nombre réel c tel que $a_n \leq c \leq b_n$ pour tout $n \in \mathbb{N}$, et $\lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} b_n = c$.

Démonstration : comme (b_n) est décroissante et $(a_n) \leq b_n$, on a pour tout n , $a_n \leq b_0$. La suite (a_n) est croissante et majorée et donc convergente. Puisque $\lim b_n - a_n = 0$, on a $\lim b_n = \lim(b_n - a_n) + \lim a_n = \lim a_n$. \square
Donnons un premier exemple de nombre réel défini par deux suites adjacentes. Nous allons démontrer le résultat suivant.

Proposition 7.28 – Tout nombre réel positif ou nul a une racine carrée dans \mathbb{R} .

Rappelons notre règle du jeu, qui est de ne rien accepter sur les réels que ce qui découle logiquement des axiomes que l'on a posés. On n'a rien dit dans ces axiomes de l'existence de racines carrées, donc il faut bien montrer à partir des axiomes que la racine carrée d'un réel positif ou nul existe !

Démonstration : soit r un nombre réel, $0 \leq r$. On va définir par récurrence une suite de segments emboîtés $[a_n, b_n]$, par un procédé que nous reverrons plusieurs fois : la *dichotomie* ("action de couper en deux"). On veut que pour tout entier n , l'inégalité suivante soit vérifiée :

$$(a_n)^2 \leq r < (b_n)^2 .$$

Pour le choix du premier segment, on procède de la manière suivante : on définit b_0 comme étant le plus petit entier naturel qui vérifie $r < (b_0)^2$. D'après l'axiome d'archimédianité il y a des entiers naturels p plus grands que r , et un tel p vérifie $p^2 \geq p > r$. Puisqu'il y a des entiers dont le carré est strictement plus grand que r , on peut bien prendre le plus petit de ces entiers. On pose $a_0 = b_0 - 1$. Comme $b_0 \geq 1$, on a $a_0 \geq 0$. Par définition de b_0 , on a $(a_0)^2 \leq r < (b_0)^2$.

Supposons maintenant que l'on a déjà construit le segment $[a_n, b_n]$ vérifiant l'inégalité $(a_n)^2 \leq r < (b_n)^2$. Alors

- a) Si $\left(\frac{a_n + b_n}{2}\right)^2 \leq r$, on pose $a_{n+1} = \frac{a_n + b_n}{2}$ et $b_{n+1} = b_n$ (on garde la moitié droite du segment).
- b) Sinon, on pose $a_{n+1} = a_n$ et $b_{n+1} = \frac{a_n + b_n}{2}$ (on garde la moitié gauche).

Le choix de la moitié du segment que l'on garde s'est fait de telle manière que l'on ait bien $(a_{n+1})^2 \leq r < (b_{n+1})^2$. La dichotomie consiste à couper le segment en deux à chaque étape. Comme la longueur du segment $[a_0, b_0]$ est 1, celle du segment $[a_n, b_n]$ vaut $1/2^n$. Cette longueur tend vers 0 quand n tend vers l'infini, on l'a vu dans la proposition 7.15 (iii). Donc, d'après la proposition 7.27, il existe un et un seul réel ℓ qui vérifie $a_n \leq \ell \leq b_n$ pour tout $n \in \mathbb{N}$. On a $0 \leq a_0 \leq \ell$. Pour voir que ℓ est la racine carrée de r , il reste à vérifier que $\ell^2 = r$.

Comme $\lim a_n = \lim b_n = \ell$, on a, d'après le 3 du théorème 7.20, $\lim(a_n)^2 = \lim(b_n)^2 = \ell^2$. Des inégalités $(a_n)^2 \leq r < (b_n)^2$ on déduit par passage à la limite (Théorème 7.19) que

$$\ell^2 = \lim(a_n)^2 \leq r \leq \lim(b_n)^2 = \ell^2,$$

et donc $\ell^2 = r$. □

2.4. Limites infinies

Il est commode d'étendre la définition de limite pour englober des limites infinies.

Définition 7.29 – On dit qu'une suite de nombres réels (a_n) a pour limite $+\infty$ (respectivement $-\infty$) si, pour tout nombre réel A , il existe un entier naturel N tel que, pour tout $n \geq N$, on a $A < a_n$ (resp. $a_n < A$) :

$$\forall A \in \mathbb{R} \exists N \in \mathbb{N} \forall n \geq N \quad A < a_n.$$

Autrement dit, (a_n) tend vers $+\infty$ si et seulement si pour tout $A \in \mathbb{R}$, on a $a_n > A$ à partir d'un certain rang.

Attention : une suite (a_n) qui tend vers $+\infty$ ou vers $-\infty$ n'est pas appelée suite convergente.

Exercice - 1°) Montrer que l'on peut aussi exprimer $\lim_{n \rightarrow \infty} a_n = +\infty$ par

$$\forall A \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, \quad A \leq a_n.$$

2°)) Montrer que si $\lim a_n = +\infty$ et $b_n \geq a_n$ à partir d'un certain rang, alors $\lim b_n = +\infty$.

Proposition 7.30 – Les résultats concernant les limites de sommes et de produits de suites de nombres réels (théorème 7.20) s’étendent aux limites infinies, dans les cas correspondant aux égalités suivantes :

$$\begin{aligned} \ell + (+\infty) &= +\infty & \ell + (-\infty) &= -\infty \\ (+\infty) + (+\infty) &= +\infty & (-\infty) + (-\infty) &= -\infty \\ \ell \times (+\infty) &= \begin{cases} +\infty & \text{si } \ell > 0 \\ -\infty & \text{si } \ell < 0 \end{cases} & \ell \times (-\infty) &= \begin{cases} -\infty & \text{si } \ell > 0 \\ +\infty & \text{si } \ell < 0 \end{cases} \\ (+\infty) \times (-\infty) &= -\infty & (+\infty) \times (+\infty) &= (-\infty) \times (-\infty) = +\infty \end{aligned}$$

Les cas “indéterminés” sont $(+\infty) + (-\infty)$, $0 \times (+\infty)$ et $0 \times (-\infty)$.

Démonstration : on se limitera à un cas : si $\lim a_n = \ell > 0$ et $\lim b_n = +\infty$, alors $\lim a_n b_n = +\infty$. On se donne un réel A et on veut rendre $a_n b_n$ strictement plus grand que A . On peut supposer $A > 0$. Puisque $\lim a_n > \ell/2$, on a $a_n > \ell/2$ à partir d’un certain rang. Par ailleurs, on a $b_n > 2A/\ell$ à partir d’un certain rang. Donc $a_n b_n > A$ à partir d’un certain rang. On a bien montré $\lim a_n b_n = +\infty$. \square

Exercice - Essayez de voir comment procéder dans un ou deux autres cas.

Proposition 7.31 – Si (a_n) est une suite de nombres réels telle que $\lim |a_n| = +\infty$, alors $a_n \neq 0$ à partir d’un certain rang et $\lim 1/a_n = 0$. Si (a_n) est une suite de nombres réels strictement positifs à partir d’un certain rang telle que $\lim a_n = 0$, alors $\lim 1/a_n = +\infty$

Exercice - Faire la démonstration.

2.5. Suites extraites

Une suite extraite de la suite (u_n) est une suite obtenue en enlevant certains des termes de (u_n) , sans changer l’ordre. Pour pouvoir raisonner sur cette notion de suite extraite, il nous faut une définition plus en forme.

Définition 7.32 – Soit (u_n) une suite de nombres réels. On dit que la suite (v_n) est extraite de la suite (u_n) s’il existe une application strictement croissante φ de \mathbb{N} dans \mathbb{N} ($m < n$ entraîne $\varphi(m) < \varphi(n)$) telle que $v_n = u_{\varphi(n)}$ pour tout $n \in \mathbb{N}$.

- Exemples** - • La suite des termes de rang pair $v_n = u_{2n}$ et celle des termes de rang impair $w_n = u_{2n+1}$ sont extraites de la suite (u_n) ; la suite $v_n = 1/(4n^4)$ est extraite de la suite $u_n = 1/n^2$, au moyen de l'application $\varphi(n) = 2n^2$.
- La suite $t_n = \frac{\cos(1)}{4n+1}$ est extraite de la suite $u_n = \frac{1}{n} \sin(1+n\frac{\pi}{2})$. En effet, $t_n = u_{4n+1}$.

Lemme 7.33 – Soit φ une application strictement croissante de \mathbb{N} dans \mathbb{N} . Alors, pour tout entier naturel n , on a $n \leq \varphi(n)$.

Exercice - Démontrer le lemme en utilisant un raisonnement par récurrence.

Proposition 7.34 – Soit (u_n) une suite convergente de nombres réels, et soit (v_n) une suite extraite de (u_n) . Alors la suite (v_n) est convergente et $\lim v_n = \lim u_n$.

Démonstration : donnons nous $\varepsilon > 0$. On a un entier N tel que pour tout $n \geq N$, $|u_n - \ell| < \varepsilon$. On suppose que $v_n = u_{\varphi(n)}$ où φ est strictement croissante. On a toujours $\varphi(n) \geq n$ d'après le lemme 7.33. Donc, si $n \geq N$, alors $\varphi(n) \geq N$, d'où $|v_n - \ell| = |u_{\varphi(n)} - \ell| < \varepsilon$. Ceci montre que $\lim v_n = \ell$. \square

2.6. Développement décimal

Nous allons voir maintenant un exemple important, d'encadrement d'un nombre réel par des suites adjacentes de nombres rationnels : le *développement décimal*.

Soit ℓ un réel positif ou nul. On note $E(\ell)$ sa partie entière, c'est à dire l'entier naturel tel que $E(\ell) \leq \ell < E(\ell) + 1$. L'existence de cette partie entière est assurée par le fait que \mathbb{R} est archimédien : cet axiome entraîne qu'il y a des entiers naturels strictement plus grands que ℓ , donc on peut prendre le plus petit entier p tel que $p > \ell$ et on pose $E(\ell) = p - 1$.

Soit $x \in \mathbb{R}_+^*$; on pose, pour tout $n \in \mathbb{N}$, $x_n = 10^{-n}E(10^n x)$. On a alors $0 \leq x - x_n < 10^{-n}$ car $10^n x_n = E(10^n x) \leq 10^n x < E(10^n x) + 1$ par définition de la partie entière.

Définition 7.35 – On dit que x_n est l'approximation décimale par défaut de x à 10^{-n} près.

Proposition 7.36 – $x = \lim x_n$

Posons $a_n = E(10^n x) - 10 E(10^{n-1} x) = 10^n(x_n - x_{n-1})$.

Lemme 7.37 – a_n est un entier compris entre 0 et 9.

Démonstration : a_n est, par définition de la partie entière, un entier.

On a $E(10^{n-1}x) \leq 10^{n-1}x < E(10^{n-1}x) + 1$, d'où $10E(10^{n-1}x) \leq 10^n x < 10E(10^{n-1}x) + 10$ et, par définition de $E(10^n x)$, on obtient

$$10E(10^{n-1}x) \leq E(10^n x) < E(10^n x) + 1 \leq 10E(10^{n-1}x) + 10.$$

On en déduit que

$$0 \leq E(10^n x) - 10 E(10^{n-1}x) < 10.$$

□

On a de plus

$$\begin{array}{ll} a_n = 10^n(x_n - x_{n-1}) & 10^{-n}a_n = x_n - x_{n-1} \\ a_{n-1} = 10^{n-1}(x_{n-1} - x_{n-2}) & 10^{-(n-1)}a_{n-1} = x_{n-1} - x_{n-2} \\ \dots & \dots \\ a_1 = 10(x_1 - x_0) & 10^{-1}a_1 = x_1 - x_0 \end{array}$$

En additionnant, on obtient $x_n = x_0 + \sum_{i=1}^n \frac{a_i}{10^i}$ où $x_0 = E(x)$.

On note $x = x_0 + \sum_{i=1}^{\infty} a_i 10^{-i} = x_0, a_1 a_2 \dots a_n \dots$ et on appelle cette écriture

le développement décimal propre illimité de x .

On admet la réciproque, c'est-à-dire qu'un développement décimal illimité représente un réel et que deux développements décimaux illimités peuvent représenter le même réel. Ce résultat est démontré en deuxième année de DEUG au moment de l'étude des séries.

Exemple - $1 = 0,99999\dots$ et $0,356 = 0,355999999\dots$

Pour $x < 0$, on utilise le développement décimal propre illimité de $-x = x_0, a_1 a_2 \dots$ puis $x = -x_0, a_1 a_2 \dots$. Dans ce cas, $E(x) = -x_0 - 1$.

Théorème 7.38 – Un rationnel admet un développement décimal illimité qui est périodique à partir d'un certain rang.

La preuve se fait au moyen de la division euclidienne.

On admet la réciproque, c'est-à-dire que

Tout réel admettant un développement décimal illimité périodique à partir d'un certain rang est un rationnel.

Exemple -

$$\begin{aligned} x &= 3,46 \underbrace{53}_{53} \dots = 3 + \frac{46}{100} + \frac{53}{900} = \frac{3167}{900} \\ x &= 1, \underbrace{714285}_{714285} \dots = \frac{12}{7} \end{aligned}$$

Remarque - Le développement décimal d'un réel est unique si l'on suppose de plus que $\{a_n ; a_n < 9\}$ est infini (ce qui revient à écarter le cas d'une suite qui devient constante égale à 9).

3. Pour approfondir le sujet

3.1. Critère de Cauchy, théorème de Bolzano-Weierstrass

3.1.1. Critère de Cauchy

Définition 7.39 – Une suite (u_n) de nombres réels est dite *suite de Cauchy* quand elle vérifie la propriété suivante : pour tout nombre réel $\varepsilon > 0$, il existe un entier naturel N , tel que pour tous $p \geq N$ et $q \geq N$, on a $|u_q - u_p| < \varepsilon$.

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

Autrement dit, pour toute “tolérance” ε , on peut trouver un rang N à partir duquel l'écart entre deux termes quelconques de la suite est plus petit que ε . Il faut bien voir qu'on ne se contente pas de l'écart de deux termes successifs ! Par exemple posons, pour $n \geq 1$, $u_n = 1 + (1/2) + \dots + (1/n)$. On a $|u_n - u_{n+1}| = 1/(n+1)$; donc, quel que soit $\varepsilon > 0$, on peut trouver N tel que pour tout $n \geq N$ on a $|u_n - u_{n+1}| < \varepsilon$. Cependant, notre suite (u_n) n'est pas une suite de Cauchy. En effet si c'était une suite de Cauchy, en prenant $\varepsilon = 1/2$, on devrait trouver N tel que quels que soient $n \geq N$ et $p \geq N$, on ait $|u_n - u_p| < 1/2$. En particulier, on devrait avoir $|u_N - u_{2N}| < 1/2$. Or

$$|u_N - u_{2N}| = \frac{1}{N+1} + \frac{1}{N+2} + \dots + \frac{1}{2N} > N \times \frac{1}{2N} = \frac{1}{2}.$$

Théorème 7.40 – [Critère de Cauchy] Une suite de nombres réels est convergente si et seulement si c'est une suite de Cauchy.

Démonstration : soit (u_n) une suite convergente, et $\ell = \lim u_n$. Donnons nous $\varepsilon > 0$. On veut rendre $|u_n - u_p|$ plus petit que ε , or on sait que $|u_n - u_p| \leq |\ell - u_n| + |\ell - u_p|$. Il existe un entier N tel que pour tout $n \geq N$ on a $|\ell - u_n| < \varepsilon/2$. Donc, si l'on prend $n \geq N$ et $p \geq N$, on a $|u_n - u_p| < \varepsilon/2 + \varepsilon/2 = \varepsilon$. La suite (u_n) est donc de Cauchy.

Réciproquement, supposons que la suite (u_n) est de Cauchy. On commence par montrer qu'elle est bornée. Il existe N_1 tel que pour tout $n \geq N_1$ et tout $p \geq N_1$, on a $|u_n - u_p| < 1$. En particulier (avec $p = N_1$), on obtient que pour tout $n \geq N_1$ on a $|u_n| \leq |u_{N_1}| + 1$. Si on pose $A = \max(|u_0|, |u_1|, \dots, |u_{N_1-1}|, |u_{N_1}| + 1)$, alors $|u_n| \leq A$ quel que soit n .

On va construire deux suites adjacentes. Pour tout choix de $n \in \mathbb{N}$, l'ensemble non vide $A_n = \{u_k; k \geq n\}$ est majoré par A et minoré par $-A$. Soit $a_n = \inf\{u_k; k \geq n\}$ et $b_n = \sup\{u_k; k \geq n\}$.

Comme $A_{n+1} \subset A_n$ alors $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ par suite pour tout $n \in \mathbb{N}$, $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$.

Il reste à montrer que $\lim(b_n - a_n) = 0$.

Donnons nous $\varepsilon > 0$.

Comme $a_n = \inf\{u_k; k \geq n\}$, il existe un entier $p \geq n$ tel que $a_n \leq u_p < a_n + \frac{\varepsilon}{3}$. De même $b_n = \sup\{u_k; k \geq n\}$, il existe un entier $q \geq n$ tel que $b_n - \frac{\varepsilon}{3} < u_q \leq b_n$.

D'autre part, comme u_n est une suite de Cauchy, il existe un entier N tel que pour tout $p \geq N$ et tout $q \geq N$ on a $|u_p - u_q| < \frac{\varepsilon}{3}$.

A l'aide de l'inégalité triangulaire, $|b_n - a_n| = |(b_n - u_q) + (u_q - u_p) + (u_p - a_n)| \leq |b_n - u_q| + |u_q - u_p| + |u_p - a_n| \leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$ dès que $n \geq N$.

On a montré que les suites (a_n) et (b_n) sont adjacentes donc convergent vers une même limite.

Par ailleurs, pour tout $n \in \mathbb{N}$, $a_n \leq u_n \leq b_n$, d'où u_n est convergente. \square

L'intérêt du critère de Cauchy est surtout théorique. Il réside dans le fait que ce critère permet de caractériser les suites convergentes sans faire intervenir leurs limites.

3.1.2. Théorème de Bolzano-Weierstrass

Théorème 7.41 – [Bolzano-Weierstrass] Soit (u_n) une suite bornée de nombres réels. Alors on peut extraire de la suite (u_n) une suite (v_n) qui converge.

Démonstration : par hypothèse il existe un réel $M > 0$ tel que, pour tout n , on a $|u_n| \leq M$. On construit alors par dichotomie une suite de segments emboîtés $[a_n, b_n]$ tels que, pour tout n , il y a une infinité d'entiers p pour lesquels u_p est dans $[a_n, b_n]$. En même temps, on construit une fonction strictement croissante $\varphi : \mathbb{N} \mapsto \mathbb{N}$ telle que $u_{\varphi(n)} \in [a_n, b_n]$

On pose $a_0 = -M$ et $b_0 = M$. Tous les u_p sont dans $[a_0, b_0]$, il y a donc bien une infinité de p pour lesquels c'est vrai. On pose $\varphi(0) = 0$, on a bien $u_{\varphi(0)} \in [a_0, b_0]$.

Supposons que l'on a déjà construit $[a_n, b_n]$, qu'il y a une infinité de p pour lesquels u_p est dans $[a_n, b_n]$, et que l'on a défini $\varphi(n)$ tel que $u_{\varphi(n)} \in [a_n, b_n]$. Si le segment $[a_n, (a_n + b_n)/2]$ est tel qu'il y a une infinité de p pour lesquels u_p est dans $[a_n, b_n]$, alors on pose $a_{n+1} = a_n$ et $b_{n+1} = (a_n + b_n)/2$. Sinon, il doit y avoir une infinité de p pour lesquels u_p est dans le segment $[(a_n + b_n)/2, b_n]$, et alors on pose $a_{n+1} = (a_n + b_n)/2$ et $b_{n+1} = b_n$. Dans les deux cas, comme il y a une infinité de p tels que $u_p \in [a_{n+1}, b_{n+1}]$, il y en a des plus grands que $\varphi(n)$ et donc on peut choisir $\varphi(n+1) > \varphi(n)$ tel que $u_{\varphi(n+1)} \in [a_{n+1}, b_{n+1}]$. On construit ainsi par récurrence une suite de segments emboîtés et une fonction φ avec la propriété annoncée. La longueur du segment $[a_n, b_n]$ est $2M/2^n$; elle tend vers 0 quand n tend vers l'infini. Il y a donc un unique réel c qui appartient à tous les segments $[a_n, b_n]$. Ce nombre c est la limite commune des suites adjacentes (a_n) et (b_n) .

On extrait maintenant une suite (v_n) de la suite (u_n) en posant $v_n = u_{\varphi(n)}$, et ainsi on a $a_n \leq v_n \leq b_n$ pour tout n . La suite (v_n) est encadrée entre les deux "gendarmes" (a_n) et (b_n) qui tendent vers c , et donc d'après 7.27 $\lim_{n \rightarrow \infty} v_n = c$. \square

3.2. Combien y a-t-il de nombres réels ? (pour votre culture générale)

La question peut sembler farfelue. On va la préciser. Si A et B sont des ensembles finis, le nombre d'éléments de A est supérieur ou égal au nombre d'éléments de B si et seulement s'il existe une surjection de A sur B (une application de A dans B pour laquelle chaque élément de B est atteint). Une image : le nombre de lapins est supérieur ou égal au nombre de cages si et seulement s'il existe une manière de mettre les lapins en cage de telle sorte que chaque cage soit occupée. Pour des ensembles infinis, on ne parle plus de nombre d'éléments mais de *cardinal*, et on dit que le cardinal d'un ensemble A est supérieur ou égal au cardinal de B quand il existe une surjection de A sur B .

Définition 7.42 – Un ensemble *dénombrable* est un ensemble infini A pour lequel il existe une surjection de \mathbb{N} sur A . Autrement dit, on peut énumérer A , c'est à dire faire une liste de ses éléments, éventuellement avec répétition. L'ensemble \mathbb{Q} des nombres rationnels est dénombrable. Voici un début d'énumération :

$$0, \frac{1}{1}, \frac{-1}{1}, \frac{1}{2}, \frac{-1}{2}, \frac{2}{1}, \frac{-2}{3}, \frac{1}{3}, \frac{-1}{2}, \frac{2}{2}, \frac{-2}{1}, \frac{3}{1}, \frac{-3}{1}, \frac{4}{1}, \frac{-4}{2}, \frac{3}{2}, \frac{-3}{2}, \dots$$

Exercice - Pouvez-vous continuer, et décrire comment est fabriquée cette énumération ?

Tout nombre rationnel figure dans la liste ; il y a des répétitions. L'ordre dans la liste n'a rien à voir avec l'ordre sur \mathbb{Q} .

Par contre :

Proposition 7.43 – \mathbb{R} n'est pas dénombrable.

Démonstration : si on avait une énumération de \mathbb{R} , on aurait une énumération de l'intervalle $[0, 1[$, en jetant de la liste tous les autres réels. Cette énumération serait une liste de réels $(\alpha_1, \alpha_2, \dots)$ dont on écrit les développements décimaux (avec l'hypothèse que la suite $(i_{p,n})_n$ ne devienne pas constante égale à 9 pour avoir l'unicité du développement) :

$$\alpha_1 = 0, i_{1,1}i_{1,2}i_{1,3} \dots$$

$$\alpha_2 = 0, i_{2,1}i_{2,2}i_{2,3} \dots$$

$$\alpha_3 = 0, i_{3,1}i_{3,2}i_{3,3} \dots$$

$$\vdots$$

Tout réel de $[0, 1[$ devrait figurer dans cette liste. Or, voici comment en fabriquer un qui n'y figure pas : pour tout $n \geq 1$, on pose $j_n = 0$ si $i_{n,n} \neq 0$ et $j_n = 1$ si $i_{n,n} = 0$. On construit bien ainsi le développement décimal du réel

$\ell = 0, j_1 j_2 j_3 \dots$, ce développement ne se termine pas par des termes égaux à 9 par construction et ce réel ℓ ne figure pas dans la liste. En effet si on avait $\ell = \alpha_n$, alors les développements décimaux devraient coïncider et on aurait $j_n = i_{n,n}$, ce qui est faux. \square

L'argument que l'on vient d'employer s'appelle argument diagonal de Cantor. Georg Cantor (1845–1918) a été élève de Weierstrass à Berlin. A la suite de recherches fines d'analyse, il a été amené à étudier et à comparer des ensembles infinis. Il introduisit à cet effet de nouveaux concepts qui constituaient une véritable "arithmétique de l'infini".

3.3. A propos de la construction des nombres réels (pour votre culture générale)

Le problème est le suivant : on veut dire ce qu'est l'ensemble des nombres réels, en supposant connu l'ensemble des nombres rationnels. Autrement dit, on veut "construire" les nombres réels à partir des nombres rationnels, comme on sait construire les nombres rationnels à partir des nombres entiers, ou les nombres complexes à partir des nombres réels. L'idée de la construction est donnée par des propriétés que nous avons établies à partir des axiomes : tout nombre réel est limite d'une suite de nombres rationnels, et une suite a une limite dans \mathbb{R} si et seulement si elle vérifie le critère de Cauchy. Un nombre réel sera représenté par une suite de Cauchy de nombres rationnels, et deux suites de Cauchy de nombres rationnels représenteront le même réel si et seulement si leur différence tend vers 0.

Considérons l'ensemble \mathcal{S} des suites de Cauchy de nombres rationnels, c'est à dire l'ensemble des suites (a_n) telles que tous les a_n sont des nombres rationnels, et que pour tout rationnel $\varepsilon > 0$, il existe un entier naturel N tel que pour tous $n \geq N$ et $p \geq N$ on a $|a_n - a_p| < \varepsilon$. Sur cet ensemble \mathcal{S} , on définit une relation d'équivalence \mathcal{R} en disant que les suites (a_n) et (b_n) vérifient la relation \mathcal{R} quand pour tout rationnel $\varepsilon > 0$, il existe un entier naturel N tel que pour tout $n \geq N$ on a $|a_n - b_n| < \varepsilon$. Alors on définit \mathbb{R} comme l'ensemble des classes d'équivalence d'éléments de \mathcal{S} pour la relation d'équivalence \mathcal{R} . Cette définition est bien faite entièrement à partir des nombres rationnels.

Il reste bien sûr à définir les opérations et l'ordre sur \mathbb{R} , puis à vérifier les propriétés que l'on avait posées comme axiomes au début de ce chapitre. Par exemple, la somme du réel représenté par la suite (a_n) de \mathcal{S} et du réel représenté par la suite (b_n) de \mathcal{S} sera bien sûr le réel représenté par la suite $(a_n + b_n)$. On voit qu'il y a des vérifications à faire : que la suite $(a_n + b_n)$ est bien de Cauchy, et que si on remplace (a_n) et (b_n) par des suites (a'_n) et (b'_n) équivalentes dans \mathcal{S} , alors $(a'_n + b'_n)$ est équivalente à $(a_n + b_n)$. Ces vérifications des propriétés des opérations et de l'ordre ne sont pas très compliquées, mais fastidieuses.

Bernard Bolzano (1781–1848), Augustin Louis Cauchy (1789–1857), Karl Weierstrass (1815–1897) : trois mathématiciens qui ont contribué de façon essentielle, au cours du 19ème siècle, à la construction de la théorie des nombres réels qui fonde l'analyse moderne.

A PROPOS DE LA CONSTRUCTION DES NOMBRES RÉELS

Cauchy et Weierstrass ont eu une influence importante par leur enseignement, le premier à l'Ecole Polytechnique et le deuxième à l'Université de Berlin.

TABLE DES MATIERES

I - Ensembles et sous-ensembles _____	1
1. Notion d'ensemble - Elément d'un ensemble	1
2. Relation d'inclusion	1
3. Intersection et réunion	2
4. Complémentaire d'un ensemble	4
5. Partitions	5
6. Produit	6
II - Eléments pour comprendre un énoncé _____	11
1. Propositions	11
1.1. Négation	12
1.2. Conjonction et disjonction	12
1.3. Implication	13
1.4. Equivalence	14
2. Propositions avec des quantificateurs	15
3. Négation d'une proposition	17
4. Quelques conseils pratiques	18
III - Eléments pour comprendre	
et écrire des démonstrations _____	23
1. Pour comprendre la structure d'une démonstration	23
1.1. Règle de l'hypothèse auxiliaire	24
1.2. Règle du quel que soit	24
1.3. Règle des cas	25
1.4. Nommer un objet	26
1.5. Raisonnement par l'absurde	26
1.6. Raisonnement par contraposition	27
1.7. Pour démontrer une équivalence	27
1.8. Pour démontrer (Q ou R)	29
1.9. Raisonnement par récurrence	29
1.10. D'autres règles	32
2. Pour trouver une démonstration	32
2.1. On peut décider d'aborder le problème directement.	32
2.2. On peut utiliser des moyens indirects.	33
2.3. On peut essayer de se ramener à une proposition plus simple.	34
3. Quelques types de problèmes à résoudre	35
3.1. Résultats sur les ensembles	35
3.2. Enoncés d'analyse	35
3.3. Résolution d'équations.	36
3.4. Contre-exemples	37
4. Quelques conseils pour résoudre un problème	
et écrire une démonstration.	37

4.1. Pour bien lire le texte	37
4.2. Pour chercher une solution.	37
4.3. Pour rédiger une démonstration.	38
IV - Applications _____	45
1. Définitions et exemples	45
2. Egalité - Restriction - Prolongement	46
3. Composition des applications	47
4. Familles	48
5. Bijection - Injection - Surjection	48
6. Etude des bijections	51
7. Image directe ou réciproque	53
8. Compléments	55
V - Lois de composition internes - Relations _____	61
1. Lois de composition internes	61
1.1. Définition et exemples	61
1.2. Propriétés usuelles des lois internes	61
1.3. Exemples de structures algébriques (culture générale)	63
2. Relations	64
2.1. Définitions et exemples	64
2.2. Propriétés usuelles des relations	64
2.3. Etude des relations d'équivalence	65
2.4. Relations d'ordre	67
VI - Arithmétique _____	69
1. Divisibilité	69
1.1. Entiers naturels	69
1.2. Entiers relatifs	69
1.3. La division euclidienne, relation de divisibilité	70
2. Congruences	72
2.1. Relation de congruence. Classes de congruence	72
2.2. Opérations sur les congruences	74
3. Ensembles finis ou dénombrables (pour votre culture générale)	75
VII - Nombres réels et suites réelles _____	79
1. Les nombres réels	79
1.1. \mathbb{R} est un corps commutatif totalement ordonné	79
1.2. Axiome de la borne supérieure	81
1.3. \mathbb{Q} est dense dans \mathbb{R} (pour votre culture générale)	83
2. Suites de nombres réels	84
2.1. Suites convergentes	84
2.1.1. Définition d'une suite convergente	84
2.1.2. Unicité de la limite	85

2.1.3. Limites et inégalités	87
2.1.4. Opérations sur les suites	88
2.2. Suites croissantes	89
2.3. Suites adjacentes	90
2.4. Limites infinies	92
2.5. Suites extraites	93
2.6. Développement décimal	94
3. Pour approfondir le sujet	95
3.1. Critère de Cauchy, théorème de Bolzano-Weierstrass	95
3.1.1. Critère de Cauchy	96
3.1.2. Théorème de Bolzano-Weierstrass	97
3.2. Combien y a-t-il de nombres réels ? (pour votre culture générale)	98
3.3. A propos de la construction des nombres réels (pour votre culture générale)	99