北航中法工程师学院
Centrale Pékin

Algèbre 1

École Centrale de Pékin

Cours de mathématiques du cycle préparatoire

30 novembre 2020

Table des matières

Chapitre 1 Ensembles

Table des matières du chapitre

1.1 Premières définitions et notations

Dans cette première partie, nous revenons sur les notions d'ensemble, d'élément, d'appartenance et d'inclusion.

Définition 1

- *Un* ***ensemble*** E *est une collection d'objets, appelés* ***éléments*** *de* E.
- *On dit que* x ***appartient*** *à* E *si* x *est un élément de l'ensemble* E*, et on note* $x \in E$.
- *Deux ensembles* E *et* F *sont* ***égaux*** *s'ils ont les mêmes éléments :* $\forall x, (x \in E \Leftrightarrow x \in F)$.
  On note $E = F$.

On privilégie les lettres capitales (E, X, A, ...) pour désigner les ensembles et les lettres minuscules (a, b, x, ...) pour désigner leurs éléments.

Un ensemble n'est pas forcément un ensemble de nombres. Si E est l'ensemble des nombres réels $\mathbb{R}$ alors x désigne un nombre réel, mais si E est l'ensemble des suites réelles, alors x désigne une suite réelle ou si E est l'ensemble des droites du plan, alors x désigne une droite du plan.

Il existe plusieurs façons de décrire un ensemble.

- On peut donner la liste de tous les éléments de l'ensemble E entre accolades { }, les éléments étant séparés par des virgules. Soit on explicite tous les éléments de E, par exemple $E = \{a, b, c, d\}$, soit on en écrit seulement quelques-uns suivis de points de suspension, par exemple $E = \{x_1, x_2, \ldots, x_n\}$.
  L'ordre des éléments n'a aucune importance : les ensembles $\{a, b\}$ et $\{b, a\}$ sont égaux. De plus, un élément ne peut pas appartenir plusieurs fois à un ensemble et s'il apparait plusieurs fois dans la liste, il s'agit en fait du même élément : les ensembles $\{a, b, a\}$ et $\{a, b\}$ sont égaux car ils ont les mêmes éléments. Par convention, chaque élément est généralement énuméré une seule fois.
- On peut définir un ensemble F par une propriété $\mathcal{P}$ qui caractérise les éléments de F parmi les éléments d'un ensemble connu E : $F = \{x \in E \mid \mathcal{P}(x)\}$. On dit que F est l'ensemble des éléments x de E tels que x vérifie la propriété $\mathcal{P}$.
  Cas particulier : Si F est un sous-ensemble de E et f est une application[1] de E dans F, alors l'ensemble $\{y \in F \mid \exists\, x \in E,\ y = f(x)\}$ se note plus simplement $\{f(x),\ x \in E\}$ en remplaçant $f(x)$ par son expression. On dit que c'est l'ensemble des $f(x)$ lorsque x parcourt E.
  Par exemple, $\{x^2,\ x \in \mathbb{N}\} = \{0^2, 1^2, 2^2, 3^2, 4^2, \ldots\}$.

1. La notion d'application sera introduite dans le chapitre 2. Intuitivement, une application de E dans F associe à chaque élément de E un élément de F.

Exemples 2

- *L'ensemble E des entiers naturels n tels que n est inférieur ou égal à 4 peut s'écrire*

$$E = \{n \in \mathbb{N} \mid n \leq 4\} \text{ ou } E = \{0, 1, 2, 3, 4\}.$$

- *Soit $n \in \mathbb{N}$. L'ensemble E des entiers naturels m tels que $1 \leq m \leq n$ peut s'écrire*

$$E = \{m \in \mathbb{N} \mid 1 \leq m \leq n\} \text{ ou } E = \{1, \ldots, n\}.$$

  On utilise également la notation $[\![1, n]\!]$ pour désigner cet ensemble.
  Plus généralement, pour tout $n \in \mathbb{N}$ et tout $p \in \mathbb{N}$ tels que $n \leq p$, les notations $\{n, \ldots, p\}$ ou $[\![n, p]\!]$ désignent l'ensemble des entiers naturels compris entre n et p.

- *L'ensemble P des entiers naturels pairs peut s'écrire*

$$P = \{p \in \mathbb{N} \mid p \text{ est pair }\} \text{ ou } P = \{2k,\ k \in \mathbb{N}\},$$

  Cet ensemble est encore noté parfois $2\mathbb{N}$.

- *L'ensemble des nombres réels x tels que $0 \leq x \leq 1$ peut s'écrire*

$$\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}.$$

  Il s'agit de l'intervalle noté $[0, 1]$.
  Plus généralement, pour tout a et tout b éléments de $\mathbb{R}$, l'ensemble $\{x \in \mathbb{R} \mid a \leq x \leq b\}$ est l'intervalle noté $[a, b]$.

Définition 3

- *On appelle **ensemble vide** \空集\, noté $\emptyset$, l'ensemble ne contenant aucun élément.*
- *Un ensemble constitué d'un unique élément x est appelé un **singleton** \单元集\. Il est donc de la forme $\{x\}$.*
- *Un ensemble constitué de deux éléments distincts a et b est appelé une **paire** \二元集合\. Il est donc de la forme $\{a, b\}$.*

Remarque 4 — *On a bien sûr $\{a, b\} = \{b, a\}$.*

Définition 5
Soient E et F deux ensembles.

- *On dit que E est **inclus** \包含\ dans F si tout élément de E est un élément de F :*

$$\forall x,\ (x \in E \Rightarrow x \in F) \text{ ou encore } \forall x \in E,\ x \in F.$$

  *On note $E \subset F$. On dit aussi que E est une **partie** (ou un sous-ensemble) de F.*

- *On dit que E est **strictement inclus** dans F si $E \subset F$ et $E \neq F$.*

Méthode 6 — *Ainsi, pour démontrer que E est inclus F, on commence par se donner un élément quelconque x de E en écrivant « Soit $x \in E$. » Il s'agit ensuite de montrer que x est un élément de F.*

Exemples 7

- *Tout ensemble E est inclus dans lui-même : $E \subset E$.*
- *L'ensemble vide est inclus dans tout ensemble E : $\emptyset \subset E$.*
- *L'ensemble $\{a, c\}$ est strictement inclus dans l'ensemble $\{a, b, c\}$: $\{a, c\} \subset \{a, b, c\}$.*
- *$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, les inclusions étant strictes.*
- *$[0, 1] \subset \mathbb{R}$.*
- *$\{2p \mid p \in \mathbb{N}\} \subset \mathbb{N}$.*

Il ne faut pas confondre l'appartenance et l'inclusion : on a $2 \in \{2,4,5\}$ mais $2 \not\subset \{2,4,5\}$, et $\{2\} \subset \{2,4,5\}$ mais $\{2\} \notin \{2,4,5\}$.

Le résultat suivant, élémentaire, est très utile en pratique.

PROPOSITION 8 (Principe de double-inclusion)
Soient E et F deux ensembles. On a $E = F$ si et seulement si $E \subset F$ et $F \subset E$.

MÉTHODE 9 — *Pour prouver l'égalité de deux ensembles E et F,*

- *soit on raisonne par équivalence en montrant la propriété :*

$$\forall x,\ (x \in E \Leftrightarrow x \in F)$$

- *soit, et c'est le plus courant, on utilise le principe de double-inclusion en montrant les deux propriétés :*

$$\forall x \in E,\ x \in F \quad \text{et} \quad \forall x \in F,\ x \in E.$$

Illustrons cette méthode sur deux exemples, l'un utilisant un raisonnement par équivalence, l'autre le principe de double inclusion.

EXERCICE 10 —

- *Montrer que $\{z \in \mathbb{C}^* \mid \overline{z} = z^2\} = \{1, j, j^2\}$, où $j = \mathrm{e}^{\frac{2i\pi}{3}}$.*
  ***Preuve** — Raisonnons par équivalence. Posons $A = \{z \in \mathbb{C}^* \mid \overline{z} = z^2\}$*
  Soit $z \in \mathbb{C}^*$. Il existe $r \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$ tels que $z = re^{i\theta}$.
  Ainsi, $z \in A$ si et seulement si $\overline{z} = z^2$, soit encore si et seulement si $re^{-i\theta} = r^2e^{2i\theta}$, et r étant non nul, si et seulement si $re^{3i\theta} = 1$.
  Or $re^{3i\theta} = 1$ si et seulement si $r = 1$ et $3\theta \equiv 0\ [2\pi]$ soit encore, $r = 1$ et $\theta \equiv 0\ [2\pi/3]$.
  Donc $z \in A$ si et seulement si $z \in \{1, j, j^2\}$.
  D'où $\{z \in \mathbb{C}^* \mid \overline{z} = z^2\} = \{1, j, j^2\}$. □
- *Soient a et b deux réels tels que $a \leq b$.*
  Montrer que
  $$[a,b] = \{(1-t)a + tb \mid t \in [0,1]\}.$$
  ***Preuve** — On exclut le cas trivial où $a = b$ et donc $[a,b] = \{a\}$, et on suppose dans la suite que $a \neq b$.*
  Raisonnons par double-inclusion.
  ▷ Soit $x \in [a,b]$. Posons $t_0 = \dfrac{x-a}{b-a}$, bien défini car $b - a \neq 0$, de sorte que $x = (1-t_0)a + bt_0$. Comme $a \leq x \leq b$, on a $0 \leq x - a \leq b - a$ et donc, $b - a$ étant strictement positif, $0 \leq \dfrac{x-a}{b-a} \leq 1$, soit encore $0 \leq t_0 \leq 1$. Donc $x = (1-t_0)a + t_0b \in \{(1-t)a + tb \mid t \in [0,1]\}$.
  D'où l'inclusion $[a,b] \subset \{(1-t)a + tb \mid t \in [0,1]\}$.
  ◁ Réciproquement, soit $x \in \{(1-t)a + tb \mid t \in [0,1]\}$. Il existe $t_0 \in [0,1]$ tel que $x = (1-t_0)a + t_0b$.
  On a $0 \leq t_0 \leq 1$ et donc $0 \leq 1 - t_0 \leq 1$. De l'inégalité $a \leq b$ et par positivité de t_0 et de $1 - t_0$, on a $t_0a \leq t_0b$ et $(1-t_0)a \leq (1-t_0)b$. On obtient donc $(1-t_0)a + t_0a \leq (1-t_0)a + t_0b \leq (1-t_0)b + t_0b$, soit après simplification $a \leq x \leq b$. Donc $x \in [a,b]$.
  D'où la seconde inclusion $\{(1-t)a + tb, t \in [0,1]\} \subset [a,b]$.
  De ces deux points, il vient $[a,b] = \{(1-t)a + tb \mid t \in [0,1]\}$. □

1.2 Ensemble des parties d'un ensemble

Dans cette partie, après avoir introduit l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble, nous étudions différentes opérations dans $\mathcal{P}(E)$ et leurs propriétés.

Dans toute cette partie, E désigne un ensemble et A, B et C désignent des parties (ou sous-ensembles) de E.

1.2.1 Définition

Définition 11
On note $\mathcal{P}(E)$ l'ensemble des parties \幂集\ de E : $\mathcal{P}(E) = \{A \mid A \subset E\}$.

$\mathcal{P}(E)$ est donc l'ensemble dont les éléments sont les sous-ensembles de E : $A \in \mathcal{P}(E) \Leftrightarrow A \subset E$. Ainsi, une partie A de E est à la fois un sous-ensemble de E ($A \subset E$) et un élément de $\mathcal{P}(E)$ ($A \in \mathcal{P}(E)$).

Exemples 12

- *Considérons l'ensemble $E = \{0, 1\}$. Les parties de E sont celles à 0 élément, $\emptyset$, celles à un élément, $\{0\}$ et $\{1\}$, et celles à deux éléments, $E = \{0, 1\}$.*
  Donc $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
- *Si $E = \emptyset$ alors $\mathcal{P}(E) = \{\emptyset\}$ et donc $\mathcal{P}(E)$ n'est pas vide.*
- *On a $\mathbb{Q} \subset \mathbb{R}$ et $\mathbb{Q} \in \mathcal{P}(\mathbb{R})$.*
- *On a $\pi \in \mathbb{R}$, $\{\pi\} \subset \mathbb{R}$ et $\{\pi\} \in \mathcal{P}(\mathbb{R})$.*

Remarque 13 — *Puisque que $E \subset E$ et $\emptyset \subset E$, on a $E \in \mathcal{P}(E)$ et $\emptyset \in \mathcal{P}(E)$. Ainsi, $\mathcal{P}(E)$ n'est jamais vide.*

1.2.2 Union et intersection de deux parties

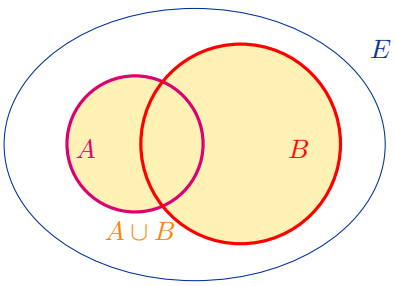
Définition 14 (Union, intersection)

- *On appelle **union** \并集\ de A et B, notée $A \cup B$ (se lit « A union B »), l'ensemble des éléments de E appartenant soit à A, soit à B :*

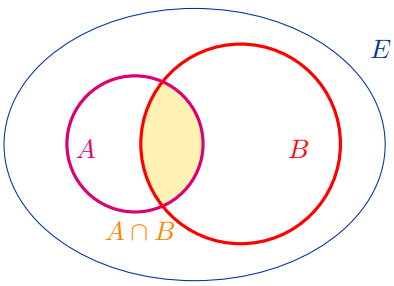
$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}.$$

- *On appelle **intersection** \交集\ de A et B, notée $A \cap B$ (se lit « A inter B »), l'ensemble des éléments de E appartenant à la fois à A et à B :*

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



Union



Intersection

Proposition 15

- *L'union $A \cup B$ vérifie :*
  - *$A \subset A \cup B$ et $B \subset A \cup B$.*
  - *Si $A \subset C$ et $B \subset C$ alors $A \cup B \subset C$.*

  On dit que $A \cup B$ est le plus petit ensemble au sens de l'inclusion qui contient A et B.
- *L'intersection $A \cap B$ vérifie :*
  - *$A \cap B \subset A$ et $A \cap B \subset B$.*
  - *Si $C \subset A$ et $C \subset B$ alors $C \subset A \cap B$.*

  On dit que $A \cap B$ est le plus grand ensemble au sens de l'inclusion qui est inclus dans A et dans B.

Preuve — Démontrons le premier point.

– Les propriétés $A \subset A \cup B$ et $B \subset A \cup B$ sont évidentes car, par exemple, si x appartient à A alors il appartient à A ou à B (puisqu'il appartient à A !), et donc à $A \cup B$.

– Supposons que $A \subset C$ et $B \subset C$. Soit $x \in A \cup B$. Montrons que $A \cup B \subset C$.

Par définition de l'union, $x \in A$ ou $x \in B$.

1er cas : $x \in A$. Alors $x \in C$ car par hypothèse $A \subset C$.

2nd cas : $x \in B$. Alors $x \in C$ car par hypothèse $B \subset C$.

Donc dans tous les cas, $x \in C$.

Donc $A \cup B \subset C$.

□

Remarque 16 — *On en déduit facilement les inclusions et égalités suivantes.*

- $A \cap B \subset A \subset A \cup B$ *et* $A \cap B \subset B \subset A \cup B$.
- $A \cup \emptyset = A$ *et* $A \cap \emptyset = \emptyset$, $A \cup E = E$ *et* $A \cap E = A$.
- *Si* $A \subset B$ *alors* $A \cup B = B$ *et* $A \cap B = A$.

Définition 17
On dit que A *et* B *sont* ***disjoints*** *si* $A \cap B = \emptyset$.

L'union $A \cup B$ *est alors souvent notée* $A \sqcup B$.

Deux ensembles sont disjoints si et seulement s'ils n'ont aucun élément en commun. Attention, deux ensembles peuvent être distincts (c'est-à-dire qu'ils ne sont pas égaux) mais non disjoints : $A = \{1, 2, 3\}$ et $B = \{3, 4, 5\}$ sont distincts car ils n'ont pas les mêmes éléments mais ils ne sont pas disjoints car 2 appartient à A et à B.

Les propositions 18 et 19 découlent directement des propriétés usuelles des connecteurs logiques « et » et « ou ». Elles se visualisent facilement sur des dessins.

Proposition 18 (Commutativité \交换律\, associativité \结合律\)

- $\cup$ *et* $\cap$ *sont* ***commutatives*** *:* $A \cup B = B \cup A$ *et* $A \cap B = B \cap A$.
- $\cup$ *et* $\cap$ *sont* ***associatives*** *:* $(A \cup B) \cup C = A \cup (B \cup C)$ *et* $(A \cap B) \cap C = A \cap (B \cap C)$.

Preuve — Traitons, par exemple, la première égalité du deuxième point, découlant de l'associativité de l'opération logique "ou" $\vee$. Les autres se démontrent en suivant le même modèle.

Soit $x \in E$.

$$\begin{aligned} x \in (A \cup B) \cup C &\Leftrightarrow x \in (A \cup B) \text{ ou } x \in C \Leftrightarrow (x \in A \text{ ou } x \in B) \text{ ou } x \in C \\ &\Leftrightarrow x \in A \text{ ou } (x \in B \text{ ou } x \in C) \Leftrightarrow x \in A \text{ ou } x \in B \cup C \\ &\Leftrightarrow x \in A \cup (B \cup C). \end{aligned}$$

Donc $(A \cup B) \cup C = A \cup (B \cup C)$. □

Proposition 19 (Distributivité \分配率\)

- *L'union est distributive sur l'intersection :*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

- *L'intersection est distributive sur l'union :*

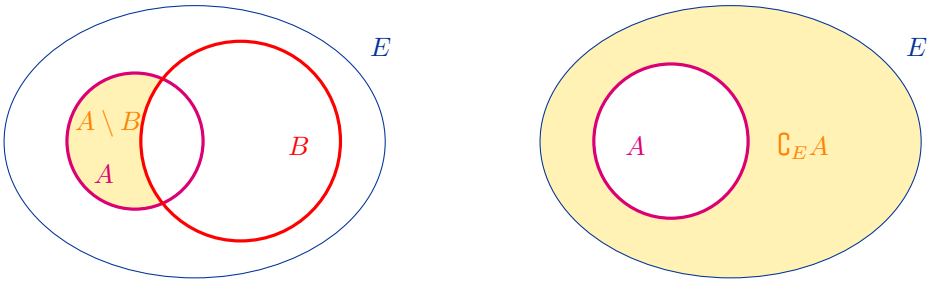
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Preuve — La première égalité découle de l'équivalence des propositions $p \vee (q \wedge r)$ et $(p \vee q) \wedge (p \vee r)$. La seconde égalité découle de l'équivalence des propositions $p \wedge (q \vee r)$ et $(p \wedge q) \vee (p \wedge r)$. □

1.2.3 Différence de deux parties et complémentaire

Définition 20

- *On appelle* ***différence*** $A \setminus B$ *(se lit « A privé de B » ou « A moins B ») l'ensemble des éléments de A n'appartenant pas à B :*
$$A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\}.$$
- *On appelle* ***complémentaire*** \补集\ *de A dans E, noté $\complement_E A$, la différence $E \setminus A$:*
$$\complement_E A = \{x \in E \mid x \notin A\}.$$



Différence Complémentaire

Lorsqu'il n'y a pas d'ambiguïté sur l'ensemble E considéré, on peut noter plus simplement $\complement A$ ou $\overline{A}$ (se lit « A barre »).

Exemples 21

- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $[0,2] \setminus [1,3] = [0,1[$.
- $\complement_{[0,1]} \left[0, \frac{1}{2}\right] = \left]\frac{1}{2}, 1\right]$.

Les propriétés suivantes découlent à nouveau des propriétés des opérateurs logiques. Elles se visualisent facilement sur des dessins.

Proposition 22 (Propriétés du complémentaire)

- $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$.
- $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$.

Preuve —

Prouvons la première égalité, la deuxième se démontrant se façon analogue .

Soit $x \in E$.

$$\begin{aligned} x \in \complement_E(A \cup B) &\Leftrightarrow x \notin A \cup B \Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow \neg(x \in A \text{ ou } x \in B) \\ &\Leftrightarrow \big(\neg(x \in A)\big) \text{ et } \big(\neg(x \in B)\big) \\ &\Leftrightarrow (x \notin A) \text{ et } (x \notin B) \Leftrightarrow x \in \complement_E A \text{ et } x \in \complement_E B \\ &\Leftrightarrow x \in \complement_E A \cap \complement_E B \end{aligned}$$

Donc $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$.

□

La proposition suivante donne une caractérisation du complémentaire.

Proposition 23
Si $A \cup B = E$ et $A \cap B = \emptyset$ alors $\complement_E A = B$.

Preuve — Supposons que $A \cup B = E$ et $A \cap B = \emptyset$.

Soit $x \in B$. Comme A et B sont disjoints, $x \notin A$ donc $x \in \complement_E A$. Donc $B \subset \complement_E A$.

Soit $x \in \complement_E A$. Comme $A \cup B = E$ et $x \notin A$, $x \in B$. Donc $\complement A \subset B$.

D'où le résultat. □

Exemple 24 — *On déduit facilement les égalités suivantes :* $\complement_E E = \emptyset$, $\complement_E \emptyset = E$, $\complement_E \complement_E A = A$.

1.2.4 Généralisation à une famille de parties

Soit I un ensemble non vide, dont les éléments sont appelés les **indices**. Pour chaque $i \in I$, on considère A_i une partie de l'ensemble E. On dit que les ensembles A_i forment une **famille** \族\ **de parties de** E, indicée par I, et notée $(A_i)_{i\in I}$.

Dans ce paragraphe, I désigne un ensemble non vide.

Les définitions et propriétés des parties précédentes se généralisent à des familles d'ensembles.

Définition 25
Soit $(A_i)_{i\in I}$ une famille de parties de E.

- *On appelle* ***union*** *de la famille $(A_i)_{i\in I}$ l'ensemble*
$$\bigcup_{i\in I} A_i = \{x \in E \mid \exists i \in I, x \in A_i\}.$$
C'est l'ensemble des éléments de E qui appartiennent au moins à l'un des A_i.
- *On appelle* ***intersection*** *de la famille $(A_i)_{i\in I}$ l'ensemble*
$$\bigcap_{i\in I} A_i = \{x \in E \mid \forall i \in I, x \in A_i\}.$$
C'est l'ensemble des éléments de E qui appartiennent à tous les A_i.

Proposition 26
Soit $(A_i)_{i\in I}$ une famille de parties de E et B une partie de E.

- $\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I} (A_i \cap B)$
- $\left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I} (A_i \cup B)$
- $\complement_E \left(\bigcup_{i\in I} A_i\right) = \bigcap \left(\complement_E A_i\right)$.
- $\complement_E \left(\bigcap_{i\in I} A_i\right) = \bigcup \left(\complement_E A_i\right)$.

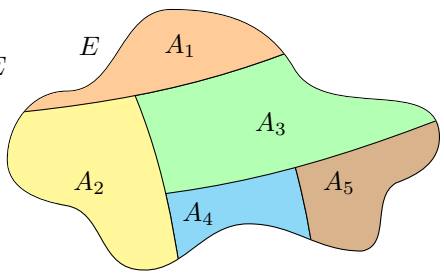
Définition 27
Soit $(A_i)_{i\in I}$ une famille de parties de E.

On dit que les ensembles A_i sont ***disjoints deux à deux*** *si pour tout i et tout j éléments distincts de I ($i \neq j$), $A_i \bigcap A_j = \emptyset$.*

L'union $\bigcup_{i\in I} A_i$ est alors notée $\bigsqcup_{i\in I} A_i$.

Définition 28
Soit $(A_i)_{i\in I}$ une famille de parties de E
On dit que la famille $(A_i)_{i\in I}$ forme une ***partition*** \划分\ *de E si*

1. *pour tout $i \in I$, A_i est non vide : $\forall i \in I, A_i \neq \emptyset$,*
2. *les A_i sont deux à deux disjoints : $\forall i \neq j, A_i \cap A_j = \emptyset$,*
3. $\bigcup_{i\in I} A_i = E$.



EXEMPLES 29

- *Notons $P = \{2k, k \in \mathbb{N}\}$ l'ensemble des nombres pairs et $I = \{2k+1, k \in \mathbb{N}\}$ l'ensemble des nombres impairs. P et I sont des ensembles non vides et disjoints. De plus, $P \cup I = \mathbb{N}$.*
  La famille $\{P, I\}$ forme donc une partition de $\mathbb{N}$.
- *La famille $([n, n+1[)_{n\in\mathbb{Z}}$ est une partition de $\mathbb{R}$.*

1.3 PRODUIT CARTÉSIEN D'ENSEMBLES

1.3.1 Couples et n-uplets

Un **couple** d'éléments est la donnée de deux éléments dans un certain ordre. On note un couple entre parenthèses : (a, b). Deux couples (a_1, b_1) et (a_2, b_2) sont égaux si et seulement si $a_1 = a_2$ et $b_1 = b_2$. On distingue donc le couple (a, b) (énumération ordonnée) de la paire $\{a, b\} = \{b, a\}$ (énumération non ordonnée). En général, $(a, b) \neq (b, a)$ alors que $\{a, b\} = \{b, a\}$. Enfin, dans le couple (a, b), les éléments a et b peuvent être égaux, le couple s'écrivant alors (a, a), mais l'ensemble $\{a, a\} = \{a\}$ est un singleton.

Pour tout $n \in \mathbb{N}$, la notion de couples se généralise à celle de **n-uplets** $(x_1, \ldots, x_n)$. Dans le cas où $n = 3$, on parle de **triplet** (x, y, z). Dans un n-uplet, certains éléments peuvent être égaux entre eux.

 Il ne faut pas confondre le n-uplet (ou la famille) $(x_1, \ldots, x_n)$ et l'ensemble $\{x_1, \ldots, x_n\}$. Par exemple, $(1, 2, 3) \neq (3, 2, 1)$ alors que $\{1, 2, 3\} = \{3, 2, 1\}$, ou $(1, 1, 2) \neq (1, 2)$ alors que $\{1, 1, 2\} = \{1, 2\}$.

1.3.2 Produit cartésien

DÉFINITION 30
*Soient E et F deux ensembles. Le **produit cartésien** \笛卡尔积\ de E par F, noté $E \times F$, est l'ensemble des couples (x, y) tels que $x \in E$ et $y \in F$:*

$$E \times F = \{(x, y) \mid x \in E, y \in F\}.$$

NOTATION Si $E = F$, le produit cartésien $E \times F$ se note E^2.

EXEMPLES 31

- *Soient $E = \{a, b\}$ et $F = \{1, 2, 3\}$.*
  Alors $E \times F = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.
- *$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ est l'ensemble des couples (x, y) de réels. On visualise cet ensemble comme un plan muni d'un repère, et le couple (x, y) est identifié au point de coordonnées (x, y).*
- *L'ensemble $\mathbb{R} \times \{0\} = \{(x, 0) \mid x \in \mathbb{R}\}$ correspond, dans le plan muni d'un repère, à l'axe des abscisses.*
- *$(\mathcal{P}(E))^2 = \mathcal{P}(E) \times \mathcal{P}(E)$ est l'ensemble des couples (A, B) où A et B sont des parties de E.*

 En général, $E \times F \neq F \times E$ car l'ordre importe dans un couple.

Le produit cartésien se généralise au produit de n ensembles.

DÉFINITION 32
*Soit n un entier naturel supérieur ou égal à 2. Soient E_1, ..., E_n n ensembles. On appelle **produit cartésien** de E_1, ..., E_n, noté $E_1 \times \ldots \times E_n$, l'ensemble des n-uplets $(x_1, \ldots, x_n)$ tels que pour tout $i \in \{1, \ldots, n\}$, $x_i \in E_i$:*

$$E_1 \times \ldots \times E_n = \{(x_1, \ldots, x_n) \mid \forall i \in \{1, \ldots, n\}, x_i \in E_i\}.$$

NOTATION Si $E_1 = \ldots = E_n = E$, on note le produit cartésien E^n.

Exemples 33

- $\mathbb{R}^n$ *désigne l'ensemble des* n*-uplets* $(x_1, \ldots, x_n)$ *de réels, i.e. tels que pour tout* $i \in \{1, \ldots, n\}$, $x_i \in \mathbb{R}$.
- $[0, +\infty[\times[0, 2\pi[\times[0, \pi[$ *est l'ensemble des triplets* (r, θ, φ) *où* $r \in [0, +\infty[$, $\theta \in [0, 2\pi[$ *et* $\varphi \in [0, \pi[$.

Chapitre 2 Applications

Table des matières du chapitre

2.1 Applications

2.1.1 Définitions

Intuitivement, une application f d'un ensemble E dans un ensemble F est un objet qui à tout élément x de E associe un unique élément y de F, noté $f(x)$.

Nous allons en donner une définition rigoureuse au moyen des ensembles.

Définition 1
*Soient E et F deux ensembles. On appelle **application de E dans F** \映射\ tout triplet $f = (E, F, \mathcal{G})$ où E, F et $\mathcal{G}$ sont trois ensembles vérifiant :*

1. *$\mathcal{G}$ est un sous-ensemble de $E \times F$,*
2. *pour tout élément x de E, il existe un unique élément y de F tel que $(x, y) \in \mathcal{G}$.*

Avec les notations précédentes,

- *E est appelé l'**ensemble de définition** \函数f的定义域\ ou ensemble de départ de f,*
- *F est appelé l'**ensemble d'arrivée** de f,*
- *$\mathcal{G}$ est appelé le **graphe** de f.*
- *Pour tout élément x de E, l'unique élément y de F tel que $(x, y) \in \mathcal{G}$ est noté $f(x)$, et est appelé **image** \像或值\ de x par f.*
- *Pour tout élément y de F, on appelle **antécédent** \原像\ de y par l'application f, tout élément x de E tel que $y = f(x)$.*
- *L'ensemble des applications de E dans F est noté F^E ou $\mathcal{F}(E, F)$.*

Remarque 2 — *Le graphe $\mathcal{G}$ de f est donc égal à $\mathcal{G} = \{(x, f(x)) \mid x \in E\}$.*

Notation En général, le triplet $f = (E, F, \mathcal{G})$ est noté de la façon suivante :

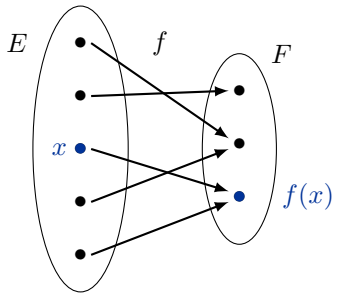
$$\begin{array}{rccc} f : & E & \longrightarrow & F \\ & x & \longmapsto & f(x) \end{array},$$

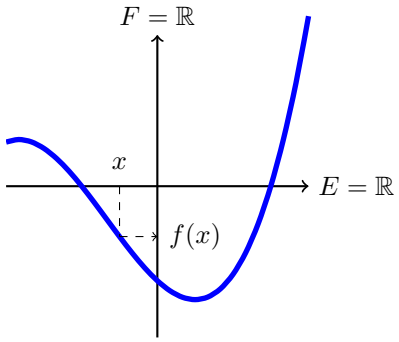
$f(x)$ étant remplacé par son expression.

On utilise également la notation $f : E \longrightarrow F$ pour signifier que f est une application de E dans F.

Remarque 3 — *Dans ce cours, on ne fera pas de distinction entre application et fonction.*

On peut représenter une application de deux manières : soit sous forme de diagrammes fléchés, soit en représentant son graphe dans le plan muni d'un repère, à la manière des courbes représentatives d'une fonction numérique.

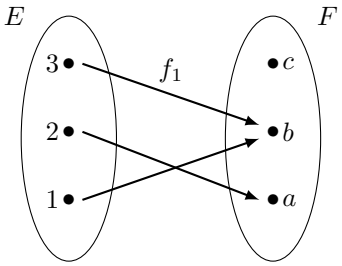




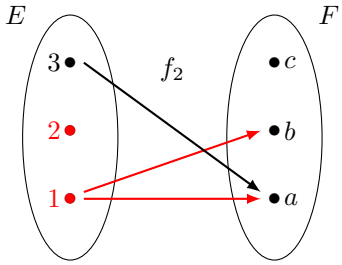
Exemples 4

- *Considérons les ensembles* $E = \{1, 2, 3\}$ *et* $F = \{a, b, c\}$. *Soient* $\mathcal{G}_1 = \{(1, b), (2, a), (3, b)\}$ *et* $\mathcal{G}_2 = \{(1, a), (1, b), (3, a)\}$ *deux sous-ensembles de* $E \times F$.

  Le triplet $(E, F, \mathcal{G}_1)$ *vérifie les points 1. et 2. de la définition et est donc une application* f_1 *de* E *dans* F. *On a* $f_1(1) = b$, $f_1(2) = a$ *et* $f_1(3) = b$.



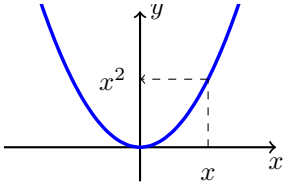
  Le triplet $(E, F, \mathcal{G}_2)$ *vérifie le point 1. mais ne vérifie pas le point 2. de la définition : à l'élément* 1 *de* E, *on ne peut pas associer un unique élément de* F *car les couples* $(1, a)$ *et* $(1, b)$ *sont éléments de* $\mathcal{G}_2$. *De plus, l'élément* 2 *de* E *ne peut être associé à aucun élément de* F *car il n'y a pas de couples de la forme* $(2, \cdot)$ *dans* $\mathcal{G}_2$. *Ainsi, ce triplet ne définit pas une application de* E *dans* F.



- *Considérons les ensembles* $E = \mathbb{R}$ *et* $F = \mathbb{R}$. *Soit* $\mathcal{G}_1 = \{(x, x^2) \mid x \in \mathbb{R}\}$ *un sous-ensemble de* $E \times F$.

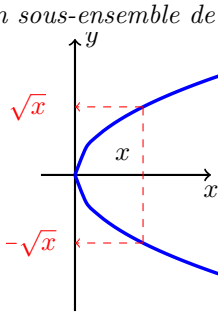
  Le triplet $(\mathbb{R}, \mathbb{R}, \mathcal{G}_1)$ *est une application* f *de* $\mathbb{R}$ *dans* $\mathbb{R}$, *notée*

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}.$$



- *Considérons les ensembles* $E = \mathbb{R}_+$ *et* $F = \mathbb{R}$. *Soit* $\mathcal{G}_2 = \{(x^2, x) \mid x \in \mathbb{R}\}$ *un sous-ensemble de* $E \times F$.

  Le triplet $(\mathbb{R}_+, \mathbb{R}, \mathcal{G}_2)$ *vérifie le point 1. mais ne vérifie pas le point 2. de la définition : à chaque élément* x *non nul de* $E = \mathbb{R}_+$, *on ne peut pas associer un unique élément de* $F = \mathbb{R}$ *car les couples* $(x, \sqrt{x})$ *et* $(x, -\sqrt{x})$ *sont éléments de* $\mathcal{G}_2$. *Ce triplet ne définit donc pas une application de* E *dans* F.



Remarque 5 — *Pour définir une application $f : E \longrightarrow F$, il suffit de préciser comment, à chaque élément x de E, est associée son image $f(x)$ dans F. C'est le principe de la notation $f : E \longrightarrow F\ ;\ x \longmapsto f(x)$.*

C'est désormais ainsi que nous définirons et manipulerons les applications.

Exemples 6

- *Soit E un ensemble. On appelle* ***application identité*** *de E, notée id_E, l'application définie par*
$$\begin{array}{rccc} \mathrm{id}_E : & E & \longrightarrow & E \\ & x & \longmapsto & x \end{array}.$$
- *Soient E et F deux ensembles. Soit a un élément de F. On appelle* ***fonction constante*** *égale à a l'application définie par*
$$\begin{array}{rccc} f : & E & \longrightarrow & F \\ & x & \longmapsto & a \end{array}.$$
- *Soient E et F deux ensembles tels que $E \subset F$. On appelle* ***injection canonique*** *de E dans F l'application définie par*
$$\begin{array}{rccc} i : & E & \longrightarrow & F \\ & x & \longmapsto & x \end{array}.$$
- *Soient E un ensemble non vide et A une partie de E. On appelle* ***fonction indicatrice de*** *A, notée $\mathbb{1}_A$ la fonction définie par*
$$\begin{array}{rccc} \mathbb{1}_A : & E & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases} \end{array}.$$
- *La fonction exponentielle* $\begin{array}{rccc} \exp : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \mathrm{e}^x \end{array}$ *est une application de $\mathbb{R}$ dans $\mathbb{R}$. La fonction logarithme* $\begin{array}{rccc} \ln : &]0;+\infty[& \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \ln x \end{array}$ *est une application de $]0;+\infty[$ dans $\mathbb{R}$.*

Remarque 7 — *Pour vérifier qu'une fonction $f : E \longrightarrow F$ définie par $x \longmapsto f(x)$ est bien définie, il faut vérifier les deux points suivants :*

1. *tout élément de E doit posséder une image et une seule,*
2. *cette image doit être dans F.*

Exemples 8

- *La relation $f : \mathbb{R} \longrightarrow \mathbb{R}\ ;\ x \longmapsto \dfrac{1}{x}$ n'est pas une application car 0 n'a pas d'image par f. Mais la relation $g : \mathbb{R}^* \longrightarrow \mathbb{R}\ ;\ x \longmapsto \dfrac{1}{x}$ est bien une application.*
- *La relation $f : \mathbb{U} \longrightarrow \mathbb{R}\ ;\ z \longmapsto \arg(z)$ n'est pas une application car tout élément de $\mathbb{U}$ possède une infinité d'images car l'argument d'un nombre complexe est défini modulo 2π.*
- *La relation $f : \mathbb{R} \longrightarrow \mathbb{R}_+\ ;\ x \longmapsto x^2 + 2x + 1$ est une application car pour tout $x \in \mathbb{R}$, x a une seule image par f, égale à $x^2 + 2x + 1$, et $x^2 + 2x + 1 = (x+1)^2 \geq 0$ donc $f(x) \in \mathbb{R}_+$.*

Définition 9

Deux applications f et g sont dites ***égales*** *si elles ont :*

1. *le même ensemble de départ E,*
2. *le même ensemble d'arrivée F,*
3. *le même graphe : pour tout $x \in E$, $f(x) = g(x)$.*

On note $f = g$.

Exemple 10 — *Les applications $f : \mathbb{R} \longrightarrow \mathbb{R}\ ;\ x \longmapsto x^2$ et $g : \mathbb{R}_+ \longrightarrow \mathbb{R}\ ;\ x \longmapsto x^2$ ne sont pas égales car elles n'ont pas le même ensemble de départ.*

2.1.2 Restrictions et prolongements

Définition 11
Soient E et F deux ensembles. Soit A une partie de E. Soit $f : E \longrightarrow F$ une application. On appelle ***restriction*** *de f à A, l'application, notée $f_{|A}$, définie par*

$$f_{|A} : \begin{array}{ccc} A & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} .$$

Exemple 12 — *La fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie pour tout $x \in \mathbb{R}$ par $f(x) = x^2$ n'est pas strictement croissante mais la restriction $f_{|\mathbb{R}_+}$ de f à $\mathbb{R}_+$ l'est.*

Définition 13
Soient E et F deux ensembles. Soit A une partie de E. Soit $f : A \longrightarrow F$ une application. On appelle ***prolongement*** *de f à E, toute application g de E dans F telle que, pour tout élément x de A, $g(x) = f(x)$.*

Un tel prolongement vérifie $g_{|A} = f$. Il n'est bien sûr pas unique. On parlera donc **d'un** prolongement et non **du** prolongement.

Exemple 14 — *On peut prolonger l'application $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ définie pour tout $x \in \mathbb{R}^*$ par $f(x) = \dfrac{\sin(x)}{x}$ sur $\mathbb{R}$ en fixant une valeur en 0. Par exemple, l'application suivante est un prolongement de f sur $\mathbb{R}$:*

$$\tilde{f} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \dfrac{\sin(x)}{x} \text{ si } x \neq 0, \\ 1 \text{ si } x = 0 \end{cases} \end{array} .$$

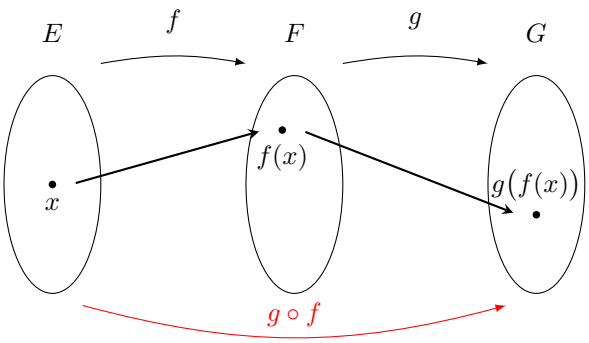
La valeur choisie en 0 est 1. Il s'agit de la limite de $\dfrac{\sin(x)}{x}$ lorsque x tend vers 0. L'intérêt de ce prolongement parmi les autres est que la fonction $\tilde{f}$ ainsi définie est continue sur $\mathbb{R}$.

2.1.3 Composée d'applications

Définition 15
Soient E, F et G trois ensembles. Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. La ***composée*** *$g \circ f$ \函数f和g的复合\ est l'application définie par :*

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

On pourra retenir le schéma suivant :



Remarques 16

- *Avec les notations ci-dessus, $g \circ f$ est bien définie mais ce n'est pas forcément le cas de $f \circ g$: on doit s'assurer que pour tout $x \in F$, $g(x) \in E$ afin de pouvoir appliquer f.*
- *Si $E = G$ alors $g \circ f$ et $f \circ g$ sont bien définies mais en général, ces deux applications ne sont pas égales : $g \circ f \neq f \circ g$. On dit que la composition $\circ$ n'est pas commutative.*

 On fera donc attention à l'ordre : pour calculer $\big(g \circ f\big)(x)$, on calcule d'abord $f(x)$ puis $g\big(f(x)\big)$.

Exemple 17 — *Soient f et g deux applications définies par*

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \qquad \text{et} \qquad g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x+1 \end{array} .$$

Pour tout $x \in \mathbb{R}$, on a $\big(g \circ f\big)(x) = g\big(f(x)\big) = f(x) + 1 = x^2 + 1$

et $\big(f \circ g\big)(x) = f\big(g(x)\big) = \big(g(x)\big)^2 = (x+1)^2 = x^2 + 2x + 1$.

Donc $g \circ f$ et $f \circ g$ ne sont pas égales.

Remarque 18 — *Par abus, lorsque l'on a deux applications $f : E \longrightarrow F$ et $g : H \longrightarrow G$ avec seulement $F \subset H$ (au lieu de $F = H$), on utilise aussi la notation $g \circ f$ pour désigner la composée $g_{|F} \circ h$.*

Proposition 19
Soient E, F, G et H des ensembles. Soient $f : E \longrightarrow F$, $g : F \longrightarrow G$ et $h : G \longrightarrow H$ trois applications. Alors

- *$\circ$ est associative : $(h \circ g) \circ f = h \circ (g \circ f)$.*
- $\mathrm{id}_E \circ f = f \circ \mathrm{id}_E = f$.

Preuve —

- Soit $x \in E$. On a $\Big((h \circ g) \circ f\Big)(x) = (h \circ g)(f(x)) = h\Big(g\big(f(x)\big)\Big) = h\big(\,(g \circ f)\,(x)\big) = \big(h \circ (g \circ f)\big)(x)$.
  D'où le premier point.
- Soit $x \in E$. On a $\big(\mathrm{id}_E \circ f\big)(x) = \mathrm{id}_E\big(f(x)\big) = f(x) = f\big(\mathrm{id}_E(x)\big) = \big(f \circ \mathrm{id}_E\big)(x)$.
  D'où le second point.

□

Notation Soient E un ensemble non vide et f une application de E dans E. On peut composer f avec elle-même autant de fois que l'on veut.

On note ainsi pour tout $n \in \mathbb{N}^*$, $f^n = \underbrace{f \circ f \ldots \circ f}_{n \text{ fois}}$ et $f^0 = \mathrm{id}_E$.

 En général, la composition $\circ$ n'étant pas commutative, si f et g sont deux applications d'un ensemble E dans lui même, $(g \circ f)^n \neq g^n \circ f^n$. Mais si f et g commutent, alors $(g \circ f)^n = g^n \circ f^n$.

Exemples 20

- *Soit l'application $f : \mathbb{R} \to \mathbb{R}$ définie, pour tout $x \in \mathbb{R}$, par $f(x) = x + 1$.*
  Pour tout $n \in \mathbb{N}$ et tout $x \in \mathbb{R}$, $f^n(x) = \Big(\big((x+1)+1\big) + \ldots\Big) + 1 = x + n$.
- *Reprenons l'exemple 17 où f et g sont deux applications de $\mathbb{R}$ dans $\mathbb{R}$ définies pour tout $x \in \mathbb{R}$, par $f(x) = x^2$ et $g(x) = x + 1$.*
  On a vu que pour tout $x \in \mathbb{R}$, $\big(g \circ f\big)(x) = x^2 + 1$, donc $\big(g \circ f\big)^2(x) = \big(g \circ f\big)(x^2 + 1) = (x^2+1)^2 + 1 = x^4 + 2x^2 + 2$.
  De plus, pour tout $x \in \mathbb{R}$, $f^2(x) = x^4$ et $g^2(x) = x + 2$. Donc $\big(g^2 \circ f^2\big)(x) = g^2\big(x^4\big) = x^4 + 2$.
  Donc $(g \circ f)^2 \neq g^2 \circ f^2$.

2.1.4 Familles

Définition 21
Soient E et I deux ensembles. On appelle ***famille d'éléments de E indexée par I****, toute application $x : I \longrightarrow E$. On la note $(x_i)_{i\in I}$, où pour tout $i \in I$, $x_i = x(i)$.*

L'élément x_i de la famille $(x_i)_{i\in I}$ s'appelle le ***terme d'indice*** *i.*

Exemple 22 — *Une famille $(x_1, \dots, x_n)$ d'éléments de E correspond donc à l'application $x : [\![1, n]\!] \longrightarrow E$ telle que pour tout $i \in [\![1, n]\!]$, $x(i) = x_i$.*

Définition 23
Soit E un ensemble. Une ***suite*** *d'éléments de E est une famille d'éléments de E indexée par $\mathbb{N}$. On la note souvent $(u_n)_{n\in\mathbb{N}}$.*

Exemple 24 — *L'ensemble des suites réelles est l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{R}$, noté $\mathbb{R}^{\mathbb{N}}$.*

2.2 Image directe, image réciproque

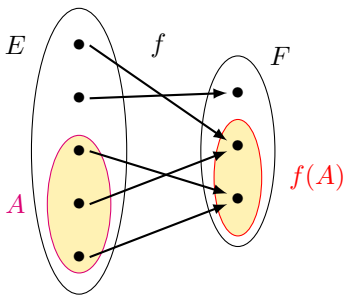
2.2.1 Image directe

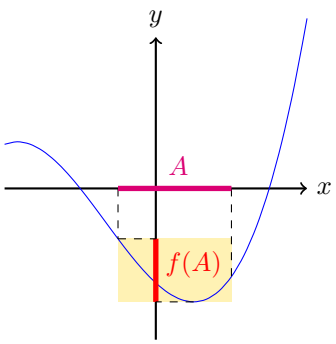
Définition 25
Soit $f : E \longrightarrow F$ une application. Soit A une partie de E.

- *On appelle* ***image directe*** *de A par f \集合A在映射f下的像\, notée $f(A)$, l'ensemble des images par f des éléments de A :*

$$f(A) = \{y \in F \mid \exists\, x \in A, y = f(x)\} = \{f(x) \mid x \in A\}.$$

- *L'image de E tout entier par f est simplement appelée* ***image de*** *f. Elle est souvent notée $\mathrm{Im}(f)$ plutôt que $f(E)$.*





L'image de f correspond à l'ensemble des éléments de F qui ont au moins un antécédent par f. En général, si $f : E \longrightarrow F$, l'inclusion $\mathrm{Im}(f) \subset F$ est stricte.

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

Si $x \in A$ alors $f(x) \in f(A)$ mais la réciproque est fausse : $f(x) \in f(A)$ n'implique pas $x \in A$ (voir le schéma ci-dessus).

EXEMPLES 26

- *L'image de l'application identité* id_E *est* E.
- *Soit* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *l'application définie, pour tout* $x \in \mathbb{R}$, *par* $f(x) = x^2$.
  Alors $f([-2,2]) = [0,4]$, $f([-1,2]) = [0,4]$ *et* $\mathrm{Im}(f) = \mathbb{R}_+$.
  Plus généralement, pour déterminer l'ensemble image d'une fonction $f : I \longrightarrow \mathbb{R}$ *où* I *est un intervalle de* $\mathbb{R}$, *on étudie les variations de* f *et sa continuité.*
- *Soit* $f : \mathbb{C} \longrightarrow \mathbb{R}$ *l'application définie, pour tout* $z \in \mathbb{C}$, *par* $f(z) = \mathrm{Im}(z)^2$. *L'image de* f *est l'ensemble* $\mathbb{R}_+$ *:* $\mathrm{Im}(f) = \mathbb{R}_+$.
  Preuve *— Montrons ce résultat par double-inclusion.*
  Pour tout $z \in \mathbb{C}$, $\mathrm{Im}(z) \in \mathbb{R}$ *et donc* $\mathrm{Im}(z)^2 \in \mathbb{R}_+$. *Donc* $\mathrm{Im}(f) \subset \mathbb{R}_+$.
  Réciproquement, soit $x \in \mathbb{R}_+$. *Posons* $z = i\sqrt{x} \in \mathbb{C}$. *Alors* $\mathrm{Im(z)} = \sqrt{x}$ *et donc* $f(z) = \left(\sqrt{x}\right)^2 = x$. *Donc* $x \in \mathrm{Im}(f)$.
  D'où $\mathbb{R}_+ \subset \mathrm{Im}(f)$. □
- *L'image de* $\pi\mathbb{Z} = \{\pi k, k \in \mathbb{Z}\}$ *par l'application* $\sin : \mathbb{R} \longrightarrow \mathbb{R}$ *est égale à* $\{0\}$. *L'image de* $[0, 2\pi]$ *est* $[-1,1]$, *celle de* $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ *est aussi* $[-1,1]$.

DÉFINITION 27
Soient $f : E \longrightarrow F$ *une application et* B *un sous-ensemble de* F. *On dit que* f *est* ***à valeurs dans*** B *si l'image de* f *est incluse dans* B *:* $\mathrm{Im}(f) \subset B$.

Autrement dit, pour tout $x \in E$, $f(x) \in B$.

PROPOSITION 28
Soit $f : E \longrightarrow F$ *une application. Soient* A *et* B *des parties de* E.

1. *Si* $A \subset B$ *alors* $f(A) \subset f(B)$.
2. $f(A \cup B) = f(A) \cup f(B)$.
3. $f(A \cap B) \subset f(A) \cap f(B)$.

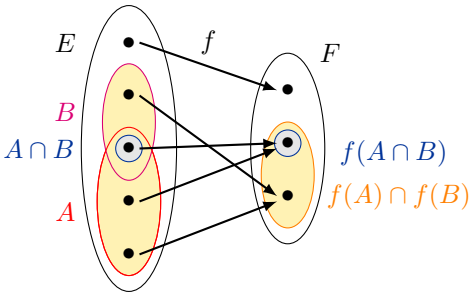
REMARQUE 29 — *Les propriétés* 2. *et* 3. *se généralisent à une famille quelconque de parties de* E.

Preuve —

1. Supposons $A \subset B$. Montrons que $f(A) \subset f(B)$. Soit $y \in f(A)$.
   Par définition de $f(A)$, il existe $x \in A$ tel que $y = f(x)$. Or $A \subset B$, donc $x \in B$. Donc $y = f(x) \in f(B)$.
   D'où $f(A) \subset f(B)$.
2. ▷ Montrons que $f(A \cup B) \subset f(A) \cup f(B)$.
   Soit $y \in f(A \cup B)$. Par définition de $f(A \cup B)$, il existe $x \in A \cup B$ tel que $y = f(x)$.
   1er cas : $x \in A$. Alors $y = f(x) \in f(A)$. Or $f(A) \subset f(A) \cup f(B)$. Donc $x \in f(A) \cup f(B)$.
   2nd cas : $x \in B$. Alors $y = f(x) \in f(B)$. Or $f(B) \subset f(A) \cup f(B)$. Donc $x \in f(A) \cup f(B)$.
   Dans tous les cas, $x \in f(A) \cup f(B)$. Donc $f(A \cup B) \subset f(A) \cup f(B)$.
   ◁ Réciproquement, montrons que $f(A) \cup f(B) \subset f(A \cup B)$.
   On a $A \subset A \cup B$ donc, d'après le deuxième point, $f(A) \subset f(A \cup B)$.
   De même, comme $B \subset A \cup B$, $f(B) \subset f(A \cup B)$.
   Donc $f(A \cup B)$ contient $f(A)$ et $f(B)$. Or $f(A) \cup f(B)$ est le plus petit ensemble qui contient $f(A)$ et $f(B)$, donc $f(A) \cup f(B) \subset f(A \cup B)$.
   De ces deux points, on obtient le résultat.
3. Soit $y \in f(A \cap B)$. Par définition de $A \cap B$, il existe $x \in A \cap B$ tel que $y = f(x)$.
   Comme $A \cap B \subset A$, $x \in A$ et $y = f(x) \in f(A)$.
   Comme $A \cap B \subset B$, $x \in B$ et $y = f(x) \in f(B)$.
   Donc $x \in f(A) \cap f(B)$.
   D'où le résultat.

□

Attention, l'inclusion $f(A \cap B) \subset f(A) \cap f(B)$ peut être stricte, comme le montre le schéma suivant. On peut également considérer l'exemple suivant : $\sin([0, 2\pi]) \cap \sin([-\pi, \pi]) = [-1, 1]$ et $\sin([0, 2\pi] \cap [-\pi, \pi]) = [0, 1]$.



Remarque 30 — *On ne peut en général rien dire sur* $f\left(\complement_E A\right)$ *et* $\complement_F f(A)$.

Exemple 31 — *Soit* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *l'application définie, pour tout* $x \in \mathbb{R}$, *par* $f(x) = x^2$. *Soit* $A = [-1; 3]$.

On a $\complement A =]-\infty, -1[\cup]3, +\infty[$.

Donc $f\left(\complement A\right) =]1, +\infty[$ *et* $\complement f(A) = \complement[0, 9] =]-\infty, 0[\cup]9, +\infty[$. *Il n'y a donc aucune inclusion entre ces ensembles.*

Définition 32
Soient E *un ensemble et* A *une partie de* E. *Soit* $f : E \longrightarrow E$ *une application. On dit que* A *est* ***stable*** *par* f *si* $f(A) \subset A$.

Autrement dit, pour tout $x \in A$, $f(x) \in A$.

Exemple 33 — *L'intervalle* $[-1, 1]$ *est une partie stable par la fonction* $f : \mathbb{R} \longrightarrow \mathbb{R}$; $x \longmapsto x^2$.

2.2.2 Image réciproque

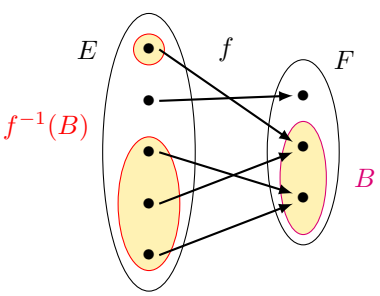
Définition 34
Soit $f : E \longrightarrow F$ *une application. Soit* B *une partie de* F. *On appelle* ***image réciproque*** *de* B *par* f \集合B在映射f下的原像\ , *notée* $f^{-1}(B)$, *l'ensemble*

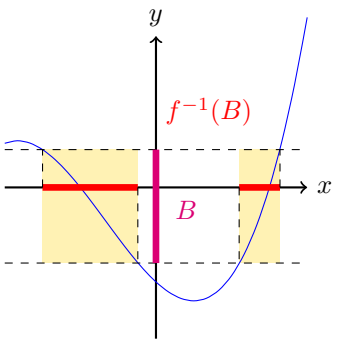
$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

$f^{-1}(B)$ correspond à l'ensemble des éléments de E dont l'image par f appartient à B. C'est aussi l'ensemble des antécédents des éléments de B par f.

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

Remarque 35 — *Si* $f : E \longrightarrow F$, *on a toujours* $f^{-1}(F) = E$.





Remarques 36

- *Pour chercher l'image réciproque par une application $f : \mathbb{R} \longrightarrow \mathbb{R}$ d'un singleton $\{y\}$, on résout l'équation $f(x) = y$ d'inconnue x,*
- *Pour chercher l'image réciproque par une application $f : \mathbb{R} \longrightarrow \mathbb{R}$ d'un intervalle $[a, b]$, on résout l'inéquation $a \leq f(x) \leq b$.*

L'image directe d'un singleton est un singleton : $f(\{x\}) = \{f(x)\}$, mais on ne peut rien dire sur l'image réciproque d'un singleton $f^{-1}(\{y\})$, qui correspond à l'ensemble des antécédents de y : cela peut être un singleton, un ensemble à plusieurs éléments, E tout entier (si f est constante égale à y) ou encore l'ensemble vide (si y n'a pas d'antécédent).

Exemples 37

- *Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ l'application définie, pour tout $x \in \mathbb{R}$, par $f(x) = x^2$. Alors $f^{-1}([0, 4]) = [-2, 2]$, $f^{-1}([-2, 4]) = [-2, 2]$, $f^{-1}([-2, -1]) = \emptyset$,$f^{-1}([9, +\infty[) =]-\infty, 3] \cup [3, +\infty[$.*
- *L'image réciproque de $\mathbb{R}_+$ par l'application* exp *est $\mathbb{R}$.*
- *L'image réciproque de $\{1\}$ par la fonction* sin $: \mathbb{R} \longrightarrow \mathbb{R}$ *est l'ensemble $\dfrac{\pi}{2} + 2\pi\mathbb{Z}$. L'image réciproque de $\{2\}$ est l'ensemble vide. L'image réciproque de $[0, 1]$ est $\bigcup_{k\in\mathbb{Z}} [2k\pi, (2k + 1)\pi]$.*

Proposition 38
Soit $f : E \longrightarrow F$ une application. Soient A et B des parties de F.

1. *Si $A \subset B$ alors $f^{-1}(A) \subset f^{-1}(B)$.*
2. *$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.*
3. *$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.*
4. *$f^{-1}\left(\complement_E A\right) = \complement_E f^{-1}(A)$.*

Preuve —

1. Supposons $A \subset B$. Soit $x \in f^{-1}(A)$.
   Alors $f(x) \in A$. Or $A \subset B$, donc $f(x) \in B$. Donc $x \in f^{-1}(B)$.
   Donc $f^{-1}(A) \subset f^{-1}(B)$.
2. Soit $x \in E$.
   $x \in f^{-1}(A \cup B) \Leftrightarrow f(x) \in A \cup B \Leftrightarrow f(x) \in A$ ou $f(x) \in B \Leftrightarrow x \in f^{-1}(A)$ ou $x \in f^{-1}(B) \Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B)$.
   D'où le deuxième point.
3. Soit $x \in E$.
   $x \in f^{-1}(A \cap B) \Leftrightarrow f(x) \in A \cap B \Leftrightarrow f(x) \in A$ et $f(x) \in B \Leftrightarrow x \in f^{-1}(A)$ et $x \in f^{-1}(B) \Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B)$.
   D'où le troisième point.
4. Soit $x \in E$.
   $x \in f^{-1}(\complement_E A) \Leftrightarrow f(x) \in \complement_E A \Leftrightarrow f(x) \notin A \Leftrightarrow x \notin f^{-1}(A) \Leftrightarrow x \in \complement_E f^{-1}(A)$.
   D'où le quatrième point.

□

Proposition 39
Soit $f : E \longrightarrow F$ une application. Soient A une partie de E et B une partie de F.

1. *$A \subset f^{-1}(f(A))$.*
2. *$f\left(f^{-1}(B)\right) \subset B$.*

Preuve —

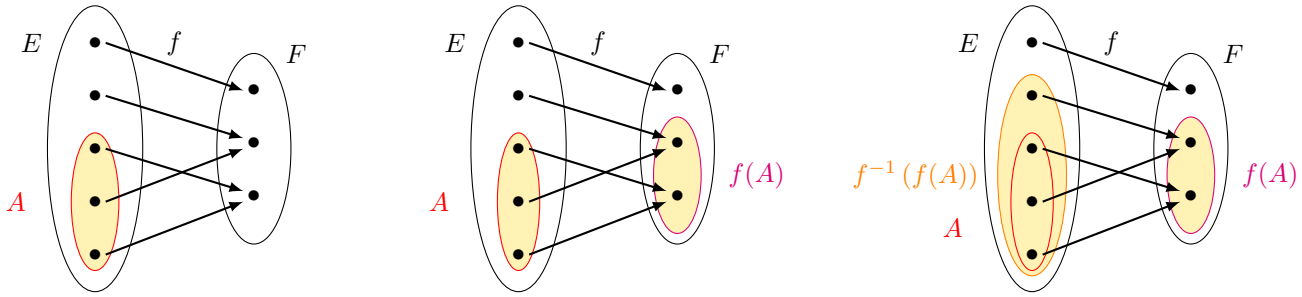
1. Soit $x \in A$. Alors $f(x) \in f(A)$. Donc $x \in f^{-1}(f(A))$. D'où le premier point.
2. Soit $y \in f\left(f^{-1}(B)\right)$. Alors il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. Comme $x \in f^{-1}(B)$, $f(x) \in B$. Donc $y = f(x) \in B$.
   D'où le second point.

□

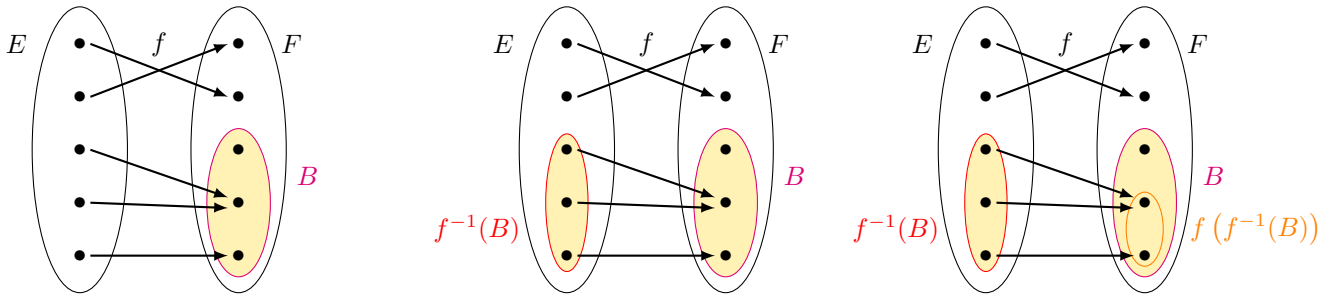
Le deuxième point nous dit que l'image d'un antécédent d'un élément de B est dans B.

Les inclusions sont strictes comme on peut le voir sur les schémas suivants.

• $A \subset f^{-1}(f(A))$ et l'inclusion est stricte :



• $f\left(f^{-1}(B)\right) \subset B$ et l'inclusion est stricte :



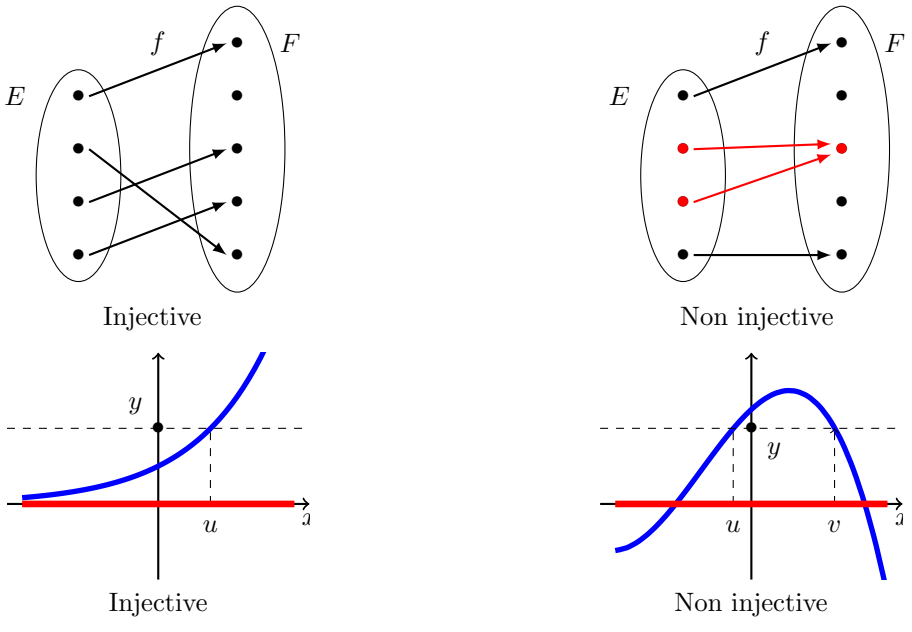
On peut également prendre les exemples suivants :

$[0, 2\pi] \subset \mathbb{R} = \cos^{-1}(\cos([0, 2\pi]))$ et $\cos\left(\cos^{-1}(\mathbb{R})\right) = [-1, 1] \subset \mathbb{R}$.

2.3 Injectivité, surjectivité et bijectivité

2.3.1 Injectivité

Définition 40
On dit qu'une application $f : E \longrightarrow F$ est ***injective*** \单射\ *si tout élément de l'ensemble d'arrivée F a au plus* \至多\ *un antécédent dans E par f.*



PROPOSITION 41
Soit $f : E \longrightarrow F$ une application. Les propositions suivantes sont équivalentes :

1. *f est injective,*
2. *Pour tout $(u, v) \in E^2$, si $f(u) = f(v)$ alors $u = v$,*
3. *Pour tout $(u, v) \in E^2$, si $u \neq v$ alors $f(u) \neq f(v)$.*

Preuve — • Supposons f injective. Soit $(u, v) \in E^2$ tel que $f(u) = f(v)$. Posons $y = f(u) = f(v)$. Les éléments u et v sont deux antécédents de y. Or, par définition d'une application injective, y a au plus un antécédent par f. Donc $u = v$.

• Réciproquement, supposons que pour tout $(u, v) \in E^2$, si $f(u) = f(v)$ alors $u = v$. Soit $y \in F$. Supposons, par l'absurde, que y possède au moins deux antécédents distincts par f. Alors il existe deux éléments u_0 et v_0 de E distincts tels que $y = f(u_0) = f(v_0)$. Donc, par hypothèse, $u_0 = v_0$, ce qui est absurde. Donc y possède au plus un antécédent dans E par f. Tout élément de F possède donc au plus un antécédent et f est donc injective.

• Le point 2 est équivalent au point 3 par contraposée. □

Le deuxième point dit que si les images de deux éléments sont égales alors les éléments sont égaux. Le troisième point dit que deux éléments différents ont des images différentes. Cette dernière formulation est plus simple à comprendre mais plus difficile à manipuler en pratique. On privilégiera donc plutôt le deuxième point pour démontrer qu'une application est injective.

MÉTHODE 42 — *Pour montrer qu'une application f n'est* pas *injective, on montre qu'il existe deux éléments u et v de E* distincts *tels que $f(u) = f(v)$, en donnant explicitement les éléments u et v.*

EXEMPLES 43

- *L'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie pour tout $x \in \mathbb{R}$ par $f(x) = x^2$ n'est pas injective.*
  ***Preuve** — En effet, en prenant $u = 1$ et $v = -1$, on a $u \neq v$ et $f(u) = f(v) = 1$.* □
- *L'application $g : \mathbb{C} \setminus \{1\} \longrightarrow \mathbb{C}$ définie pour tout $z \in \mathbb{C} \setminus \{1\}$ par $g(z) = \dfrac{z+i}{z-1}$ est injective.*
  ***Preuve** — En effet, soit z_1 et z_2 deux éléments de $\mathbb{C} \setminus \{1\}$ tels que $g(z_1) = g(z_2)$. Montrons que $z_1 = z_2$.*
  On a $\dfrac{z_1+i}{z_1-1} = \dfrac{z_2+i}{z_2-1}$, et après calculs, $z_1(1+i) = z_2(1+i)$. Donc $z_1 = z_2$.
  Donc g est injective. □
- *Soient E et F deux ensembles tels que $E \subset F$. L'application identité id_E et l'injection $i : E \longrightarrow F$ définie pour tout $x \in E$ par $i(x) = x$ sont injectives.*

PROPOSITION 44
Soit I un intervalle de $\mathbb{R}$. Soit $f : I \longrightarrow \mathbb{R}$ une application à valeurs réelles. Si f est strictement monotone sur I alors f est injective.

Preuve — Supposons f strictement monotone. Quitte à considérer $-f$, supposons f strictement croissante. Montrons que f est injective.

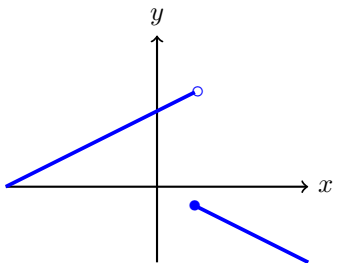
Soient u et v deux éléments de I tels que $f(u) = f(v)$.

Si $u < v$ alors par stricte croissance de f, $f(u) < f(v)$, ce qui est absurde.

Si $u > v$ alors par stricte croissance de f, $f(u) > f(v)$, ce qui est absurde.

Donc finalement, $u = v$ et l'application f est injective. □

La réciproque est fausse comme le montre la représentation graphique suivante :



EXEMPLE 45 — *La fonction $\exp : \mathbb{R} \longrightarrow \mathbb{R}$ est strictement croissante sur $\mathbb{R}$ donc injective.*

PROPOSITION 46
Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- *Si f et g sont injectives alors $g \circ f$ est injective.*
- *Si $g \circ f$ est injective alors f est injective.*

Preuve —

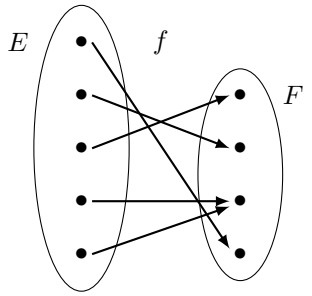
- Supposons f et g injectives. Montrons que $g \circ f$ est injective.
  Soient u et v deux éléments de E tels que $(g \circ f)(u) = (g \circ f)(v)$. Alors $g(f(u)) = g(f(v))$. Par injectivité de g, on a donc $f(u) = f(v)$, puis par injectivité de f, on obtient $u = v$.
  Donc $g \circ f$ est injective.
- Supposons $g \circ f$ injective. Montrons que f est injective.
  Soient u et v deux éléments de E tels que $f(u) = f(v)$. Alors $g(f(u)) = g(f(v))$, soit encore $(g \circ f)(u) = (g \circ f)(v)$. Par injectivité de $g \circ f$, on en déduit que $u = v$.
  Donc f est injective.

□

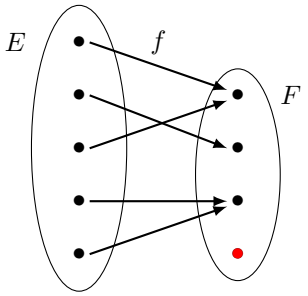
Dans le deuxième point, l'application g n'a aucune raison d'être injective. Par exemple, en considérant $f : \mathbb{R} \longrightarrow \mathbb{R}$; $x \longmapsto \exp(x)$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$; $x \longmapsto x^2$, l'application $g \circ f$ est injective mais g n'est évidemment pas injective !

2.3.2 Surjectivité

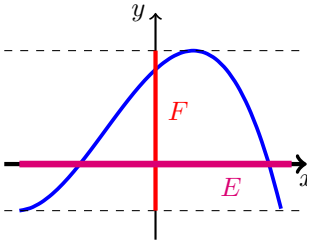
DÉFINITION 47
*On dit qu'une application $f : E \longrightarrow F$ est **surjective** \满射\ si tout élément de l'ensemble d'arrivée F a au moins \至少\ un antécédent dans E par f.*



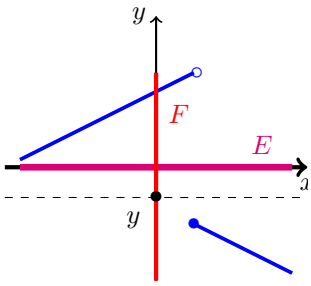
Surjective



Non surjective



Surjective



Non surjective

PROPOSITION 48
Soit $f : E \longrightarrow F$ une application. Les propositions suivantes sont équivalentes :

1. *f est surjective,*
2. *Pour tout élément y de F, il existe un élément x de E tel que $y = f(x)$,*
3. *$\mathrm{Im}(f) = F$.*

Preuve —

- Par définition de la surjectivité, f est surjective si et seulement pour tout élément y de F, y admet un antécédent $x \in E$ par f, soit si et seulement si pour tout $y \in E$, il existe $x \in E$ tel que $y = f(x)$.
- On a $\mathrm{Im}(f) = \{y \in F \mid \exists x \in E, y = f(x)\}$.
  Donc $\mathrm{Im}(f) = F$ si et seulement pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$.

□

Remarque 49 — *Soit $f : E \longrightarrow F$ une application. L'application induite par f de E sur $\mathrm{Im}(f)$, définie par $E \longrightarrow \mathrm{Im}(f)$; $x \longmapsto f(x)$, est surjective.*

Méthode 50 — *Pour montrer qu'une application $f : E \longrightarrow F$ est surjective, on peut montrer que pour tout $y \in F$, l'équation $y = f(x)$ d'inconnue x admet au moins une solution dans E.*

Exemples 51

- *L'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie pour tout $x \in \mathbb{R}$ par $f(x) = x^2$ n'est pas surjective car par exemple -1 n'a pas d'antécédent par f. Mais l'application induite par f de $\mathbb{R}$ sur son image $\mathbb{R}_+$ est surjective.*
- *L'application $g : \mathbb{R} \longrightarrow \mathbb{U}$ définie pour tout $\theta \in \mathbb{R}$ par $g(\theta) = e^{i\theta}$ est surjective.*
- *Soit E un ensemble. L'application id_E est surjective.*

Remarque 52 — *Il existe des applications qui ne sont ni surjectives, ni injectives, comme la fonction carré de $\mathbb{R}$ dans $\mathbb{R}$.*

Proposition 53
Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- *Si f et g sont surjectives alors $g \circ f$ est surjective.*
- *Si $g \circ f$ est surjective alors g est surjective.*

Preuve —

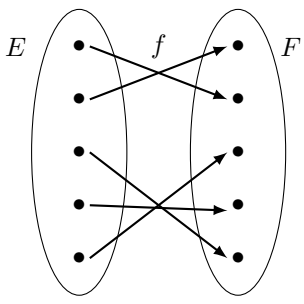
- Supposons f et g surjectives. Montrons que $g \circ f$ est surjective.
  Soit $z \in G$. Par surjectivité de g, il existe $y \in F$ tel que $z = g(y)$. Puis, par surjectivité de f, il existe $x \in E$ tel que $y = f(x)$. Donc $z = g(f(x)) = (g \circ f)(x)$.
  On a donc prouvé l'existence d'un élément x dans E tel que $z = (g \circ f)(x)$. L'application $g \circ f$ est donc surjective.
- Supposons $g \circ f$ surjective. Montrons que g est surjective.
  Soit $y \in G$. Par surjectivité de $g \circ f$, il existe $t \in E$ tel que $y = (g \circ f)(t)$, c'est-à-dire $y = g(f(t))$. En posant $x = f(t)$, on a donc $y = g(x)$ avec $x \in F$.
  On a donc prouvé l'existence d'un élément x dans F tel que $y = g(x)$. L'application g est donc surjective.

□

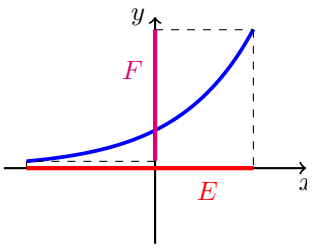
Dans le deuxième point, l'application f n'a aucune raison d'être surjective. Par exemple, en considérant $f : \mathbb{R} \longrightarrow \mathbb{R}$; $x \longmapsto e^x - 1$ et $g : \mathbb{R} \longrightarrow \mathbb{R}_+$; $x \longmapsto x^2$, l'application $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}_+$ est surjective mais f n'est évidemment pas surjective.

2.3.3 Bijectivité

Définition 54
*Soit $f : E \longrightarrow F$ une application. On dit que f est **bijective** \双射（一一映射）\ si tout élément de l'ensemble d'arrivée F a un unique \有且仅有一个\ antécédent dans E par f.*



Bijective



Bijective

PROPOSITION 55
Soit $f : E \longrightarrow F$ une application. Les propositions suivantes sont équivalentes :

1. *f est bijective,*
2. *pour tout élément y de F, il existe un unique élément x de E tel que $y = f(x)$,*
3. *f est injective et surjective.*

EXEMPLES 56

- *L'application $\mathrm{id}_E : E \longrightarrow E$ est bijective.*
- *L'application $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ définie pour tout $x \in \mathbb{R}_+$ par $f(x) = x^2$ est injective et surjective, donc bijective.*

PROPOSITION-DÉFINITION 57
Soit $f : E \longrightarrow F$ une application.

- *L'application f est bijective si et seulement s'il existe une application $g : F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.*
- *Dans ce cas, l'application g est unique. Elle est appelée **bijection réciproque** \f的逆映射\ de f et est notée f^{-1}.*

Preuve — • ▷ Supposons f bijective. Nous allons construire une application $g : F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.

Pour tout $y \in F$, il existe un unique élément x de E tel que $y = f(x)$. Posons, pour tout $y \in F$, $g(y) = x$, où $x \in E$ est l'unique antécédent de y par f. Alors $g : F \longrightarrow E$ définit bien une application de F dans E, la bijectivité assurant l'unicité de l'image.

Soit $y \in F$. Notons x l'unique élément de E tel que $y = f(x)$. Alors $g(y) = x$ et $(f \circ g)(y) = f(g(y))) = f(x) = y$. Donc $f \circ g = \mathrm{id}_F$.

Soit $x \in E$. Posons $y = f(x)$. Alors $g(y) = x$. Donc $(g \circ f)(x) = g(f(x)) = g(y) = x$. Donc $g \circ f = \mathrm{id}_E$.

L'application g convient donc.

◁ Réciproquement, supposons qu'il existe une application $g : F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.

De l'égalité $f \circ g = \mathrm{id}_F$, l'application id_F étant surjective, d'après la proposition 53, f est surjective.

De l'égalité $g \circ f = \mathrm{id}_E$, l'application id_E étant injective, d'après la proposition 46, f est injective.

Donc f est bijective.

• Montrons que l'application g est unique. Soit $h : F \longrightarrow E$ une autre application vérifiant $h \circ f = \mathrm{id}_E$ et $f \circ h = \mathrm{id}_F$. En particulier, $\mathrm{id}_F = f \circ g = f \circ h$. Donc pour tout $y \in F$, $f(g(y)) = f(h(y))$, et f étant bijective donc injective, $g(y) = h(y)$. Donc $g = h$. L'application g est donc unique. □

Il ne suffit pas que $g \circ f = \mathrm{id}_E$ ou que $f \circ g = \mathrm{id}_F$ pour que f soit bijective. Considérons par exemple les fonctions $f : \mathbb{N} \longrightarrow \mathbb{N}$ et $g : \mathbb{N} \longrightarrow \mathbb{N}$ définies, pour tout $n \in \mathbb{N}$, par $f(n) = n + 1$ et $g(n) = \max(0, n - 1)$. Alors $g \circ f = \mathrm{id}_{\mathbb{N}}$ mais f n'est pas surjective car 0 n'a pas d'antécédent par f. Notons que $f \circ g \neq \mathrm{id}_{\mathbb{N}}$ car $(f \circ g)(0) = 1 \neq 0$.

EXEMPLES 58

- *La fonction $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+ \ ; \ x \longmapsto x^2$ et la fonction $g : \mathbb{R}_+ \longrightarrow \mathbb{R}_+ \ ; \ x \longmapsto \sqrt{x}$ sont bijectives et sont des bijections réciproques l'une de l'autre : pour tout $x \in \mathbb{R}_+$,*

$$(g \circ f)(x) = \sqrt{x^2} = x \quad \text{et} \quad (f \circ g)(x) = \left(\sqrt{x}\right)^2 = x.$$

- *La fonction $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ et la fonction $\ln : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ sont bijectives et sont des bijections réciproques l'une de l'autre :*

$$\forall x \in \mathbb{R}_+^*, \ \exp(\ln(x)) \quad \text{et} \quad \forall x \in \mathbb{R}, \ \ln(\exp(x)) = x.$$

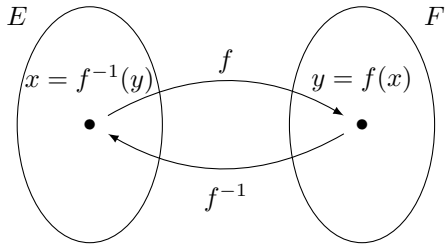
- *L'application $\mathrm{id}_E : E \longrightarrow E$ est bijective, de bijection réciproque $\mathrm{id}_E^{-1} = \mathrm{id}_E$:*

$$\mathrm{id}_E \circ \mathrm{id}_E = \mathrm{id}_E.$$

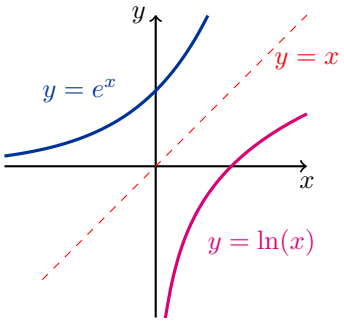
Si f est bijective, la bijection réciproque est l'application qui à un élément y de F associe l'unique antécédent de y par f dans E, noté x :

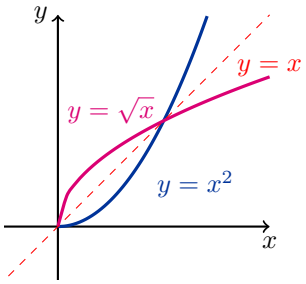
$$\begin{array}{rccl} f^{-1}: & F & \longrightarrow & E \\ & y & \longmapsto & x \text{ tel que } y = f(x) \end{array}.$$

Si f est bijective : $y = f(x) \Leftrightarrow x = f^{-1}(y)$



Dans le cas d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$, cela signifie que les graphes de f et f^{-1} sont symétriques l'un de l'autre par rapport à la droite d'équation $y = x$.





Méthode 59 — *Pour déterminer si une application est bijective,*

- *soit on donne directement l'expression d'une fonction g telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$, et dans ce cas, f est bijective, de bijection réciproque $f^{-1} = g$,*
- *soit on résout, pour tout $y \in F$, l'équation $y = f(x)$ d'inconnue x. Si, pour tout $y \in F$, cette équation admet une unique solution x, alors f est bijective et on a également obtenu l'expression de f^{-1},*
- *soit on montre que f est injective et surjective à l'aide des caractérisations, mais dans ce cas on n'a pas l'expression explicite f^{-1}.*

Exemple 60 — *Montrons que l'application* $\mathrm{sh} : \mathbb{R} \longrightarrow \mathbb{R}\ ;\ x \longmapsto \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}$ *est bijective et déterminons sa bijection réciproque.*

Soit $y \in \mathbb{R}$. Résolvons l'équation $y = \mathrm{sh}(x)$ d'inconnue $x \in \mathbb{R}$. Pour tout $x \in \mathbb{R}$,

$y = \mathrm{sh}(x) = \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}$ *si et seulement si* $(\mathrm{e}^x)^2 - 2y\mathrm{e}^x - 1 = 0$, *soit encore si et seulement si* e^x *est une racine strictement positive de* $X^2 - 2yX - 1$, *soit encore si et seulement si* $\mathrm{e}^x = y + \sqrt{y^2+1}$.

Donc, pour tout $x \in \mathbb{R}$, $y = \mathrm{sh}(x)$ si et seulement si $x = \ln(y + \sqrt{y^2+1})$.

Ainsi, pour tout $y \in \mathbb{R}$, l'équation $y = \mathrm{sh}(x)$ admet une unique solution x sur $\mathbb{R}$, $x = \ln(y + \sqrt{y^2+1})$.

La fonction sh *est donc bijective, de bijection réciproque* $\mathrm{sh}^{-1} : \mathbb{R} \longrightarrow \mathbb{R}\ ;\ y \longmapsto \ln\left(y + \sqrt{y^2+1}\right)$.

PROPOSITION 61
Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

- *Si f est bijective alors f^{-1} est bijective et $\left(f^{-1}\right)^{-1} = f$.*
- *Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Preuve —
- Si f est bijective alors d'après la proposition 57, $f \circ f^{-1} = \mathrm{id}_F$ et $f^{-1} \circ f = \mathrm{id}_E$ et donc f^{-1} est bijective par la même proposition 57 et $\left(f^{-1}\right)^{-1} = f$.
- Supposons f et g bijectives.
  Alors $(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) = g \circ \left(f \circ f^{-1}\right) \circ g^{-1} = g \circ \mathrm{id}_F \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_G$
  et $\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) = f^{-1} \circ \left(g^{-1} \circ g\right) \circ f = f^{-1} \circ \mathrm{id}_E \circ f = f^{-1} \circ f = \mathrm{id}_E$.
  Cela montre que $g \circ f$ est bijective de bijection réciproque $f^{-1} \circ g^{-1}$.

□

REMARQUE 62 — *Soient $f : E \longrightarrow F$ une application et B une partie de F.*

Si f est bijective, l'image réciproque de B par f, que l'on a notée précédemment $f^{-1}(B)$, est exactement l'image directe de B par f^{-1}, qui se note également $f^{-1}(B)$. Il n'y a donc pas d'ambiguïté sur la notation lorsque f est bijective.

***Preuve** — En effet, supposons f bijective et utilisons provisoirement la notation $f^{\leftarrow}(B)$ pour désigner l'image réciproque de B par f.*

Soit $x \in F$. $x \in f^{\leftarrow}(B) \Leftrightarrow f(x) \in B \Leftrightarrow \exists y \in B \mid f(x) = y \Leftrightarrow \exists y \in B \mid x = f^{-1}(y) \Leftrightarrow x \in f^{-1}(B)$

Donc $f^{\leftarrow}(B) = f^{-1}(B)$. □

Mais on rappelle que la notation $f^{-1}(B)$ ne suppose pas f bijective.

Si f n'est pas bijective, f n'admet pas bijection réciproque f^{-1}. L'ensemble $f^{-1}(B)$ ne peut donc en aucun cas désigner l'image directe de B par f^{-1} (puisqu'elle n'existe pas !)

On retiendra que $f^{-1}(\{y\})$ existe toujours, que f soit bijective ou non, contrairement à $f^{-1}(y)$ qui n'est défini que si f est bijective.

PROPOSITION 63
Si $f : E \longrightarrow F$ est une application injective alors l'application induite de E sur $\mathrm{Im}(f)$ est bijective.

En particulier, si I est un intervalle de $\mathbb{R}$ et $f : I \longrightarrow \mathbb{R}$ est une application continue strictement monotone, alors f induit une bijection de I sur l'intervalle $f(I)$.

EXEMPLE 64 — *La fonction $\cos : [0, \pi] \longrightarrow \mathbb{R}$ est continue strictement décroissante. Elle induit donc une bijection de $[0, \pi]$ sur $\cos([0, \pi]) = [-1, 1]$.*

DÉFINITION 65
L'ensemble des applications bijectives de E sur E est noté $S(E)$ et s'appelle l'ensemble des permutations de E. Lorsque $E = \{1, \ldots, n\}$ où $n \in \mathbb{N}^*$, on note alors plus simplement S_n.

DÉFINITION 66
*On appelle **involution** toute application $f : E \longrightarrow E$ telle que $f \circ f = \mathrm{id}_E$. Une telle application est bijective, de bijection réciproque $f^{-1} = f$.*

EXEMPLES 67
- *La fonction $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$; $x \longmapsto \dfrac{1}{x}$ est une involution et est donc bijective, de bijection réciproque elle-même.*
- *L'application $f : \mathcal{P}(E) \longrightarrow \mathcal{P}(E)$; $A \longmapsto \complement_E A$ est une involution et est donc bijective, de bijection réciproque elle-même.*

Chapitre 3 Relations binaires

Nous allons étudier dans ce chapitre des relations liant deux éléments d'un même ensemble. Souvent, nous cherchons à comparer des éléments ou à expliquer ce qui les rapproche ou les distingue. Par exemple, on peut comparer l'âge de deux individus, ou dire s'ils habitent dans le même pays, etc. Nous allons définir proprement la notion de relation en mathématiques.

3.1 Premières définitions

Définition 1
Soient E et F deux ensembles. On appelle ***relation binaire*** \关系\ *entre E et F tout triplet $\mathcal{R} = (E, F, G)$ où G est une partie de $E \times F$. Si $(x, y) \in G$, on note $x\mathcal{R}y$ et on dit que x* ***est en relation avec*** *y. On parle de la relation $\mathcal{R}$.*

On a donc $G = \{(x, y) \in E \times F \mid x\mathcal{R}y\}$.

 L'ordre dans un couple importe donc on peut avoir $x\mathcal{R}y$ mais pas $y\mathcal{R}x$.

Remarque 2 — *Les applications de E dans F sont des cas particuliers de relations binaires : pour tout $(x, y) \in E \times F$, $x\mathcal{R}y$ si $y = f(x)$.*

Dans la suite du cours, nous nous intéresserons plus particulièrement aux relations binaires de E sur lui-même, qui sont les relations les plus utiles en mathématiques. Lorsque $E = F$, la relation $\mathcal{R}$ de E sur lui-même est appelée **relation binaire sur** E.

Une relation $\mathcal{R}$ est souvent notée par un symbole $\equiv$, $\leq$, $\sim$, $\subset$...

Exemples 3 *Donnons quelques exemples de relations binaires d'un ensemble sur lui-même :*

- *la relation d'égalité $=$ sur E,*
- *les relations d'inégalité $\leq$, $<$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$,*
- *la relation d'inclusion $\subset$ sur $\mathcal{P}(E)$,*
- *la relation $\leq$ sur l'espace des fonctions de E dans $\mathbb{R}$, définie par $f \leq g$ si pour tout $x \in E$, $f(x) \leq g(x)$,*
- *la relation de divisibilité $\mid$ sur $\mathbb{Z}$, définie par $m \mid n$ s'il existe $k \in \mathbb{Z}$ tel que $n = mk$.*
- *pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$, notée $\equiv \mod n$, définie par $a \equiv b \mod n$ s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.*
- *pour tout $\alpha \in \mathbb{R}$, la relation de congruence modulo α sur $\mathbb{R}$, notée $\equiv \mod \alpha$, définie par $a \equiv b \mod \alpha$ s'il existe $k \in \mathbb{Z}$ tel que $a = b + k\alpha$.*
- *la relation « avoir le même signe » sur $\mathbb{R}^*$.*

Une relation binaire peut satisfaire certaines propriétés.

Définition 4
Soit E un ensemble. Soit $\mathcal{R}$ une relation binaire sur E.

- *$\mathcal{R}$ est dite* ***réflexive*** \自反性\ *si, pour tout $x \in E$, $x\mathcal{R}x$,*
- *$\mathcal{R}$ est dite* ***symétrique*** \对称性\ *si, pour tout $(x, y) \in E^2$, si $x\mathcal{R}y$ alors $y\mathcal{R}x$,*
- *$\mathcal{R}$ est dite* ***antisymétrique*** \反对称性\ *si, pour tout $(x, y) \in E^2$, si $x\mathcal{R}y$ et $y\mathcal{R}x$ alors $x = y$,*
- *$\mathcal{R}$ est dite* ***transitive*** \传递性\ *si, pour tout $(x, y, z) \in E^3$, si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.*

Exemples 5

- *La relation d'égalité $=$ sur E est réflexive, symétrique, antisymétrique et transitive. On notera qu'une relation peut donc être symétrique et antisymétrique.*
- *La relation $\leq$ sur $\mathbb{R}$ est réflexive, antisymétrique et transitive. Elle n'est pas symétrique car par exemple $2 \leq 3$ mais $3 \not\leq 2$.*
- *La relation $<$ sur $\mathbb{R}$ est symétrique et transitive. Elle n'est ni réflexive, ni antisymétrique. Par exemple, $1 \not< 1$.*
- *La relation de divisibilité sur $\mathbb{Z}$ est réflexive et transitive. Elle n'est ni symétrique, ni antisymétrique. En effet, on a $1|2$ mais $2 \nmid 1$, et $1|-1$ et $-1|1$ mais $1 \neq -1$.*
- *La relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ est réflexive, antisymétrique et transitive. Elle n'est pas symétrique car par exemple $\{1\} \subset \{1,2\}$ mais $\{1,2\} \not\subset \{1\}$.*
- *La relation « avoir le même signe » sur $\mathbb{R}^*$ est réflexive, symétrique et transitive. Elle n'est pas antisymétrique car par exemple, $1\mathcal{R}2$ et $2\mathcal{R}1$ mais $1 \neq 2$.*

3.2 Relations d'équivalence

Nous définissons dans cette partie un premier type de relation, celle d'équivalence. Une telle relation permet d'identifier sous une même étiquette les éléments qui sont en relation et de ne plus les distinguer. Par exemple, on identifie les individus à leur nationalité.

3.2.1 Définition et exemples

Définition 6
Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est une ***relation d'équivalence*** \等价关系\ *sur E si $\mathcal{R}$ est réflexive, symétrique et transitive.*

Une relation d'équivalence est souvent notée $\equiv$, ou $\sim$, ...

Exemples 7

- *La relation d'égalité $=$ sur E est une relation d'équivalence.*
- *La relation « avoir le même signe » sur $\mathbb{R}^*$ est une relation d'équivalence.*
- *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$ est une relation d'équivalence.*
  Preuve — *Soit $n \in \mathbb{N}$.*
  - ***Réflexivité :*** *Soit $p \in \mathbb{Z}$. On a $p = p + 0 \times n$ et $0 \in \mathbb{Z}$ donc $p \equiv p \bmod n$. Donc la relation de congruence modulo n est réflexive.*
  - ***Symétrie :*** *Soit $(p,q) \in \mathbb{Z}^2$. Supposons que $p \equiv q \bmod n$. Alors il existe $k \in \mathbb{Z}$ tel que $p = q + kn$. Donc $q = p - kn = p + (-k)n$ et $-k \in \mathbb{Z}$. Donc $q \equiv p \bmod n$. Donc la relation de congruence modulo n est symétrique.*
  - ***Transitivité :*** *Soit $(p,q,r) \in \mathbb{Z}^3$. Supposons que $p \equiv q \bmod n$ et $q \equiv r \bmod n$. Montrons que $p \equiv r \bmod n$. Il existe $k_1 \in \mathbb{Z}$ tel que $p = q + k_1 n$ et il existe $k_2 \in \mathbb{Z}$ tel que $q = r + k_2 n$. Donc $p = r + k_2 n + k_1 n = r + (k_1 + k_2)n$ et $(k_1 + k_2) \in \mathbb{Z}$. Donc $p \equiv r \bmod n$. Donc la relation de congruence modulo n est transitive.*

  De ces trois points, il vient que la relation de congruence modulo n est une relation d'équivalence. □
- *Pour tout $\alpha \in \mathbb{R}$, la relation de congruence modulo α sur $\mathbb{R}$ est une relation d'équivalence.*
  Preuve — *Analogue à la preuve précédente.* □
- *Si $(A_i)_{i \in I}$ est une partition de E, la relation d'appartenance au même sous-ensemble A_i est une relation d'équivalence.*

Remarque 8 — *Les écritures $x\mathcal{R}y$ et $y\mathcal{R}x$ sont équivalentes car $\mathcal{R}$ est symétrique.*

3.2.2 Classes d'équivalence et ensemble quotient

Définition 9
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Soit x un élément de E. On appelle ***classe d'équivalence*** *de x \x的等价类\ pour la relation $\mathcal{R}$ (ou plus simplement classe de x), notée $\mathrm{Cl}(x)$ ou $\overline{x}$, l'ensemble des éléments y de E qui sont en relation avec x :*

$$\mathrm{Cl}(x) = \{y \in E \mid x\mathcal{R}y\}\,.$$

Exemples 10

- *La classe d'équivalence de 1 pour la relation d'équivalence « avoir le même signe » sur $\mathbb{R}^*$ est l'ensemble des nombres réels non nuls de même signe que 1, c'est-à-dire l'ensemble des nombres réels strictement positifs :* $\mathrm{Cl}(1) = \mathbb{R}_+^*$.
- *Soit $n \in \mathbb{N}$. Soit $r \in \mathbb{Z}$. La classe d'équivalence de r pour la relation de congruence modulo n dans $\mathbb{Z}$ est*

$$\begin{aligned}\mathrm{Cl}(r) &= \{p \in \mathbb{Z} \mid p \equiv r \bmod n\}\\ &= \{p \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, p = r + kn\}\\ &= \{r + kn \mid k \in \mathbb{Z}\}\\ &= n\mathbb{Z} + r\end{aligned}$$

Proposition 11
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Pour tout $(x, y) \in E^2$, $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ si et seulement si $x\mathcal{R}y$.

Preuve — Soit $(x, y) \in E^2$.

▷ Supposons que $\mathrm{Cl}(x) = \mathrm{Cl}(y)$. Comme $\mathcal{R}$ est réflexive, on a $y\mathcal{R}y$ donc $y \in \mathrm{Cl}(y)$. Or, par hypothèse, $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, donc $y \in \mathrm{Cl}(x)$. Donc par définition d'une classe d'équivalence, $x\mathcal{R}y$.

◁ Supposons que $x\mathcal{R}y$. Soit $z \in \mathrm{Cl}(x)$. Alors $x\mathcal{R}z$. Comme $x\mathcal{R}y$, on a, par symétrie de $\mathcal{R}$, $y\mathcal{R}x$. Donc par transitivité de $\mathcal{R}$, comme $y\mathcal{R}x$ et $x\mathcal{R}z$, on a $y\mathcal{R}z$. Donc $z \in \mathrm{Cl}(y)$. D'où $\mathrm{Cl}(x) \subset \mathrm{Cl}(y)$. Par symétrie des rôles de x et y, on a de la même manière $\mathrm{Cl}(y) \subset \mathrm{Cl}(x)$. Finalement, $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.

□

Notons donc que si $y \in \mathrm{Cl}(x)$ alors $\mathrm{Cl}(y) = \mathrm{Cl}(x)$.

Définition 12
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Soit C une classe d'équivalence. On appelle ***représentant*** *de la classe d'équivalence C tout élément x de C.*

Exemple 13 — *Nous avons vu que $\mathbb{R}_+^*$ est une classe d'équivalence (celle de 1) pour la relation d'équivalence « avoir le même signe » sur $\mathbb{R}^*$. Tout élément de $\mathbb{R}_+^*$ est un représentant de cette classe. Des représentants de cette classe sont donc par exemple 1, ou π, ou $\sqrt{2}$... Ainsi, $\mathbb{R}_+^* = \mathrm{Cl}(1) = \mathrm{Cl}(\pi) = \mathrm{Cl}(\sqrt{2})$...*

Proposition 14
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence de E forme une partition de E, c'est-à-dire :

- *Elles sont non vides,*
- *Elle sont deux à deux disjointes,*
- *Leur réunion est égale à E.*

Preuve —

- Une classe d'équivalence C est toujours la classe d'équivalence d'un élément x de E : $C = \mathrm{Cl}(x)$. Comme $x \in \mathrm{Cl}(x)$ puisque $x\mathcal{R}x$ par réflexivité de $\mathcal{R}$, on a $x \in C$ et C est non vide.

- Soient C_1 et C_2 deux classes d'équivalence. Supposons $C_1 \cap C_2 \neq \emptyset$. Soient x_1 un représentant de C_1 et x_2 un représentant de C_2. Ainsi, $C_1 = \mathrm{Cl}(x_1)$ et $C_2 = \mathrm{Cl}(x_2)$. Par hypothèse, il existe $x \in C_1 \cap C_2$. En particulier, $x \in C_1$ donc $x \mathcal{R} x_1$ et $x \in C_2$ donc $x \mathcal{R} x_2$. Par symétrie et transitivité de $\mathcal{R}$, $x_1 \mathcal{R} x_2$. Donc d'après la proposition précédente, $\mathrm{Cl}(x_1) = \mathrm{Cl}(x_2)$, soit $C_1 = C_2$. Ainsi, deux classes sont soit égales soit disjointes.
- Soit $x \in E$. Alors $x \in \mathrm{Cl}(x)$ donc x appartient à la réunion des classes d'équivalence. Donc E est inclus dans la réunion des classes d'équivalence. L'inclusion réciproque étant évidente puisque une classe d'équivalence est une partie de E, la réunion est égale à E.

De ces trois points, il vient que l'ensemble des classes d'équivalence de E forme une partition de E. □

Exemples 15

- *La relation « avoir le même signe » sur $\mathbb{R}^*$ a exactement deux classes d'équivalence : $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$. Ces deux classes d'équivalence forment bien une partition de $\mathbb{R}^*$.*

  Preuve *— Soit C une classe d'équivalence et considérons x un représentant de C. Si x est positif, alors $C = \mathrm{Cl}(x) = \mathbb{R}_+^*$. Si x est négatif, alors $C = \mathrm{Cl}(x) = \mathbb{R}_-^*$. Les classes $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$ sont bien sûr distinctes.* □
- *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$ possède exactement n classes d'équivalence : les ensembles $n\mathbb{Z} + r = \{nk + r \mid k \in \mathbb{Z}\}$ avec $r \in \{0, \ldots, n-1\}$. On les note souvent $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$. On a choisi comme représentant des différentes classes les entiers 0, 1, …, $n-1$.*

  Preuve *— Soit C une classe d'équivalence et considérons p un représentant de C. Comme $p \in \mathbb{Z}$, on peut effectuer la division euclidienne de p par n. Il existe donc $k \in \mathbb{Z}$ et $r \in \{0, \ldots, n-1\}$ tel que $p = kn + r$. Donc $p \equiv r \bmod n$. Donc $C = \mathrm{Cl}(r) = n\mathbb{Z} + r$. De plus, les n classes d'équivalence $n\mathbb{Z} + r$ où $r \in \{0, \ldots, n-1\}$ deux à deux disjointes car si r_1 et r_2 sont deux éléments distincts de $\{0, \ldots, n-1\}$ alors r_1 n'est pas congru à r_2 modulo n.* □

Définition 16
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence de E pour la relation $\mathcal{R}$ s'appelle ***l'ensemble quotient de E par $\mathcal{R}$****. On le note $E/\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$.*

Exemples 17

- *L'ensemble quotient de $\mathbb{R}^*$ par la relation « avoir le même signe » est l'ensemble $\{\mathbb{R}_-^*, \mathbb{R}_+^*\}$.*
- *Soit $n \in \mathbb{Z}$. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est l'ensemble $\{n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+n-1\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. On note cet ensemble $\mathbb{Z}/n\mathbb{Z}$.*

3.3 Relations d'ordre et ensembles ordonnés

Nous définissons dans cette dernière partie la notion de relation d'ordre. Une telle relation permet intuitivement de hiérarchiser, d'ordonner les éléments. Cela généralise l'ordre naturel sur les nombres.

3.3.1 Définitions et exemples

Définition 18
Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est une ***relation d'ordre*** *\偏序\ sur E si $\mathcal{R}$ est réflexive, antisymétrique et transitive. Dans ce cas, on dit que $(E, \mathcal{R})$ est un* ***ensemble ordonné****.*

Remarques 19 *Une relation d'ordre est souvent notée $\preccurlyeq$, ou $\leq$,…. Les écritures $x \preccurlyeq y$ et $y \succcurlyeq x$ sont équivalentes.*

Souvent, $x \preccurlyeq y$ se lit « x plus petit que y » mais cela n'est qu'une convention.

La notation $x \preccurlyeq y \preccurlyeq z$ signifie $x \preccurlyeq y$ et $y \preccurlyeq z$.

Exemples 20

- *La relation $\leq$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$ est une relation d'ordre.*
- *La relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ est une relation d'ordre.*

- *La relation $\leq$ sur l'espace des fonctions de E dans $\mathbb{R}$ est une relation d'ordre.*
- *La relation $<$ n'est pas une relation d'ordre sur $\mathbb{R}$ car elle n'est pas réflexive. En effet, $1 \not< 1$.*
- *La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre.*
  ***Preuve** —*
  - ***Réflexivité :** Pour tout $n \in \mathbb{N}$, on a $n = n \times 1$ donc $n|n$. Donc la relation de divisibilité sur $\mathbb{N}$ est réflexive.*
  - ***Antisymétrie :** Soit $(p, q) \in \mathbb{N}^2$. Supposons que $p|q$ et $q|p$. Alors il existe $k_1 \in \mathbb{N}$ tel que $p = k_1 \times q$ et il existe $k_2 \in \mathbb{N}$ tel que $q = k_2 \times p$. Donc $p = k_1 \times k_2 \times p$. Donc $p(1 - k_1 k_2) = 0$.*
    Si $p = 0$ alors $q = k_2 \times p = k_2 \times 0 = 0$ donc $p = q = 0$.
    Sinon, $k_1 k_2 = 1$ et comme k_1 et k_2 sont des entiers naturels, on a $k_1 = k_2 = 1$. Donc $p = k_1 \times q = q$. Donc la relation de divisibilité sur $\mathbb{N}$ est antisymétrique.
  - ***Transitivité :** Soit $(m, n, p) \in \mathbb{N}^3$ tel que $m|n$ et $n|p$. Montrons que $m|p$. Il existe $k_1 \in \mathbb{N}$ tel que $n = k_1 \times n$ et il existe $k_2 \in \mathbb{N}$ tel que $p = k_2 \times n$. Donc $p = k_2 \times k_1 \times m$ et $k_1 \times k_2 \in \mathbb{N}$. Donc $m|p$. Donc la relation de divisibilité sur $\mathbb{N}$ est transitive.*

  De ces trois points, il vient que la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre. □
- *Mais la relation de divisibilité sur $\mathbb{Z}$ n'est pas une relation d'ordre car elle n'est pas antisymétrique.*

Dans $\mathbb{R}$ muni de l'ordre usuel $\leq$, on peut comparer deux à deux tous les éléments (on a toujours $x \leq y$ ou $y \leq x$), mais ce n'est pas toujours le cas, par exemple pour l'inclusion sur $\mathcal{P}(E)$. Nous introduisons donc la définition suivante.

Définition 21
Soit $(E, \preccurlyeq)$ un ensemble ordonné.

- *On dit que l'ordre $\preccurlyeq$ est **total** \全序\ si, pour tout $(x, y) \in E^2$, on a $x \preccurlyeq y$ ou $y \preccurlyeq x$. L'ensemble $(E, \preccurlyeq)$ est alors appelé **ensemble totalement ordonné**.*
- *Sinon, on dit que l'ordre est **partiel** et l'ensemble $(E, \preccurlyeq)$ est appelé **ensemble partiellement ordonné**.*

Lorsque $x \preccurlyeq y$ ou $y \preccurlyeq x$, on dit que les éléments x et y sont **comparables**.

Exemples 22

- *L'ensemble $(\mathbb{R}, \leq)$ est un ensemble totalement ordonné.*
- *Si E contient plus de deux éléments, l'ensemble $(\mathcal{P}(E), \subset)$ est un ensemble partiellement ordonné. En effet, si a et b sont des éléments distincts de E, alors on a $\{a\} \not\subset \{b\}$ et $\{b\} \not\subset \{a\}$.*
- *La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre partiel. Par exemple, $2 \nmid 3$ et $3 \nmid 2$.*

Définition 23
*Soit $(E, \preccurlyeq)$ un ensemble ordonné. La relation $\prec$ sur E associée à $\preccurlyeq$, appelée **relation d'ordre strict** associée à $\preccurlyeq$, est définie, pour tout $(x, y) \in E^2$, par $x \prec y$ si, par définition, $x \preccurlyeq y$ et $x \neq y$.*

Proposition 24
Soit $(E, \preccurlyeq)$ un ensemble ordonné. La relation d'ordre strict $\prec$ est antisymétrique et transitive.

Preuve —

- **Antisymétrie :** Soit $(x, y) \in E^2$. Supposons que $x \prec y$ et $y \prec x$. Alors $x \preccurlyeq y$ et $y \preccurlyeq x$, donc par antisymétrie de $\preccurlyeq$, $x = y$. Donc $\prec$ est antisymétrique.
- **Transitivité :** Soit $(x, y, z) \in E^3$. Supposons que $x \prec y$ et $y \prec z$. Alors $x \preccurlyeq y$ et $y \preccurlyeq z$ donc $x \preccurlyeq z$. Il reste à montrer que $x \neq z$. Supposons par l'absurde que $x = z$. Alors $x \preccurlyeq y$ et comme $y \preccurlyeq z$, on a aussi $y \preccurlyeq x$. Donc par antisymétrie de $\preccurlyeq$, on a $x = y$, contredisant $x \prec y$. Donc $x \neq z$. D'où $x \prec z$. Donc $\prec$ est transitive.

□

Exemple 25 — *La relation $<$ sur $\mathbb{R}$ est la relation d'ordre strict de $\leq$.*


La négation de $x \preccurlyeq y$ est, x et y ne sont pas comparables ou x et y sont comparables et $y \prec x$.

3.3.2 Majorant et minorant

Définition 26
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- *Soit $M \in E$. On dit que M est un **majorant** \上界\ de A si, pour tout $a \in A$, $a \preccurlyeq M$.*
- *Soit $m \in E$. On dit que m est un **minorant** \下界\ de A si, pour tout $a \in A$, $m \preccurlyeq a$.*

Exemples 27

- *Dans $(\mathbb{R}, \leq)$, l'ensemble $\mathbb{R}_-$ est l'ensemble des minorants de $\mathbb{R}_+$. $\mathbb{R}_+$ n'admet pas de majorant.*
  ***Preuve** — En effet, supposons que M soit un majorant de $\mathbb{R}_+$. Alors, comme $M+1 \in \mathbb{R}_+$, on a $M+1 \leq M$, ce qui est absurde.* □
- *Pour la relation d'inclusion, $\emptyset$ est un minorant de $\mathcal{P}(E)$ et E est un majorant de $\mathcal{P}(E)$.*
- *Pour la relation de divisibilité sur $\mathbb{N}$, l'ensemble $\{1, 2\}$ est l'ensemble des minorants de l'ensemble $\{4, 6\}$ et l'ensemble des multiples de 12 est l'ensemble des majorants.*
  ***Preuve** —*
  - *Soit m un minorant de $\{4, 6\}$. Alors $m|4$ et $m|6$ donc $m|6-4=2$. Donc $m=1$ ou $m=2$. 1 et 2 divisent évidemment 4 et 6. Donc l'ensemble des minorants est $\{1, 2\}$.*
  - *Soit M un majorant de $\{4, 6\}$. Alors $4|M$ et $6|M$ donc $12 = \text{ppcm}(4, 6)|M$. Donc M est un multiple de 12. 4 et 6 divisent évidemment tout multiple de 12. Donc l'ensemble des majorants est $\{12n \mid n \in \mathbb{N}^*\}$.*

  □

Remarque 28 — *Un majorant ou un minorant, s'ils existent, ne sont pas nécessairement uniques comme on vient de le voir.*

Définition 29

- *On dit que A est une partie **majorée** si A admet au moins un majorant M. Autrement dit, A est majorée s'il existe $M \in E$ tel que pour tout $a \in A$, $a \preccurlyeq M$.*
  On dit aussi que M majore A ou que A est majorée par M.
- *On dit que A est une partie **minorée** si A admet au moins un minorant m. Autrement dit, A est minorée s'il existe $m \in E$ tel que pour tout $a \in A$, $m \preccurlyeq a$.*
  On dit aussi que m minore A ou que A est minorée par m.
- *On dit que A est **bornée** si A est majorée et minorée. Autrement dit, A est bornée s'il existe $(m, M) \in E^2$ tel que pour tout $a \in A$, $m \preccurlyeq a \preccurlyeq M$.*

Exemples 30

- *Pour la relation $\leq$ sur $\mathbb{R}$, $\mathbb{R}_+$ est une partie minorée, par exemple par 0. $\mathbb{R}_+$ n'est pas majorée car elle n'admet pas de majorant.*
- *Pour la relation d'inclusion, $\mathcal{P}(E)$ est minorée (par $\emptyset$) et majorée (par E). $\mathcal{P}(E)$ est donc une partie bornée pour l'inclusion.*
- *Pour la relation de divisibilité sur $\mathbb{N}$, l'ensemble $\{4, 6\}$ est minoré, par exemple par 2, et majoré, par exemple par 12. C'est donc une partie bornée pour la relation de divisibilité.*

3.3.3 Maximum et minimum

Définition 31
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- *On dit que A admet un **maximum** \最大値\ s'il existe $M \in A$ tel que pour tout $a \in A$, $a \preccurlyeq M$.*
- *On dit que A admet un **minimum** \最小値\ s'il existe $m \in A$ tel que pour tout $a \in A$, $m \preccurlyeq a$.*

Remarque 32 — *Un maximum (resp. minimum) de A est donc un majorant (resp. minorant) de A qui appartient à A.*

PROPOSITION 33

- *Si A admet un maximum alors celui-ci est unique, et est noté* $\max(A)$.
- *Si A admet un minimum alors celui-ci est unique, et est noté* $\min(A)$.

Preuve —

- Supposons que A admette deux maximums M_1 et M_2. Montrons que $M_1 = M_2$. Par définition du maximum, M_1 et M_2 sont des éléments de A et sont des majorants de A. Comme M_1 est un majorant de A et $M_2 \in A$, on a $M_2 \preccurlyeq M_1$. De même, M_2 étant un majorant de A et $M_1 \in A$, on a $M_1 \preccurlyeq M_2$. Donc par antisymétrie de $\preccurlyeq$, on en déduit que $M_1 = M_2$. Donc, si A admet un maximum alors celui-ci est unique.
- La preuve est analogue au cas précédent.

□

REMARQUE 34 — *S'ils existent, on peut donc parler* DU *maximum et* DU *minimum, mais on parle toujours d'*UN *majorant et d'*UN *minorant.*

EXEMPLES 35

- 0 *est le minimum de* $\mathbb{R}_+$. $\mathbb{R}_+$ *n'admet pas de maximum.*
- $\emptyset$ *est le minimum de* $\mathcal{P}(E)$ *et* E *le maximum pour la relation d'inclusion.*
- *Dans* $(\mathbb{N}, |\ )$, *l'ensemble* $\{4, 6\}$ *n'admet pas de minimum ni de maximum. En effet, aucun des minorants* $\{1, 2\}$ *et aucun des majorants* $\{12n \mid n \in \mathbb{N}^*\}$ *n'appartient à* $\{4, 6\}$.
- *Dans* $(\mathbb{R}, \leq)$, *soit* $I = [0, 1[$. *Le minimum de* I *est* 0 *et* I *n'admet pas de maximum.*

  Preuve — *Supposons que I admette un maximum M. Alors $M \in [0, 1[$ donc $M < 1$. Posons $M' = \dfrac{M+1}{2}$. Alors $M' \in [0, 1[$ et $M < M'$, contredisant la maximalité de M. Donc I n'admet pas de maximum.* □
- *Dans* $(\mathbb{R}, \leq)$, *soit* $A = \left\{ \dfrac{1}{n} \mid n \in \mathbb{N}^* \right\}$. *Le maximum de A est 1 et A n'admet pas de minimum.*

  Preuve —

  – *On a* $1 = \dfrac{1}{1}$ *donc* $1 \in A$ *et pour tout* $n \in \mathbb{N}^*$, $\dfrac{1}{n} \leq 1$ *donc A admet un maximum et* $\max(A) = 1$.

  – *Supposons que A admette un minimum m. Alors $m \in A$ et il existe $n_0 \in \mathbb{N}^*$ tel que $m = \dfrac{1}{n_0}$. m étant un minorant, pour tout $n \in \mathbb{N}^*$, $m \leq \dfrac{1}{n}$. En particulier, pour $n = n_0 + 1$, on a $\dfrac{1}{n_0} \leq \dfrac{1}{n_0+1}$, ce qui est absurde. Donc A n'admet pas de minimum.*

  □

Citons trois propriétés fondamentales de $\mathbb{N}$.

PROPOSITION 36
Dans l'ensemble ordonné $(\mathbb{N}, \leq)$,

- *Toute partie non vide de* $\mathbb{N}$ *admet un minimum,*
- *Toute partie non vide majorée de* $\mathbb{N}$ *admet un maximum,*
- $\mathbb{N}$ *n'a pas de maximum.*

3.3.4 Borne supérieure et borne inférieure

§ *1. Cas général*

DÉFINITION 37
Soient $(E, \preccurlyeq)$ *un ensemble ordonné et A une partie de E.*

- *On appelle* ***borne supérieure*** \上確界\ *de A, si elle existe, le plus petit des majorants de A. On la note alors* $\sup(A)$.
- *On appelle* ***borne inférieure*** \下確界\ *de A, si elle existe, le plus grand des minorants de A. On la note alors* $\inf(A)$.

Remarque 38 — *La borne supérieure (resp. inférieure) n'existe pas nécessairement mais, si elle existe, elle est unique par unicité du minimum des majorants de A (resp. maximum des minorants).*

Méthode 39 — *Pour démontrer que A admet une borne supérieure (resp. inférieure) égale à M (resp. m),*

1. *on commence par montrer que M (resp. m) est un majorant (resp. minorant) de A : pour tout $a \in A$, $a \preccurlyeq M$ (resp. $m \preccurlyeq a$),*
2. *puis on montre que tout majorant (resp. minorant) de A est supérieur (resp. inférieur) à M (resp. m) : en considérant un majorant M' (resp. un minorant m'), on montre que $M \preccurlyeq M'$ (resp. $m' \preccurlyeq m$).*

On montre ainsi que M est le plus petit des majorants (resp. m est le plus grand des minorants).

 La différence entre $\max(A)$ et $\sup(A)$ est que $\max(A)$ est un élément de A alors que $\sup(A)$ n'est pas nécessairement un élément de A.

On dispose tout de même du résultat suivant.

Proposition 40
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- *Si A possède un maximum alors A possède une borne supérieure et* $\max(A) = \sup(A)$.
- *Si A possède un minimum alors A possède une borne inférieure et* $\min(A) = \inf(A)$.

Preuve —

- Supposons que A possède un maximum M. Alors M est un majorant de A. De plus, comme $M \in A$, pour tout majorant M' de A, on a $M \preccurlyeq M'$.
  Donc M est le plus petit des majorants. Donc A admet une borne supérieure et $M = \sup(A)$.
- Preuve analogue à la précédente.

□

Exemples 41

- *0 est le minimum donc la borne inférieure de $\mathbb{R}_+$. $\mathbb{R}_+$ n'admet pas de borne supérieure car $\mathbb{R}_+$ n'est pas majoré.*
- *Pour la relation d'inclusion sur $\mathcal{P}(E)$, $\emptyset$ est le minimum donc la borne inférieure de $\mathcal{P}(E)$, E est le maximum donc la borne supérieure de $\mathcal{P}(E)$.*
- *Pour la relation de divisibilité, la borne inférieure de $\{4, 6\}$ est 2 et la borne supérieure est 12.*
  ***Preuve** — Nous avons vu que l'ensemble des minorants est $\{1, 2\}$. Donc le plus grand des minorants existe et vaut 2. Donc $\sup(\{4, 6\}) = 2$. L'ensemble des majorants est $\{12n \mid n \in \mathbb{N}^*\}$. Donc le plus petit des majorants existe et vaut 12. Donc $\inf(\{4, 6\}) = 12$.* □
- *Dans $(\mathbb{R}, \leq)$, $[0, 1[$ n'admet pas de maximum mais admet une borne supérieure égale à 1. Sa borne inférieure est égale à son minimum, 0.*
  ***Preuve** — Nous avons déjà vu que $[0, 1[$ n'admet pas de maximum.*
  Montrons que $[0, 1[$ admet une borne supérieure égale à 1.
  Pour tout $x \in [0, 1[$, on a $x \leq 1$. Donc 1 majore $[0, 1[$.
  Montrons que 1 est le plus petit des majorants. Soit M un majorant de $[0, 1[$. Pour tout $n \in \mathbb{N}^*$, $1 - \frac{1}{n} \in [0, 1[$, donc $1 - \frac{1}{n} \leq M$. En laissant tendre n vers $+\infty$, on en déduit que $1 \leq M$.
  Donc 1 est le plus petit des majorants de $[0, 1[$ et $\sup(A) = 1$. □
- *Dans $(\mathbb{R}, \leq)$, l'ensemble $A = \left\{\frac{1}{n} \mid n \in \mathbb{N}^*\right\}$ n'admet pas de minimum mais admet une borne inférieure égale à 0. Sa borne supérieure est égale à son maximum, 1.*
  ***Preuve** — Nous avons déjà vu que A n'admet pas de minimum.*
  Montrons que A admet une borne inférieure égale à 0.
  Pour tout $n \in \mathbb{N}^*$, $0 \leq \frac{1}{n}$. Donc 0 est un minorant de A.
  Montrons que 0 est le plus grand des minorants. Soit m un minorant de A. Comme m minore A, pour tout $n \in \mathbb{N}^*$, on a $m \leq \frac{1}{n}$. En laissant tendre n vers $+\infty$, on obtient $m \leq 0$.
  Donc 0 est le plus grand des minorants de A et $\inf(A) = 0$. □

D'après les deux derniers exemples, une partie A peut donc admettre une borne supérieure (resp. inférieure) sans admettre de maximum (resp. minimum).

§ *2. Cas particulier de l'ensemble ordonné* $(\mathbb{R}, \leq)$

Citons deux propriétés fondamentales de $\mathbb{R}$. On admet ces propriétés qui découlent de la construction de $\mathbb{R}$. La démonstration de nombreux théorèmes d'analyse repose sur ces propriétés.

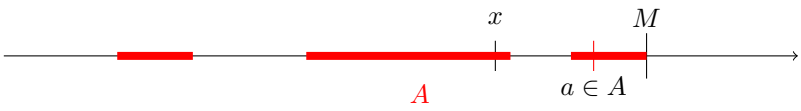
PROPOSITION 42 (Propriété de la borne supérieure/inférieure)
Dans l'ensemble ordonné $(\mathbb{R}, \leq)$,

- *Toute partie non vide majorée admet une borne supérieure,*
- *Toute partie non vide minorée admet une borne inférieure.*

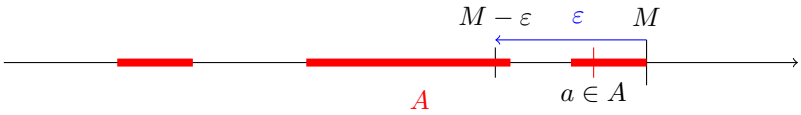
REMARQUE 43 — *La propriété de la borne supérieure est un résultat d'existence, elle ne donne pas la valeur de cette borne supérieure. Dans certains cas, on a une idée de la borne supérieure, par exemple, on a vu que* $\sup([0,1[) = 1$, *et on le démontre en revenant à la définition de la borne supérieure. Dans d'autres cas, on ne connaît pas cette valeur mais cette propriété permet de justifier que la borne supérieure existe.*

PROPOSITION 44 (Caractérisation de la borne supérieure)
Soit A *une partie non vide majorée de* $\mathbb{R}$. *Soit* $M \in \mathbb{R}$.

Alors $M = \sup(A)$ *si et seulement si* $\begin{cases} 1.\ M \text{ majore } A \\ 2.\ \text{pour tout } x \in \mathbb{R} \text{ tel que } x < M, \text{ il existe } a \in A \text{ tel que } x < a \leq M. \end{cases}$

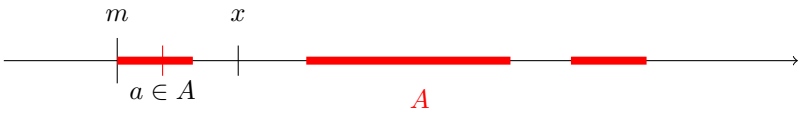


soit encore, si et seulement si $\begin{cases} 1.\ M \text{ majore } A, \\ 2.\ \text{pour tout } \varepsilon > 0, \text{ il existe } a \in A \text{ tel que } M - \varepsilon < a \leq M. \end{cases}$

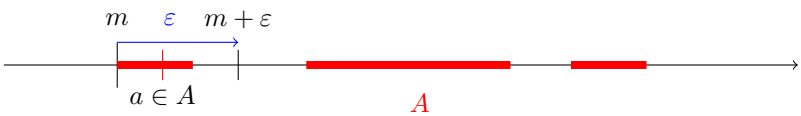


PROPOSITION 45 (Caractérisation de la borne inférieure)
Soit A *une partie non vide minorée de* $\mathbb{R}$. *Soit* $m \in \mathbb{R}$.

Alors $m = \inf(A)$ *si et seulement si* $\begin{cases} 1.\ m \text{ minore } A \\ 2.\ \text{pour tout } x \in \mathbb{R} \text{ tel que } x > m, \text{ il existe } a \in A \text{ tel que } m \leq a < x. \end{cases}$



soit encore, si et seulement si $\begin{cases} 1.\ m \text{ minore } A, \\ 2.\ \text{pour tout } \varepsilon > 0, \text{ il existe } a \in A \text{ tel que } m \leq a < m + \varepsilon. \end{cases}$



EXEMPLE 46 — *Retrouvons la valeur de la borne inférieure de l'exemple* $A = \left\{ \frac{1}{n} \mid n \in \mathbb{N}^* \right\}$.

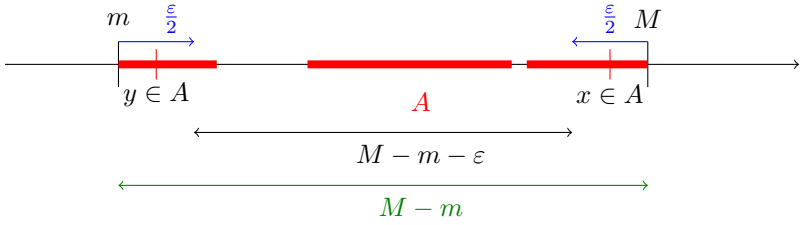
1.. 0 *minore* A.

2. *Soit* $\varepsilon > 0$. *Comme* $\lim_{n\to+\infty} \frac{1}{n} = 0$, *il existe* $n_0 \in \mathbb{N}^*$ *tel que* $0 < \frac{1}{n_0} \leq \varepsilon$ *et* $\frac{1}{n_0} \in A$.

Donc par la caractérisation de la borne supérieure, $\inf(A) = 0$.

EXEMPLE 47 — *Soit* A *une partie non vide bornée de* $\mathbb{R}$. *Posons* $E = \left\{ |x-y| \mid (x,y) \in A^2 \right\}$. E *est donc l'ensemble des distances entre deux points de* A.

- A *étant non vide, on peut trouver un élément* $x \in A$. *Alors, comme* $(x,x) \in A^2$, $|x-x| = 0 \in E$. *Donc* E *est une partie non vide de* $\mathbb{R}$.
- A *étant bornée, il existe* $b \in \mathbb{R}$ *tel que pour tout* $x \in A$, $|x| \leq b$.
  Soit $(x,y) \in A^2$. *Par inégalité triangulaire, on a* $|x-y| \leq |x| + |y| \leq b + b = 2b$. *Donc* E *est majoré par* $2b$.
- E *étant une partie non vide et majorée de* $\mathbb{R}$, E *admet donc une borne supérieure, que l'on note* δ.
- *Déterminons* δ.
  A *étant non vide et bornée,* A *est en particulier non vide et minorée, donc* $m = \inf(A)$ *existe. De même,* A *est en particulier non vide et majorée, donc* $M = \sup(A)$ *existe.*
  Montrons que $\delta = M - m$.



1. *Pour tout* $(x,y) \in A^2$, $m \leq x \leq M$ *et* $m \leq y \leq M$. *Donc* $-(M-m) \leq x - y \leq M - m$, *soit* $|x-y| \leq M - m$.
Donc $M - m$ *majore* E.
2. *Soit* $\varepsilon > 0$. *D'après la caractérisation de la borne supérieure (en prenant* $\varepsilon' = \frac{\varepsilon}{2}$*), il existe* $x \in A$ *tel* $M - \frac{\varepsilon}{2} < x \leq M$.
D'après la caractérisation de la borne inférieure (en prenant $\varepsilon' = \frac{\varepsilon}{2}$*), il existe* $y \in A$ *tel que* $m \leq y < m + \frac{\varepsilon}{2}$.
Alors $M - m - \varepsilon < x - y \leq |x-y|$.
En posant $d = |x-y|$, *on a donc* $d \in E$ *et* $M - m - \varepsilon < d \leq M - m$.
Donc d'après la caractérisation de la borne supérieure, $\delta = M - m = \sup(A) - \inf(A)$.

PROPOSITION 48
Soient a *et* b *deux nombres réels.*

- *Si, pour tout* $\varepsilon > 0$, $a \geq b - \varepsilon$ *alors* $a \geq b$.
- *Si, pour tout* $\varepsilon > 0$, $a \leq b + \varepsilon$ *alors* $a \leq b$.

Preuve — Traitons le premier point, le deuxième point se traitant de manière analogue. Supposons que pour tout $\varepsilon > 0$, $a \geq b - \varepsilon$. Posons $B = \left\{ b - \varepsilon \mid \varepsilon \in \mathbb{R}_+^* \right\}$. On a $\sup(B) = b$ d'après la caractérisation de la borne supérieure et, par hypothèse, a est un majorant de B. La borne supérieure étant le plus petit des majorants, on en déduit que $b \leq a$. D'où le résultat. □

PROPOSITION 49 (Caractérisation séquentielle)
Soit A une partie non vide de $\mathbb{R}$. Soit $(m, M) \in \mathbb{R}^2$.

• *Supposons A est majorée.*

Alors $M = \sup(A)$ *si et seulement si* $\begin{cases} 1.\ M \text{ majore } A \\ 2.\ \text{il existe une suite } (a_n)_{n\in\mathbb{N}} \text{ d'éléments de } A \text{ qui converge vers } M. \end{cases}$

• *Supposons A minorée.*

Alors $m = \inf(A)$ *si et seulement si* $\begin{cases} 1.\ m \text{ minore } A \\ 2.\ \text{il existe une suite } (a_n)_{n\in\mathbb{N}} \text{ d'éléments de } A \text{ qui converge vers } m. \end{cases}$

Preuve — Traitons le cas de la borne supérieure. A étant une partie non vide majorée de $\mathbb{R}$, A admet une borne supérieure.

• Supposons que $M = \sup(A)$.

Alors, par définition de la borne supérieure, M majore A. D'où le premier point.

Construisons une suite d'éléments de A qui converge vers M. Pour tout $n \in \mathbb{N}$, on va utiliser la caractérisation de la borne supérieure avec $\varepsilon = \dfrac{1}{n+1} > 0$. Pour tout $n \in \mathbb{N}$, il existe $a_n \in A$ tel que $M - \dfrac{1}{n+1} < a_n \leq M$. La suite $(a_n)_{n\in\mathbb{N}}$ est donc une suite d'éléments de A. De plus, en laissant tendre n vers $+\infty$, on en déduit que $M \leq \lim\limits_{n\to+\infty} a_n \leq M$, soit $\lim\limits_{n\to+\infty} a_n = M$. On a donc construit une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers M.

• Réciproquement, soit $M \in \mathbb{R}$. Supposons que M majore A et qu'il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers M. Utilisons la caractérisation de la borne supérieure.

1. Par hypothèse, M majore de A.

2. Soit $\varepsilon > 0$. Comme $\lim\limits_{n\to+\infty} a_n = M$, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $a_n > M - \varepsilon$. En particulier, on a $a_{n_0} \in A$ et $M - \varepsilon < a_{n_0} \leq M$.

Donc, par la caractérisation de la borne supérieure, $M = \sup(A)$.

□

EXEMPLE 50 — *Retrouvons la valeur de borne inférieure de l'exemple* $A = \left\{ \dfrac{1}{n} \mid n \in \mathbb{N}^* \right\}$.

1. *A est minoré par* 0.

2. *Posons, pour tout $n \in \mathbb{N}^*$, $u_n = \dfrac{1}{n}$. Pour tout $n \in \mathbb{N}^*$, $u_n \in A$ et $u_n \to 0$ lorsque n tend vers $+\infty$. La suite $(u_n)_{n\in\mathbb{N}^*}$ d'éléments de A converge donc vers* 0.

Donc, d'après la caractérisation séquentielle de la borne supérieure, $\inf(A) = 0$.

EXEMPLE 51 — *Soit* $B = \left\{ \dfrac{q}{2^p + q} \mid (p, q) \in \mathbb{N}^{*2} \right\}$.

• *Remarquons que B est non vide et pour tout $(p, q) \in \mathbb{N}^{*2}$, $\dfrac{q}{2^p+q} \leq 1$ donc B est majoré par* 1. *B étant une partie de $\mathbb{R}$ non vide majorée, B admet une borne supérieure.*

1. 1 *majore B.*

2. *Posons, pour tout $n \in \mathbb{N}^*$, $u_n = \dfrac{n}{2+n}$. Alors, pour tout $n \in \mathbb{N}^*$, $u_n \in B$ et $(u_n)_{n\in\mathbb{N}^*}$ converge vers* 1.

Donc, par la caractérisation séquentielle de la borne supérieure $\sup(B) = 1$.

• *Remarquons que B est non vide et pour tout $(p, q) \in \mathbb{N}^{*2}$, $0 \leq \dfrac{q}{2^p+q}$ donc B est minoré par* 0. *B étant une partie de $\mathbb{R}$ non vide minorée, B admet une borne inférieure.*

1. 0 *minore B.*

2. *Posons, pour tout $n \in \mathbb{N}^*$, $v_n = \dfrac{1}{2^n+1}$. Alors, pour tout $n \in \mathbb{N}^*$, $v_n \in B$ et $(v_n)_{n\in\mathbb{N}^*}$ converge vers* 0.

Donc, d'après la caractérisation séquentielle de la borne inférieure, $\inf(B) = 0$.

Chapitre 4 Arithmétique dans $\mathbb{Z}$

4.1 Divisibilité dans $\mathbb{Z}$

4.1.1 Définitions et premières propriétés

Définition 1
*Soit $(a,b) \in \mathbb{Z}^2$. On dit que a **divise** b \整除\ s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$. On note $a \mid b$.*

*On dit aussi que a est un **diviseur** de b, ou que b est **divisible** par a, ou que b est un **multiple** de a.*

Exemples 2

- *2 divise 6 mais 2 ne divise pas 7.*
- *Soit $a \in \mathbb{Z}$. Alors 1, -1, a et $-a$ divisent a.*

Remarques 3

- *Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est l'ensemble*

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\} = \{\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots\}.$$

  Rappelons que pour tout $a \in \mathbb{Z}$, $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (voir cours de Géométrie 1). Plus précisément, les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.
- *Si un entier a divise un entier b alors l'ensemble des multiples de b est inclus dans l'ensemble des multiples de a :*

$$a \mid b \quad \Leftrightarrow \quad b\mathbb{Z} \subset a\mathbb{Z}.$$

  ***Preuve** — Supposons que $a \mid b$. Soit $m \in b\mathbb{Z}$. Alors il existe $p \in \mathbb{Z}$ tel que $m = pb$. Comme $a \mid b$, il existe $k \in \mathbb{Z}$ tel que $b = ka$. Donc $m = pka \in a\mathbb{Z}$ car $pk \in \mathbb{Z}$. Donc $b\mathbb{Z} \subset a\mathbb{Z}$.*
  Supposons $b\mathbb{Z} \subset a\mathbb{Z}$. Comme $b = 1 \times b \in b\mathbb{Z}$, $b \in a\mathbb{Z}$ donc il existe $k \in \mathbb{Z}$ tel que $b = ka$. Donc a divise b.
  D'où le résultat. □

Proposition 4
Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Si a divise b alors $|a| \leq |b|$.

Preuve — Supposons que a divise b. Alors il existe $k \in \mathbb{Z}$ tel que $b = ka$. Comme b est non nul, k l'est également et $|k| \geq 1$. Donc $|b| = |ka| \geq |a|$. □

Proposition 5 *Soient a, b, c et d des éléments de $\mathbb{Z}$.*

- *La relation de divisibilité est une relation d'ordre partiel sur $\mathbb{N}$ mais n'est pas une relation d'ordre sur $\mathbb{Z}$ (non antisymétrique) :*

$$a \mid b \text{ et } b \mid a \quad \Leftrightarrow \quad a\mathbb{Z} = b\mathbb{Z} \quad \Leftrightarrow \quad |a| = |b| \quad \Leftrightarrow \quad a = b \text{ ou } a = -b.$$

  La transitivité s'écrit : Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
- *Si $d \mid a$ et $d \mid b$ alors pour tout $(u,v) \in \mathbb{Z}^2$, $d \mid (au + bv)$.*
- *Si $a \mid b$ et $c \mid d$ alors $ac \mid bd$. En particulier, si $a \mid b$ alors pour tout $n \in \mathbb{N}$, $a^n \mid b^n$.*
- *Si $ab \mid c$ alors $a \mid c$ et $b \mid c$.*

Preuve —

- Nous avons vu au chapitre 3 que la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre partiel. Nous avons également vu que la relation de divisibilité sur $\mathbb{Z}$ est réflexive et transitive mais n'est pas antisymétrique car $1 \mid -1$ et $-1 \mid 1$ mais $1 \neq -1$.
  Si b est nul alors a est nul puisque b divise a. De même, si a est nul alors b est nul. Supposons donc a et b non nuls.
  On a $a \mid b$ et $b \mid a$ si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$ et $a\mathbb{Z} \subset b\mathbb{Z}$, soit si et seulement si $a\mathbb{Z} = b\mathbb{Z}$.
  On a $a \mid b$ et $b \mid a$ si et seulement si $|a| \leq |b|$ et $|b| \leq |a|$, soit si et seulement si $|a| = |b|$.

- Supposons que $d \mid a$ et $d \mid b$. Alors il existe $k_1 \in \mathbb{Z}$ tel que $a = k_1 d$ et il existe $k_2 \in \mathbb{Z}$ tel que $b = k_2 d$. Donc $au + bv = d(uk_1 + vk_2)$ et $uk_1 + vk_2 \in \mathbb{Z}$.
  Donc $d \mid au + bv$.
- Supposons que $a \mid b$ et $c \mid d$. Alors il existe $k_1 \in \mathbb{Z}$ tel que $b = ak_1$ et il existe $k_2 \in \mathbb{Z}$ tel que $d = ck_2$. Donc $bd = ack_1k_2$ et $k_1k_2 \in \mathbb{Z}$. Donc $ac \mid bd$.

□

Remarque 6 — *La réciproque de la dernière proposition est fausse :* $4 \mid 12$ *et* $6 \mid 12$ *mais* $4 \times 6 = 24$ *ne divise pas* 12.

Exemple 7 — *Déterminons les entiers naturels* n *tels que* $2n + 3$ *divise* $3n + 7$.

Soit $n \in \mathbb{N}$. *Supposons que* $2 + 3n \mid 3n + 7$. *Alors* $2n + 3 \mid 2n + 3$ *et* $2n + 3 \mid 3n + 7$. *Donc*

$$2 + 3n \mid 2(3n + 7) - 3(2n + 3) = 5.$$

Donc, comme $n \in \mathbb{N}$, *on a* $2n + 3 \in \mathbb{N}^*$ *et* $2n + 3$ *divise* 5. *Or, les diviseurs positifs de* 5 *sont* 1 *et* 5. *Donc* $2n + 3 = 1$ *ou* $2n + 3 = 5$, *soit* $n = -1$ *ou* $n = 1$. *Comme* n *est positif, on en déduit que* $n = 1$.

Réciproquement, si $n = 1$ *alors* $2n + 3 = 5$ *et* $3n + 7 = 10$, *et donc* $2n + 3 \mid 3n + 7$.

Il existe donc un unique entier naturel, $n = 1$, *tel que* $2n + 3$ *divise* $3n + 7$.

4.1.2 Division euclidienne

Théorème 8
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. *Il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *tel que*

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

L'entier q *est appelé le* ***quotient*** \商\ *et l'entier* r *est appelé le* ***reste*** \余数\ *de la division euclidienne de* a *par* b \整数的带余除法（或欧几里德除法）\.

Preuve —

- Existence : Posons $q = \mathrm{E}\left(\frac{a}{b}\right)$ et $r = a - qb$. Alors $(q, r) \in \mathbb{Z} \times \mathbb{N}$ et $a = bq + r$. De plus, comme $q = \mathrm{E}\left(\frac{a}{b}\right)$, on a $q \leq \frac{a}{b} < q + 1$, donc, b étant strictement positif, $bq \leq a < bq + b$. Donc $0 \leq r = a - bq < b$. Ainsi, le couple (q, r) convient.
- Unicité : Soient (q_1, r_1) et (q_2, r_2) deux couples vérifiant l'énoncé. Alors $a = bq_1 + r_1$ et $a = bq_2 + r_2$, donc $bq_1 + r_1 = bq_2 + r_2$. Donc $b(q_1 - q_2) = r_2 - r_1$.
  Comme $|r_2 - r_1| < b$, on en déduit que $b|q_1 - q_2| < b$. Donc $|q_1 - q_2| < 1$. Comme $q_1 - q_2 \in \mathbb{Z}$, on obtient $q_1 - q_2 = 0$, soit $q_1 = q2$, et donc $r_1 = r_2$.

□

Remarque 9 — *On a donc montré en particulier que* $q = \mathrm{E}\left(\frac{a}{b}\right)$

Exemples 10

- *On a* $22 = 3 \times 6 + 4$ *et* $0 \leq 4 < 6$, *donc le quotient de la division euclidienne de* 22 *par* 6 *est* 3 *et le reste est* 4.
  Les relations $22 = 2 \times 6 + 10$ *ou* $22 = 4 \times 6 - 2$ *ne vérifient pas les relations imposées sur le reste* r.
- *On a* $-12 = -3 \times 5 + 3$ *et* $0 \leq 3 < 5$, *donc le quotient de la division euclidienne de* -12 *par* 3 *est* -3 *et le reste est* 3.

Proposition 11
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. *Alors* b *divise* a *si et seulement si le reste de la division euclidienne de* a *par* b *est nul.*

Preuve —

- Supposons que b divise a. Alors il existe $k \in \mathbb{Z}$ tel que $a = kb$. Donc $a = kb + 0$ et par unicité de la division euclidienne, le reste de la division euclidienne de a par b vaut 0.
- Supposons que le reste de la division euclidienne de a par b soit nul. Alors il existe $q \in \mathbb{Z}$ tel que $a = qb + 0$, soit $a = qb$. Donc b divise a.

□

4.1.3 Relation de congruence modulo un entier

Définition 12
*Soient a, b et $n \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n si n divise $b-a$, soit encore, s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. On note alors $a \equiv b \bmod n$.*

Exemple 13 — $11 \equiv 1 \bmod 5$, $-1 \equiv 2 \bmod 3$, $0 \equiv 100 \bmod 2$.

Remarque 14 — $n \mid a \Leftrightarrow a \equiv 0 \bmod n$.

La proposition suivante a déjà été vue dans le chapitre 3.

Proposition 15
La relation de congruence est une relation d'équivalence.

En particulier, la relation étant symétrique, on a $a \equiv b \bmod n$ si et seulement si $b \equiv a \bmod n$. On peut donc dire que des entiers sont congrus modulo n.

Proposition 16 (Opérations sur les congruences)
Soit $a, b, c, d, m, n \in \mathbb{Z}$.

1. *$a \equiv b \bmod n$ si et seulement si $a + c \equiv b + c \bmod n$.*
2. *Si $a \equiv b \bmod n$ et $c \equiv d \bmod n$ alors $a + c \equiv b + d \bmod n$.*
3. *Si $a \equiv b \bmod n$ alors $ac \equiv bc \bmod n$.*
4. *Si $a \equiv b \bmod n$ et $c \equiv d \bmod n$ alors $ac \equiv bd \bmod n$.*
   En particulier, si $a \equiv b \bmod n$ alors pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \bmod n$.
5. *Si m est non nul, alors $a \equiv b \bmod n$ si et seulement si $ma \equiv mb \bmod mn$.*

Preuve —

1. On a $a \equiv b \bmod n$ si et seulement si n divise $b - a = (b + c) - (a + c)$, soit si et seulement si $a + c \equiv b + c \bmod n$.
2. Supposons $a \equiv b \bmod n$ et $c \equiv d \bmod n$. D'après le point précédent, $a + c \equiv b + c \bmod n$ et $b + c \equiv b + d \bmod n$. Donc, par transitivité, $a + c \equiv b + d \bmod n$.
3. Supposons $a \equiv b \bmod n$. Alors n divise $b - a$, donc n divise $c(b - a) = bc - ac$. Donc $ac \equiv bc \bmod n$.
4. Supposons $a \equiv b \bmod n$ et $c \equiv d \bmod n$. D'après le point précédent, $ac \equiv bc \bmod n$ et $bc \equiv bd \bmod n$. Donc, par transitivité, $ac \equiv bd \bmod n$.
5. Supposons que $a \equiv b \bmod n$. Alors il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Donc $mb = ma + k(mn)$ et $ma \equiv mb \bmod mn$. Réciproquement, supposons que $ma \equiv mb \bmod mn$. Alors il existe $k \in \mathbb{Z}$ tel que $mb = ma + kmn$. m étant non nul, par division par m, on obtient $b = a + kn$, donc $a \equiv b \bmod n$.

□

Exemples 17

- $2^{518} + 8^{211}$ *est divisible par* 3.
  ***Preuve** — En effet, on a $2 \equiv -1 \bmod 3$, donc $2^{518} \equiv (-1)^{518} \equiv 1 \bmod 3$ et $8 \equiv -1 \bmod 3$ donc $8^{211} \equiv (-1)^{211} \equiv -1 \bmod 3$ donc*
  $$2^{518} + 8^{211} \equiv 1 - 1 \equiv 0 \bmod 3.$$
  Donc 3 divise $2^{518} + 8^{211}$. □
- *Déterminons les entiers n tels que $3n + 5 \equiv 4 \bmod 7$.*
  Soit $n \in \mathbb{Z}$. Alors
  $$3n + 5 \equiv 4 \bmod 7 \Leftrightarrow 3n \equiv -1 \bmod 7 \Leftrightarrow 5 \times 3n \equiv -1 \times 5 \bmod 7 \Leftrightarrow n \equiv 2 \bmod 7.$$
  Donc l'ensemble des entiers tels que $3n + 5 \equiv 4 \bmod 7$ est l'ensemble $\{2 + 7k \mid k \in \mathbb{Z}\} = 2 + 7\mathbb{Z}$.
- *Pour tout entier $n \in \mathbb{Z}$ impair, 8 divise $n^2 - 1$.*
  ***Preuve** — En effet, soit n un entier impair. Il existe donc $k \in \mathbb{Z}$ tel que $n = 2k+1$. Alors $n^2 - 1 = 4k^2 + 4k = 4k(k+1)$. Or k et $k+1$ étant deux entiers successifs, l'un d'entre eux est pair et donc $k(k+1)$ est pair. Donc $k(k+1) \equiv 0 \bmod 2$. Donc $4k(k+1) \equiv 0 \bmod 8$. Donc $n^2 - 1 \equiv 0 \bmod 8$. D'où le résultat.* □

D'après le théorème de division euclidienne dans $\mathbb{Z}$, pour tout $a \in \mathbb{Z}$, il existe un unique $r \in \{0, \dots, n-1\}$ tel que $a \equiv r \bmod n$. Dire que $a \equiv b \bmod n$ est donc équivalent à dire que a et b ont le même reste dans la division euclidienne par n.

La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ et la classe d'équivalence d'un élément $a \in \mathbb{Z}$ est notée $\overline{a}^n$ ou lorsqu'il n'y a pas d'ambiguïté, $\overline{a}$:

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

L'ensemble de toutes ces classes d'équivalence modulo n, appelé ensemble quotient, est noté $\mathbb{Z}/n\mathbb{Z}$.

Exemples 18
- *Dans* $\mathbb{Z}/3\mathbb{Z}$, *on a* $\overline{1} = 1 + 3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$ *et par exemple* $\overline{1} = \overline{7}$.
- *Dans* $\mathbb{Z}/7\mathbb{Z}$, *on a* $\overline{2} = \{\dots, -12, -5, 2, 9, 16, \dots\}$ *et par exemple* $\overline{-12} = \overline{2}$.

Proposition 19
Pour tout $n \in \mathbb{N}^*$, *on a* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ *et cet ensemble est constitué de* n *éléments distincts.*

Preuve — Cela découle du théorème de division euclidienne. □

Exemple 20 — $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

Rappelons (voir cours de Géométrie 1) que l'on définit une somme $\underset{n}{+}$ et un produit $\underset{n}{\times}$ dans $\mathbb{Z}/n\mathbb{Z}$ de la façon suivante : pour a et b éléments de $\mathbb{Z}/n\mathbb{Z}$, en notant $\overline{x}$ et $\overline{y}$ des représentants de a et b,

$$a \underset{n}{+} b = \overline{x + y} \quad \text{et} \quad a \underset{n}{\times} b = \overline{x \times y}.$$

Ces opérations sont bien définies car elles ne dépendent pas du choix des représentants d'après la proposition 16.

Exemple 21 — *Dans* $\mathbb{Z}/6\mathbb{Z}$, $\overline{4} + \overline{3} = \overline{7} = \overline{1}$ *et* $\overline{4} \times \overline{3} = \overline{12} = \overline{0}$.

Enfin, rappelons que $\left(\mathbb{Z}/n\mathbb{Z}, \underset{n}{+}\right)$ est un groupe.

4.2 PGCD, PPCM

4.2.1 Plus grand diviseur commun

Définition 22
Soient $a_1, \dots, a_n$ *des éléments de* $\mathbb{Z}$. *On appelle* ***diviseur commun*** \公约数组成的集合\ *de* $a_1, \dots, a_n$ *tout élément* $d \in \mathbb{Z}$ *tel que pour tout* $i \in \{1, \dots, n\}$, $d \mid a_i$.

Exemples 23
- 6 *est un diviseur commun de* 12 *et* 18.
- 3 *est un diviseur commun de* 9, 12 *et* 21.

Lemme 24
Soient a *et* b *deux éléments de* $\mathbb{Z}$. *L'ensemble* $a\mathbb{Z} + b\mathbb{Z} = \{ak_1 + bk_2 \mid (k_1, k_2) \in \mathbb{Z}^2\}$ *est un sous-groupe de* $(\mathbb{Z}, +)$.

Preuve — D'après la définition, $a\mathbb{Z} + b\mathbb{Z}$ est un sous-ensemble de $\mathbb{Z}$.

• $0 = 0 \times a + 0 \times b$ donc $0 \in a\mathbb{Z} + b\mathbb{Z}$.

• Soient $(x, y) \in (a\mathbb{Z} + b\mathbb{Z})^2$. Il existe k_1, k_2, k_3 et k_4 dans $\mathbb{Z}$ tels que $x = ak_1 + bk_2$ et $y = ak_3 + bk_4$.

Donc $x - y = ak_1 + bk_2 - (ak_3 + bk_4) = a(k_1 - k_3) + b(k_2 - k_4)$ et $k_1 - k_3 \in \mathbb{Z}$ et $k_2 - k_3 \in \mathbb{Z}$. Donc $x - y \in a\mathbb{Z} + b\mathbb{Z}$.

De ces deux points, il vient que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. □

DÉFINITION 25
Soient a et b des éléments de $\mathbb{Z}$. Il existe un unique élément $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Cet élément d est appelé le ***plus grand diviseur commun*** \最大公约数\ *de a et b, en abrégé* pgcd. *Il s'agit de l'unique générateur positif de $a\mathbb{Z} + b\mathbb{Z}$. On note $d = \text{pgcd}(a, b)$ ou encore $d = a \wedge b$.*

Preuve — D'après le lemme, $a\mathbb{Z} + d\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Or pour tout sous-groupe H de $(\mathbb{Z}, +)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. □

PROPOSITION 26
Soient a et b des éléments de $\mathbb{Z}$. Alors $d = \text{pgcd}(a, b)$ si et seulement si

1. *$d \mid a$ et $d \mid b$, (autrement dit, d est un diviseur commun à a et b),*
2. *Pour tout $d' \in \mathbb{Z}$, si $d' \mid a$ et $d' \mid b$ alors $d' \mid d$. (autrement dit, tout diviseur commun de a et b divise d).*

Preuve —

• Supposons que $d = \text{pgcd}(a, b)$. Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Comme $a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$, $a \in d\mathbb{Z}$ donc $d \mid a$. De même, $b \in d\mathbb{Z}$ et $d \mid b$. D'où le premier point.

Soit $d' \in \mathbb{Z}$ tel que $d' \mid a$ et $d' \mid b$. Alors $a\mathbb{Z} \subset d'\mathbb{Z}$ et $b\mathbb{Z} \subset d'\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} \subset d'\mathbb{Z}$. Donc $d\mathbb{Z} \subset d'\mathbb{Z}$ et $d' \mid d$. D'où le second point.

• Réciproquement, supposons 1 et 2. Montrons par double inclusion que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

▷ Comme $d \mid a$ et $d \mid b$, on a $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$.

◁ Soit $d' \in \mathbb{N}$ tel que $d'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Alors $a \in d'\mathbb{Z}$ donc $d' \mid a$ et $b \in d'\mathbb{Z}$ donc $d' \mid b$. Donc $d' \mid d$. Donc $d\mathbb{Z} \subset d'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Finalement, $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. □

REMARQUE 27 — *On peut également définir le pgcd d'une famille d'éléments $a_1, \ldots, a_n$ comme étant le générateur positif de $a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$, sous-groupe de $(\mathbb{Z}, +)$. On montre que ce sont des diviseurs communs de $a_1, \ldots, a_n$, multiples de tout autre diviseur commun.*

REMARQUE 28 — *Le pgcd de a et b est le plus grand diviseur commun pour la relation d'ordre $\leq$ sur $\mathbb{N}$. C'est aussi le plus grand diviseur commun pour la relation d'ordre de divisibilité sur $\mathbb{N}$.*

EXEMPLE 29 — $\text{pgcd}(12, 18) = 6$, $\text{pgcd}(10, 12, 18) = 2$.

PROPOSITION 30
Soient a et b des éléments de $\mathbb{Z}$. Notons $d = \text{pgcd}(a, b)$. Alors il existe deux éléments u_0 et v_0 de $\mathbb{Z}$ tels que

$$au_0 + bv_0 = d.$$

Preuve — Par définition, on a $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Donc $d \in a\mathbb{Z} + b\mathbb{Z}$. Il existe donc $(u_0, v_0) \in \mathbb{Z}^2$ tel que $d = au_0 + bv_0$. □

EXEMPLE 31 — *On a $\text{pgcd}(4, 6) = 2$ et $4 \times (-1) + 6 \times 1 = 2$ mais aussi $4 \times 2 + 6 \times (-1) = 2$.*

On voit donc que les entiers u et v ne sont pas uniques.

PROPOSITION 32
Soient a, b, c et k des éléments de $\mathbb{Z}$. On a

- $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$,
- $\text{pgcd}(a, 0) = |a|$,
- $\text{pgcd}(a, 1) = 1$,
- $\text{pgcd}(a, b) = \text{pgcd}(b, a)$,
- $\text{pgcd}(a, \text{pgcd}(b, c)) = \text{pgcd}(\text{pgcd}(a, b), c)$,
- $\text{pgcd}(ka, kb) = |k|\text{pgcd}(a, b)$.

Preuve — Ces propriétés découlent immédiatement de la définition du pgcd comme l'unique générateur positif de $a\mathbb{Z}+b\mathbb{Z}$.

1. $a\mathbb{Z}+b\mathbb{Z}=|a|\mathbb{Z}+|b|\mathbb{Z}$,
2. $a\mathbb{Z}+0\mathbb{Z}=a\mathbb{Z}$,
3. $a\mathbb{Z}+\mathbb{Z}=\mathbb{Z}$,
4. $d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}=b\mathbb{Z}+a\mathbb{Z}$,
5. $a\mathbb{Z}+(b\mathbb{Z}+c\mathbb{Z})=(a\mathbb{Z}+b\mathbb{Z})+c\mathbb{Z}$,
6. $ak\mathbb{Z}+bk\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$.

□

4.2.2 Calcul du PGCD avec l'algorithme d'Euclide

Le pgcd se calcule facilement de manière algorithmique. Il est basé sur le résultat suivant.

LEMME 33
Soient a et b deux éléments de $\mathbb{Z}$. Notons r le reste de la division euclidienne de a par b. Alors

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

Preuve — Par division euclidienne, il existe $q\in\mathbb{Z}$ tel que $a=bq+r$. On vérifie alors que $a\mathbb{Z}+b\mathbb{Z}=r\mathbb{Z}+b\mathbb{Z}$. Par définition du pgcd, on a donc $\text{pgcd}(a,b)=\text{pgcd}(b,r)$. □

L'algorithme d'Euclide permet de calculer le pgcd de deux entiers, il est basé sur des divisions euclidiennes successives. D'après le lemme, le pgcd est le dernier reste non nul obtenu.

PRINCIPE DE L'ALGORITHME D'EUCLIDE

Soient a et b deux entiers tels que $0\leq b\leq a$.

Si $b=0$ alors $\text{pgcd}(a,b)=a$ *et c'est terminé. On suppose donc b non nul.*

- Étape 1 : *On effectue la division euclidienne de a par b : $a=bq_0+r_0$ avec $0\leq r_0<b$.*
  D'après le lemme, $\text{pgcd}(a,b)=\text{pgcd}(b,r_0)$.
  Si $r_0=0$ alors $\text{pgcd}(a,b)=b$ *et c'est terminé.*
  Sinon, on passe à l'étape suivante.
- Étape 2 : *On effectue la division euclidienne de b par r_0 : $b=r_0q_1+r_1$ avec $0\leq r_1<r_0$.*
  D'après le lemme, $\text{pgcd}(a,b)=\text{pgcd}(b,r_0)=\text{pgcd}(r_0,r_1)$.
  Si $r_1=0$ alors $\text{pgcd}(r_0,r_1)=r_0$ *et donc* $\text{pgcd}(a,b)=r_0$ *et c'est terminé.*
  Sinon, on passe à l'étape suivante.
- Étape 3 : *On effectue la division euclidienne de r_0 par r_1 : $r_0=r_1q_2+r_2$ avec $0\leq r_2<r_1$.*
  D'après le lemme, $\text{pgcd}(a,b)=\text{pgcd}(r_0,r_1)=\text{pgcd}(r_1,r_2)$.
  Si $r_2=0$ alors $\text{pgcd}(r_1,r_2)=r_1$ *et donc* $\text{pgcd}(a,b)=r_1$ *et c'est terminé.*
  Sinon on passe à l'étape suite, etc.
- ...

La suite des restes obtenus est une suite strictement décroissante d'entiers positifs, il existe donc un élément $n_0\in\mathbb{N}$ tel que $r_{n_0}=0$. Alors, d'après le lemme, $\text{pgcd}(a,b)=\text{pgcd}(b,r_0)=\ldots=\text{pgcd}(r_{n_0-1},r_{n_0})=r_{n_0-1}$.

REMARQUE 34 — *On peut toujours se ramener au cas où $0\leq b\leq a$ en utilisant que* $\text{pgcd}(a,b)=\text{pgcd}(b,a)$ *et* $\text{pgcd}(a,b)=\text{pgcd}(|a|,|b|)$.

EXEMPLE 35 — *Calculons le pgcd de* 721 *et* 658 *à l'aide de l'algorithme d'Euclide.*

1. *Division euclidienne de* 721 *par* 658 *:* $721=658\times1+63$. *Le reste vaut* 63.
2. *Division euclidienne de* 658 *par* 63 *:* $658=63\times10+28$. *Le reste vaut* 28.
3. *Division euclidienne de* 63 *par* 28 *:* $63=28\times2+7$. *Le reste vaut* 7.
4. *Division euclidienne de* 28 *par* 7 *:* $28=7\times4+0$. *Le reste est nul !*

Le dernier reste non nul dans la suite des divisions euclidienne est donc 7. *Ainsi,* $\text{pgcd}(721,658)=7$.

4.2.3 Entiers premiers entre eux

§ *1. Définitions*

Définition 36
Soient a et b deux éléments de $\mathbb{Z}$. On dit que a et b sont ***premiers entre eux*** \互素\ *si* $\text{pgcd}(a,b)=1$.

Exemple 37 — *2 et 3 sont premiers entre eux. 9 et 16 sont premiers entre eux. 6 et 4 ne sont pas premiers entre eux.*

Si a ne divise pas b et b ne divise pas a, on ne peut pas dire que a et b sont premiers entre eux ! Par exemple, 6 ne divise pas 15 et 15 ne divise pas 6 mais $\text{pgcd}(6,15)=3$, donc 6 et 15 ne sont pas premiers entre eux.

Définition 38
Soient a_1, …, a_n des éléments de $\mathbb{Z}$. On dit que a_1, …, a_n sont ***premiers entre eux deux à deux*** *si pour tout i et tout j éléments distincts de $\{1,\dots,n\}$, a_i et a_j sont premiers entre eux.*

§ *2. Théorème de Bezout et théorème de Gauss*

Théorème 39 (Théorème de Bezout)
Soient a et b des éléments de $\mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe deux éléments u et v dans $\mathbb{Z}$ tels que

$$au+bv=1.$$

Preuve — Supposons a et b premiers entre eux. Alors $\text{pgcd}(a,b)=1$. D'après la proposition **??**, il existe donc u et v dans $\mathbb{Z}$ tels que $au+bv=1$.

Réciproquement, supposons qu'il existe u et v dans $\mathbb{Z}$ tels que $au+bv=1$. Alors $1\in a\mathbb{Z}+b\mathbb{Z}$ et donc $1\mathbb{Z}=\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}$. Comme $a\mathbb{Z}+b\mathbb{Z}\subset\mathbb{Z}$, on en déduit que $a\mathbb{Z}+b\mathbb{Z}=1\mathbb{Z}$. Donc $\text{pgcd}(a,b)=1$ et a et b sont premiers entre eux. □

Exemple 40 — *n et $n+1$ sont premiers entre eux car $(n+1)\times 1+n\times(-1)=1$.*

L'algorithme d'Euclide étendu permet d'obtenir les coefficients u et v, appelés **coefficients de Bezout**. Alors que l'algorithme d'Euclide s'intéresse uniquement aux restes successifs, l'algorithme d'Euclide étendu considère également les quotients successifs.

Principe : À l'aide de l'algorithme d'Euclide, on construit de proche en proche des éléments u_k et v_k de $\mathbb{Z}$ tels que, à chaque étape,

$$r_k=au_k+bv_k,$$

où les r_k sont les restes des divisions euclidiennes successives de l'algorithme d'Euclide.

Exemple 41 — *Expliquons sur un exemple, avec $a=1795$ et $b=343$.*

$$\begin{array}{rcrcrcrcl}
1795 &=& 1 &\times 1795 &+& 0 &\times 343 & & \\
343 &=& 0 &\times 1795 &+& 1 &\times 343 & & \\
80 &=& 1 &\times 1795 &+& (-5) &\times 343 & & 1795-5\times 343=80 \\
23 &=& -4 &\times 1795 &+& 21 &\times 343 & & 343-4\times 80=23 \\
11 &=& 13 &\times 1795 &+& (-68) &\times 343 & & 80-3\times 23=11 \\
1 &=& -30 &\times 1795 &+& 157 &\times 343 & & 23-2\times 11=1
\end{array}$$

On a donc $1=1795\times u+343\times v$ avec $u=-30$ et $v=157$. On en déduit également que $\text{pgcd}(1795,343)=1$.

Théorème 42 (Théorème de Gauss)
Soient a, b et c des éléments de $\mathbb{Z}$. Si a et b sont premiers entre eux et si $a\mid bc$ alors $a\mid c$.

Preuve — Supposons que a et b sont premiers entre eux et que $a \mid bc$. D'après le théorème de Bezout, il existe des éléments u et v dans $\mathbb{Z}$ tels que $au+bv=1$. Comme $a \mid bc$, il existe $k \in \mathbb{Z}$ tel que $bc=ak$. On a donc $c=auc+bvc=auc+avk=a(uc+vk)$. Donc $a \mid c$. □

Si a et b ne sont pas premiers entre eux, et même si $a \mid bc$ et a ne divise pas b, on ne peut pas dire que $a \mid c$! Par exemple, 8 divise 4×6 mais 8 ne divise ni 4 ni 6.

Exemple 43 — *Si* $4 \mid 3n$ *alors* $4 \mid n$ *car* 4 *et* 3 *sont premiers entre eux.*

§ *3. Conséquences*

Proposition 44
Soient a, b et c des éléments de $\mathbb{Z}$. Supposons a et b premiers entre eux. Si $a \mid c$ et $b \mid c$ alors $ab \mid c$.

Plus généralement, soient $a_1, \ldots, a_n$, c des éléments de $\mathbb{Z}$. Supposons que les a_i sont premiers entre eux deux à deux. Si, pour tout $i \in \{1, \ldots, n\}$ $a_i \mid c$ alors $a_1 \times a_2 \times \ldots a_n \mid c$.

Preuve — Supposons que $a \mid c$ et $b \mid c$ avec $\text{pgcd}(a,b)=1$. a et b étant premiers entre eux, d'après le théorème de Bezout, il existe des éléments u et v de $\mathbb{Z}$ tels que $au+bv=1$. Donc $c=auc+bvc$. Or $a \mid c$ donc $ab \mid bc$ et $b \mid c$ donc $ab \mid ac$. Donc ab divise $acu+bcv=c$.

La généralisation se montre alors par récurrence. □

Si a et b ne sont pas premiers entre eux, on ne peut rien dire ! Par exemple $4 \mid 4$ et $2 \mid 4$ mais $4 \times 2 = 8$ ne divise pas 4.

Exemple 45 — *Si* $4 \mid n$ *et* $3 \mid n$ *alors* $12 \mid n$ *car* 4 *et* 3 *sont premiers entre eux.*

Proposition 46
Soient a, b et c des éléments de $\mathbb{Z}$. Si a est premier avec b et si a est premier avec c alors a est premier avec bc.

Plus généralement, soient a, $b_1, \ldots, b_n$ des éléments de $\mathbb{Z}$. Si, pour tout $i \in \{1, \ldots, n\}$, a est premier avec b_i alors a est premier avec $b_1 \times b_2 \times \ldots \times b_n$.

De plus, si a est premier avec b alors, pour tout $(m,n) \in \mathbb{N}^2$, a^m est premier avec b^n.

Preuve — Supposons a premier avec b et avec c. D'après le théorème de Bezout, il existe u_1, u_2, v_1 et v_2 éléments de $\mathbb{Z}$ tels que $1=au_1+bv_1$ et $1=au_2+cv_2$. Par produit, on obtient

$$1 = a(au_1u_2 + u_1cv_2 + bv_1u_2) + bc(v_1v_2).$$

D'après le théorème de Bezout, a et bc sont donc premiers entre eux.

On peut démontrer la généralisation par récurrence.

□

Exemple 47 — *Soit $n \in \mathbb{N}^*$. n est premier avec $n-1$ et avec $n+1$ donc n est premier avec $(n-1)(n+1) = n^2-1$.*

Proposition 48
Soient a et b des éléments de $\mathbb{Z}$. Posons $d = \text{pgcd}(a,b)$. Alors il existe des éléments a' et b' de $\mathbb{Z}$ tels que

$$a = da', \quad b = db', \quad \text{et} \quad \text{pgcd}(a',b') = 1.$$

Preuve — Si $(a,b)=(0,0)$ alors $a'=b'=1$ conviennent.

Supposons $(a,b) \neq (0,0)$. Comme $d=\text{pgcd}(a,b)$, on sait que $d \mid a$ et $d \mid b$. Il existe donc $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$ tels que $a=da'$ et $b=db'$. On a alors $d=\text{pgcd}(a,b)=\text{pgcd}(da',db')=d\text{pgcd}(a',b')$. Donc, comme d est non nul, $\text{pgcd}(a',b')=1$. □

Proposition 49
Soit r un nombre rationnel. Alors il existe un unique couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ avec p et q premiers entre eux. L'écriture d'un rationnel sous cette forme est appelée ***forme irréductible****.*

Preuve — • Existence : Comme $r \in \mathbb{Q}$, il existe $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{a}{b}$. Posons $d = \text{pgcd}(a,b)$. Il existe donc $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $a = pd$, $b = qd$ et $\text{pgcd}(p,q) = 1$. On a donc $r = \frac{a}{b} = \frac{pd}{qd} = \frac{p}{q}$ et p et q sont premiers entre eux.

• Unicité : Supposons qu'il existe $(p_1,q_1) \in \mathbb{Z}\times\mathbb{N}^*$ et $(p_2,q_2) \in \mathbb{Z}\times\mathbb{N}^*$ tels que $r = \frac{p_1}{q_1} = \frac{p_2}{q_2}$ et $\text{pgcd}(p_1,q_1) = \text{pgcd}(p_2,q_2) = 1$. Alors $p_1q_2 = p_2q_1$. Donc $q_2 \mid p_2q_1$. Comme q_2 et p_2 sont premiers entre eux, donc d'après le théorème de Gauss, $q_2 \mid q_1$. Par symétrie des rôles de q_1 et q_2, on en déduit que $q_1 \mid q_2$. Donc $|q_1| = |q_2|$ et par positivité de q_1 et q_2, $q_1 = q_2$. Comme $p_1q_2 = p_2q_1$, on obtient également $p_1 = p_2$. □

4.2.4 Plus petit multiple commun

Définition 50
*Soient $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$. On appelle **multiple commun** de $a_1, \ldots, a_n$ tout élément m de $\mathbb{Z}$ tel que pour tout $i \in \{1,\ldots,n\}$, m est un multiple de a_i (ou encore, $a_i \mid m$).*

Exemples 51

- 12 *est un multiple commun à* 4 *et à* 6.
- 36 *est un multiple commun à* 2, 3 *et* 9.

Lemme 52
Soient a et b deux éléments de $\mathbb{Z}$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

Preuve — L'intersection de deux sous-groupes étant un sous-groupe, on en déduit immédiatement le résultat. □

Définition 53
*Soient a et b des éléments de $\mathbb{Z}$. Il existe un unique élément $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Cet élément m est appelé le **plus petit multiple commun** à a et à b, en abrégé* ppcm. *Il s'agit de l'unique générateur positif de $a\mathbb{Z} \cap b\mathbb{Z}$. On note $m = \text{ppcm}(a,b)$ ou encore $m = a \vee b$.*

Preuve — D'après le lemme, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$. Or pour tout sous-groupe H de $(\mathbb{Z},+)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. □

Proposition 54
Soient a et b des éléments de $\mathbb{Z}$. Alors $m = \text{ppcm}(a,b)$ si et seulement si

1. *$a \mid m$ et $b \mid m$, (autrement dit, m est un multiple commun à a et b),*
2. *Pour tout $m' \in \mathbb{Z}$, si $a \mid m'$ et $b \mid m'$ alors $m \mid m'$. (autrement dit, tout multiple commun à a et à b est un multiple de m).*

Preuve —

• Supposons que $m = \text{ppcm}(a,b)$. Alors $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Donc $m \in m\mathbb{Z} \subset a\mathbb{Z}$. Donc $a \mid m$. De même, $m \in b\mathbb{Z}$ donc $b \mid m$. D'où le premier point.

Soit $m' \in \mathbb{Z}$ tel que $a \mid m'$ et $b \mid m'$. Alors $m' \in a\mathbb{Z}$ et $m' \in b\mathbb{Z}$ donc $m' \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Donc $m \mid m'$.

• Réciproquement, supposons 1. et 2.. Montrons que $mZ = a\mathbb{Z} \cap b\mathbb{Z}$.

▷ D'après le premier point, $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$ donc $m \in a\mathbb{Z} \cap b\mathbb{Z}$. Donc $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

◁ Soit $m' \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$. Alors $m' \in a\mathbb{Z}$ donc $a \mid m'$ et $m' \in b\mathbb{Z}$ donc $b \mid m'$. Donc d'après le point 2., $m \mid m'$. Donc $m'\mathbb{Z} \subset m\mathbb{Z}$, soit $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$.

Finalement, $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. □

Remarque 55 — *On peut également définir le ppcm d'une famille d'éléments $a_1, \ldots, a_n$ comme étant le générateur positif de $a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}$, sous-groupe de $(\mathbb{Z},+)$. On montre que c'est un multiple commun de $a_1, \ldots, a_n$, diviseur de tout autre multiple commun.*

Remarque 56 — *La ppcm de a et b est le plus petit multiple commun pour la relation d'ordre $\leq$ sur $\mathbb{N}$. C'est aussi le plus petit multiple commun pour le relation de divisibilité sur $\mathbb{N}$.*

Exemple 57 — $\text{ppcm}(3,6) = 6, \quad \text{ppcm}(4,6) = 12.$

Proposition 58
Soient a, b et k des éléments de $\mathbb{Z}$. On a

1. $\text{ppcm}(a,b) = \text{ppcm}(|a|,|b|)$,
2. $\text{ppcm}(a,0) = 0$,
3. $\text{ppcm}(1,a) = |a|$,
4. $\text{ppcm}(a,b) = \text{ppcm}(b,a)$,
5. $\text{ppcm}(a,\text{ppcm}(b,c)) = \text{ppcm}(\text{ppcm}(a,b),c)$,
6. $\text{ppcm}(ka,kb) = |k|\text{ppcm}(a,b)$.

Preuve — Ces propriétés découlent de la définition du ppcm. □

On dispose de la relation suivante qui lie pgcd et ppcm.

Proposition 59
Soient a et b des éléments de $\mathbb{Z}$. Alors

$$\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |a| \times |b|.$$

En particulier, si a et b sont premiers entre eux, $\text{ppcm}(a,b) = |a| \times |b|$.

Preuve — On peut supposer a et b positifs.

Notons $d = \text{pgcd}(a,b)$. On exclut le cas trivial où $d = 0$ et où alors $a = 0$ ou $b = 0$. D'après la proposition ? ?, il existe des éléments a' et b' dans $\mathbb{Z}$ tels que $a = da'$, $b = db'$ et $\text{pgcd}(a',b') = 1$. On a $ab = d(da'b')$. Posons $m = da'b'$ et montrons que $m = \text{ppcm}(a,b)$.

On a $m = ab'$ donc $a \mid m$ et $m = a'b$ donc $b \mid m$. Donc m est un multiple commun à a et à b.

Soit $m' \in \mathbb{Z}$ tel que $a \mid m'$ et $b \mid m'$. Il existe donc $(u,v) \in \mathbb{Z}^2$ tel que $m' = au$ et $m' = bv$. On a donc $au = bv$, soit $da'u = db'v$. Donc $a'u = b'v$ et a' divise $b'v$. Or a' et b' sont premiers entre eux, donc d'après le théorème de Gauss, $a' \mid v$. Il existe donc $k \in \mathbb{Z}$ tel que $v = ka'$. On en déduit que $m' = bv = bka' = db'ka' = mk$. Donc $m \mid m'$.

D'où $m = \text{ppcm}(a,b)$. Or $m = \dfrac{ab}{d}$. Donc $\text{ppcm}(a,b) \times d = ab$. D'où le résultat. □

Exemple 60 — *Les multiples communs à 12 et 18 sont les multiples de 36.*

En effet, $\text{ppcm}(12,18) = \dfrac{12 \times 18}{\text{pgcd}(12,18)} = \dfrac{12 \times 18}{6} = 36.$

4.3 Nombres premiers

4.3.1 L'ensemble des nombres premiers

Définition 61
*Soit $p \in \mathbb{N}$. On dit que p est un nombre **premier** si p est différent de 1 et si ses seuls diviseurs positifs sont 1 et p.*

Exemple 62 — *2, 3, 5, 7, 11, 13, 17, 23, ..., sont les plus petits nombres premiers.*

Théorème 63
Tout entier $n \geq 2$ a au moins un diviseur premier.

Preuve — Soit $n \geq 2$. L'ensemble des diviseurs positifs différents de 1 de n est une partie non vide de $\mathbb{N} \setminus \{0,1\}$. Il admet donc un minimum p.

Si p n'est pas premier, alors il admet un diviseur q tel que $2 \leq q < p$ et comme q divise p, q divise n par transitivité. Ceci contredit la minimalité de p.

Donc p est un nombre premier qui divise n. □

PROPOSITION 64
Tout entier $n \geq 2$ qui n'est pas premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Preuve — Soit n un entier supérieur ou égal à 2 non premier. En reprenant la démonstration précédente, le minimum p de l'ensemble des diviseurs positifs de n est un nombre premier. Comme p divise n, il existe $q \in \mathbb{N}$ tel que $n = pq$. Donc q est un diviseur de n donc $p \leq q$ par minimalité de p. Donc $p^2 \leq pq = n$. D'où $p \leq \sqrt{n}$. □

REMARQUE 65 — *À l'aide du résultat précédent, on peut déterminer si un nombre n est premier ou non : on effectue successivement la division euclidienne de n par tous les entiers inférieurs à $\sqrt{n}$, et si l'une des divisions donne un reste nul alors n n'est pas premier, sinon n est premier.*

On peut dresser la liste des nombres premiers $p \leq n$ de manière algorithmique en utilisant le crible d'Eratosthène. Pour cela, on peut écrire tous les nombres compris entre 2 à n, puis procéder comme suit :

1. *le plus petit nombre est 2 qui est premier, et tous les multiples stricts de 2 ne sont pas premiers, on élimine alors tous ces multiples,*
2. *le premier nombre restant est 3, qui est donc premier, et tous les multiples stricts de 3 ne sont pas premiers, on élimine alors tous ces multiples,*
3. *le premier nombre restant est 5, qui est donc premier, et tous les multiples stricts de 5 ne sont pas premiers, on élimine alors tous ces multiples,*
4. *on poursuit ainsi jusqu'à tomber sur un nombre supérieur à $\sqrt{n}$.*

Les entiers non élimés sont alors exactement les nombres premiers inférieurs à n puisque les entiers non premiers inférieurs à n possèdent un diviseur premier inférieur à $\sqrt{n}$ et ont donc été éliminés.

PROPOSITION 66
Soient p un nombre premier et $a \in \mathbb{Z}$. Alors soit p divise a, soit p et a sont premiers entre eux.

Preuve — Supposons que p ne divise pas a. Le pgcd de p et a divise p donc, p étant premier, $\text{pgcd}(p, a) = 1$ ou $\text{pgcd}(p, a) = p$. Or p ne divise pas a donc $\text{pgcd}(p, a) \neq p$. Donc $\text{pgcd}(p, a) = 1$ et a et p sont premiers entre eux. □

Cela n'est vrai qu'avec p premier. Par exemple 6 ne divise par 15 et 6 et 15 ne sont pas premiers entre eux.

PROPOSITION 67
Deux nombres premiers distincts sont premiers entre eux.

Preuve — Soient p et q deux nombres premiers. Supposons que p et q ne sont pas premiers entre eux. Alors d'après la proposition précédente, p divise q, mais aussi q divise p. Donc $p = q$. Par contraposition, on obtient le résultat. □

PROPOSITION 68 (Théorème d'Euclide)
Soient p un nombre premier et a et b deux éléments de $\mathbb{Z}$. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Plus généralement, si $a_1, \ldots, a_n$ sont des éléments de $\mathbb{Z}$ et si p divise le produit $a_1 \times \ldots \times a_n$ alors p divise l'un des a_i.

Preuve —

- Supposons que $p \mid ab$.
  - 1er cas : p divise a.
  - 2ème cas : p ne divise pas a. Alors, p étant premier, p et a sont premiers entre eux, donc d'après le théorème de Gauss, p divise b.

  D'où le résultat.
- La généralisation s'obtient par récurrence.

□

EXEMPLE 69 — *Soit $(a, b) \in \mathbb{Z}^2$. Si $2 \mid ab$ alors $2 \mid a$ ou $2 \mid b$ car 2 est un nombre premier.*

PROPOSITION 70
Il existe une infinité de nombres premiers.

Preuve —

Supposons par l'absurde qu'il existe un nombre fini N de nombres premiers. Notons alors p_1, p_2, …, p_N la liste des nombres premiers.

Alors $p = p_1 \times p_2 \times \ldots \times p_N + 1$ est un entier supérieur ou égal à 2. Il admet donc un diviseur premier et il existe donc $i_0 \in \{1, \ldots, N\}$ tel que $p_{i_0} \mid p$. On en déduit que p_{i_0} divise p et p_{i_0} divise $p_1 \times p_2 \times \ldots \times p_n$, et donc p_{i_0} divise $p - p_1 \times p_2 \times \ldots \times p_n = 1$. Donc $p_{i_0} = 1$, ce qui est absurde car p_{i_0} est un nombre premier. □

4.3.2 Décomposition en produit de facteurs premiers

THÉORÈME 71 (Théorème fondamental de l'arithmétique)
Tout entier naturel $n \geq 2$ se décompose, de manière unique à l'ordre près des termes, en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_N^{\alpha_N},$$

où les p_i sont des nombres premiers deux à deux distincts et les α_i sont des entiers naturels non nuls.

Preuve —

- *Existence :* Démontrons ce résultat par récurrence. Pour tout $n \geq 2$, on note (H_n) la propriété : « n se décompose en produit de facteurs premiers. »
  • *Initialisation :* $n = 2$ est un nombre premier, donc n s'écrit comme le produit de nombres premiers. D'où (H_2).
  • *Hérédité :* Soit $n \geq 3$. Supposons (H_k) pour tout $2 \leq k \leq n-1$.
  Si n est premier, alors n se décompose en produit de facteurs premiers.
  Sinon, il existe des entiers naturels a et b tels que $n = ab$ avec a et b différents de 1. Alors $a < n$ et $b < n$ et donc par hypothèse de récurrence appliquée à a et à b, a et b se décomposent en produit de facteurs premiers. Donc n étant le produit de a et b, on en déduit (H_n).
- *Unicité :* Supposons que n s'écrive sous la forme

  $$n = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N} \quad \text{et} \quad n = q_1^{\beta_1} \times \ldots \times q_R^{\beta_R},$$

  où les p_i et q_i sont des nombres premiers, les p_i étant distincts deux à deux, les q_i également, et les α_i et β_i sont des entiers naturels non nuls.
  Pour tout $i \in \{1, \ldots, N\}$, $p_i \mid n$ donc p_i divise l'un des q_j et p_i et q_j étant des nombres premiers, $p_i = q_j$. Donc $\{p_1, \ldots, p_N\} \subset \{q_1, \ldots, q_R\}$.
  Par symétrie des rôles, on en déduit que $\{q_1, \ldots, q_R\} \subset \{p_1, \ldots, p_N\}$. Ces deux ensembles sont donc égaux et $N = R$. Quitte à permuter les indices, on peut supposer que pour tout $i \in \{1, \ldots, N\}$, $p_i = q_i$.
  Soit $i \in \{1, \ldots, n\}$. Alors $p_i^{\alpha_i} \mid n = p_1^{\beta_1} \times \ldots p_N^{\beta_N} = p_i^{\beta_i} k$ avec $\text{pgcd}(p_i^{\alpha_i}, k) = 1$. Donc d'après le théorème de Gauss, $p_i^{\alpha_i} \mid p_i^{\beta_i}$. Donc $\alpha_i \leq \beta_i$. Par symétrie des rôles, on a également $\beta_i \leq \alpha_i$, donc finalement $\alpha_i = \beta_i$.
  D'où l'unicité.

□

REMARQUE 72 — *Pour tout nombre premier p et tout entier $n \geq 2$, on note $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers ($\nu_p(n) = 0$ si p ne divise pas n). $\nu_p(n)$ s'appelle la* ***valuation p-adique*** *de n. On a $\nu_p(n) = \max\{k \in \mathbb{N} \mid p^k \text{ divise } n\}$.*

MÉTHODE 73 — *Pour décomposer un nombre entier $n \geq 2$, on peut procéder de la façon suivante :*

1. *On cherche la plus grande puissance $\alpha_1 \geq 0$ de 2 divisant n, on obtient $n = 2^{\alpha_1} n_1$ où $n_1 \in \mathbb{N}$ et n_1 n'est plus divisible par 2. Si $n_1 = 1$, on a terminé, sinon on passe à l'étape suivante.*
2. *On cherche la plus grande puissance $\alpha_2 \geq 0$ de 3 divisant n_1, on obtient alors $n = 2^{\alpha_1} \times 3^{\alpha_2} n_2$ où $n_2 \in \mathbb{N}$ et n_2 n'est plus divisible par 3 (ni 2 par la première étape). Si $n_2 = 1$, on a terminé, sinon on passe à l'étape suivante.*
3. *On cherche la plus grande puissance $\alpha_3 \geq 0$ de 5 divisant n_2, etc.*

EXEMPLE 74 — $360 = 2^3 \times 3^2 \times 5$, $\quad 147 = 3 \times 7^2$, $\quad 1575 = 3^2 \times 5^2 \times 7$.

PROPOSITION 75
Soit un entier $n \geq 2$. On suppose que n s'écrit sous la forme $n = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ où les p_i sont des nombres premiers distincts deux à deux et les α_i des entiers naturels non nuls.

Les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} \ldots p_N^{\beta_N}$ avec, pour tout $i \in \{1, \ldots, N\}$, $0 \leq \beta_i \leq \alpha_i$.

Exemple 76 — *Les diviseurs positifs de* $45 = 3^2 \times 5$ *sont les suivants :* $3^0 \times 5^0 = 1$, $3^0 \times 5 = 5$, $3 \times 5^0 = 3$, $3 \times 5 = 15$, $3^2 \times 5^0 = 9$, $3^2 \times 5 = 45$.

On dispose du résultat suivant pour calculer les pgcd et ppcm à partir de la décomposition en nombres premiers de chacun des termes.

Proposition 77
Soient a et b deux entiers supérieurs ou égaux à 2. On suppose que a s'écrit sous la forme $a = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ et b s'écrit sous la forme $b = p_1^{\beta_1} \times \ldots \times p_N^{\beta_N}$ où les p_i sont des nombres premiers distincts deux à deux et les α_i et β_i sont des entiers naturels. Alors

- $\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \times \ldots \times p_N^{\min(\alpha_N,\beta_N)}$,
- $\text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \times \ldots \times p_N^{\max(\alpha_N,\beta_N)}$.

Exemples 78

- $\text{pgcd}(147, 1575) = 3 \times 7 = 21$,
- $\text{ppcm}(147, 1575) = 3^2 \times 5^2 \times 7^2 = 11025$.

Proposition 79
Soient a et b des éléments de $\mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'ils n'ont pas de facteurs premiers en commun dans leur décomposition en facteurs premiers.

Preuve — Si a et b sont premiers entre eux, alors leur seul diviseur commun positif est 1 et n'ont donc pas de facteur premier en commun.

Supposons a et b premiers entre eux. Notons $d = \text{pgcd}(a,b)$. Alors $d \geq 2$ et d admet donc un diviseur premier p. Comme d divise a et b, p divise également a et b et p est donc un facteur premier commun à a et à b. □

Exemple 80 — $825 = 3 \times 5^2 \times 11$ *et* $56 = 2^3 \times 7$ *sont premiers entre eux.*