Université Moulay Ismail
Faculté des Sciences et Techniques

Notes de Cours du module

ALGÈBRE 1

2024-2025

Table des matières

Chapitre 1

Théorie des ensembles, applications et relations binaires

I. Théorie des ensembles - notions de base

I.1. Introduction

En se basant sur la connaissance intuitive que nous avons, on peut dire qu'un **ensemble** est une collection d'objets distincts appelés **éléments**, avec la propriété suivante : *pour un objet donné, l'assertion que cet objet appartient à la collection est soit vraie, soit fausse.*
Soit E un ensemble et x un objet. Si x est un élément de l'ensemble E, on écrit $x \in E$. Sinon, on écrit $x \notin E$.
On peut définir un ensemble de deux manières :

- **en extension** : on donne la liste explicite de tous les éléments.
  Exemple : l'ensemble $A = \{1,2,3,4\}$ est défini en extension.
- **en compréhension** : on donne une propriété commune vérifiée par les éléments de l'ensemble.
  Exemple : l'ensemble $B = \{n \in \mathbb{Z} \ / \ -1 \leq n \leq 6\}$ est défini en compréhension.

Exercice 1. 1. Soit $E = \{0,1,2,\ldots,20\}$.
Exprimer en extension les ensembles suivants :
$A = \{n \in E \ / \ n \text{ est premier}\}$, $B = \{n \in E \ / \ n \text{ est un multiple de } 5\}$ et
$C = \{n \in E \ / \ n \text{ divise } 20\}$.

2. Exprimer en compréhension les ensembles suivants :
$A = \{-3,-2,-1,0,1,2,3\}$, $3\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{C}$.

Vocabulaires :

1. Il existe un ensemble qui ne contient aucun élément, c'est **l'ensemble vide** et est noté $\emptyset$.
2. Un **singleton** est un ensemble qui contient un seul élément.
3. Une **paire** est un ensemble qui contient exactement deux éléments.

I.2. Inclusion et ensemble des parties

Définition 1.1. (Inclusion) Soient A et B deux ensembles.

On dit que A est **inclus** dans B et on écrit $A \subseteq B$ ou $A \subset B$ si tout élément de A est aussi un élément de B. On dit aussi que A est **une partie** de B ou encore A est un **sous-ensemble** de B.

Notations. 1. Si $A \subseteq B$ et $A \neq B$, on écrit $A \subsetneq B$ et on dit que A est strictement inclus dans B.

2. Si A n'est pas inclus dans B, on écrit $A \not\subset B$.

Par définition, on a :

$$(A \subseteq B) \Longleftrightarrow (\forall x,\, x \in A \Longrightarrow x \in B)$$

$$(A \not\subset B) \Longleftrightarrow (\exists x,\, x \in A \text{ et } x \notin B).$$

Remarque 1.1. Pour tout ensemble E, on a : $\emptyset \subset E$.

Exemple 1.1. On a $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, mais $\mathbb{C} \not\subset \mathbb{R}$ (du fait que $i \in \mathbb{C}$ mais $i \notin \mathbb{R}$).

Définition 1.2. (Égalité de deux ensembles) On dit que deux ensembles A et B sont égaux et on note $A = B$, s'ils sont constitués des mêmes éléments.

Autrement dit,

$$(A = B) \Longleftrightarrow (\forall x,\, x \in A \Longleftrightarrow x \in B).$$

Exercice 2. Prouver que :

1. $\{x \in \mathbb{R} \,/\, x^2 - 3x - 4 = 0\} = \{-1,4\}$.
2. $\{x \in \mathbb{R} \,/\, x^2 - 2x + 1 < 0\} = \emptyset$.
3. Le domaine de définition de la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \frac{x+1}{x-1}$ est $\mathbb{R} \setminus \{1\}$.

Proposition 1.1. *Soient A, B et C des ensembles. On a :*

1. *$A \subset A$;*
2. *si $A \subset B$ et $B \subset A$ alors $A = B$;*
3. *si $A \subset B$ et $B \subset C$ alors $A \subset C$.*

Démonstration. À faire à titre d'exercice. □

Remarque 1.2. Soient E et F deux ensembles.
Pour prouver que $E \subset F$, on considère généralement un élément quelconque x de E et on essaie de prouver que $x \in F$.
Pour montrer $E = F$, on procèdera souvent par double inclusion : on prouve séparément $E \subset F$ et $F \subset E$.

Notation. L'ensemble des parties d'un ensemble E, c'est-à-dire l'ensemble de tous les sous-ensembles de E, est noté $\mathcal{P}(E)$.

Ainsi,

$$A \in \mathcal{P}(E) \Longleftrightarrow A \subset E.$$

Exercice 3. 1. Déterminer l'ensemble des parties des ensembles suivants : $A = \{a\}$, $B = \{a,b\}$ et $C = \{a,b,c\}$.

2. Déterminer $\mathcal{P}(\mathcal{P}(A))$ et $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

I.3. Opérations sur les ensembles

Définition 1.3. Soient A et B deux ensembles. On définit les opérations suivantes :

- **Union** : l'union de A et B, notée $A \cup B$, est l'ensemble des éléments qui appartiennent à A ou à B, c-à-d

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

Formellement,

$$x \in A \cup B \Longleftrightarrow (x \in A \text{ ou } x \in B).$$

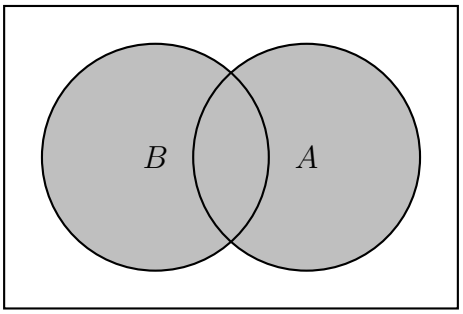


FIGURE 1.1 – L'union $A \cup B$

- **Intersection** : l'intersection de A et B, notée $A \cap B$, est l'ensemble des éléments qui appartiennent à la fois à A et à B, c-à-d

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

Formellement,

$$x \in A \cap B \Longleftrightarrow (x \in A \text{ et } x \in B).$$

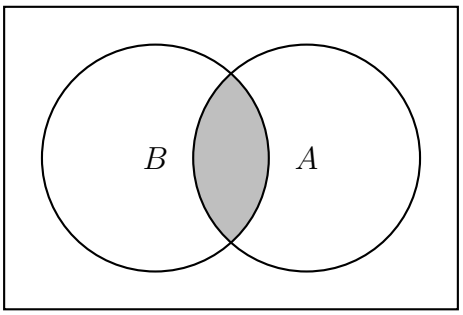


FIGURE 1.2 – L'intersection $A \cap B$

Les ensembles A et B sont dits **disjoints** si $A \cap B = \emptyset$.

- **Différence** : la différence de A et B (dans cet ordre), notée $A \setminus B$, est l'ensemble des éléments de A qui n'appartiennent pas à B, c-à-d

$$A \setminus B = \{x \mid x \in A \text{ et } x \notin B\}.$$

Formellement,

$$x \in A \setminus B \Longleftrightarrow (x \in A \text{ et } x \notin B).$$

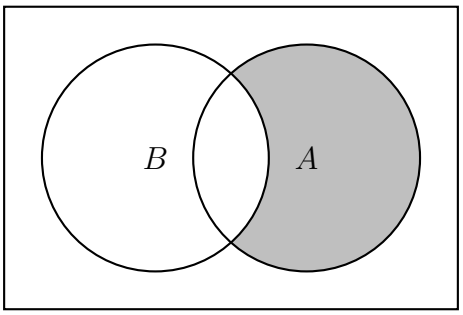


FIGURE 1.3 – La différence $A \setminus B$

- **Différence symétrique :** la différence symétrique de A et B, noté $A \triangle B$, est l'ensemble des éléments qui appartient à $A \cup B$ et qui ne sont pas dans $A \cap B$, c-à-d

$$A \triangle B = (A \cup B) \setminus (B \cap A).$$

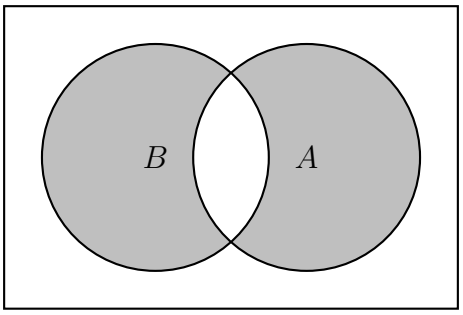


FIGURE 1.4 – La différence symétrique $A \triangle B$

- **Complémentaire** : si A **est une partie de** B, le complémentaire de A dans B, noté $\complement_B A$, est l'ensemble des éléments de B qui n'appartiennent pas à A, c-à-d

$$\complement_B A = \{x \in B \mid x \notin A\}.$$

Formellement,

$$x \in \complement_B A \Longleftrightarrow x \in B \text{ et } x \notin A.$$

Si aucune confusion n'est à craindre, le complémentaire de A dans B se note aussi A^c ou encore $\overline{A}$.
Remarquons au passage que $\complement_B A = B \setminus A$.

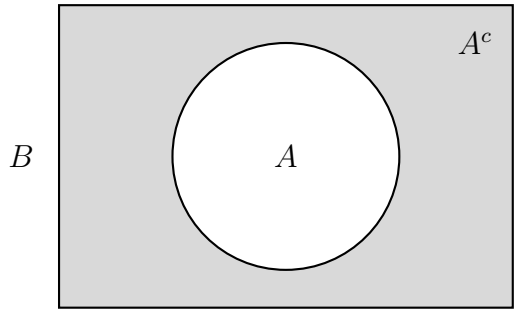


FIGURE 1.5 – Le complémentaire $\complement_B A$

Exercice 4. 1. Considérons les ensembles $E = \{1,2,3,4,5,6,7,8\}$, $A = \{1,2,3,4\}$ et $B = \{1,2,5,6,7\}$.
Déterminer les ensembles $A \cap B$, $A \cup B$, $A \setminus B$, $B \setminus A$, $A \triangle B$ et $\complement_E A$.

2. On pose $I =]-\infty,2]$ et $J =]-3,+\infty[$.
Déterminer les ensembles $I \cap J$, $I \cup J$, $I \setminus J$, $J \setminus I$, $I \triangle J$ et $\complement_{\mathbb{R}} I$.

3. Déterminer les ensembles A et B sachant que $A \cup B = \{1,2,3,4,5,6,7,8,9\}$, $A \cap B = \{4,5,6,9\}$ et $A \setminus B = \{7,8\}$.

4. Soient $A = \{1,2,3,4\}$ et $B = \{3,4,5,6\}$. Déterminer l'ensemble X tel que $A \triangle X = B$.

Union et intersection d'un nombre quelconque d'ensembles : Les notions d'union et d'intersection se généralisent à un nombre quelconque d'ensembles. Soit I un ensemble quelconque et pour tout $i \in I$, A_i est un ensemble (on parle de famille d'ensembles, notée $(A_i)_{i\in I}$, indexée par I). L'union (resp. l'intersection) des ensembles A_i, pour tout $i \in I$, est l'ensemble, noté $\bigcup_{i\in I} A_i$, des éléments qui appartiennent à au moins l'un des ensembles A_i (resp. l'ensemble, noté $\bigcap_{i\in I} A_i$, des éléments qui appartiennent à tous les ensembles A_i), c-à-d

$$\bigcup_{i\in I} A_i = \{x \ / \ \exists i_0 \in I, x \in A_{i_0}\} \quad \text{et} \quad \bigcap_{i\in I} A_i = \{x \ / \ \forall i \in I, x \in A_i\}.$$

Formellement,

$$x \in \bigcup_{i\in I} A_i \Longleftrightarrow \exists i \in I, x \in A_i \quad \text{et} \quad x \in \bigcap_{i\in I} A_i \Longleftrightarrow \forall i \in I, x \in A_i.$$

En particulier, lorsque $I = \{1,2,\ldots,n\}$ alors,

$$\bigcup_{i\in I} A_i = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n \quad \text{et} \quad \bigcap_{i\in I} A_i = \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n.$$

Exemples 1.1.
- $\bigcup_{n=1}^{4}]-n,n] =]-4,4]$ et $\bigcap_{n=1}^{4}]-n,n] =]-1,1]$.
- $\bigcup_{n\in\mathbb{N}} \{n\} = \mathbb{N}$ et $\bigcap_{n\in\mathbb{N}} \{n\} = \emptyset$.

Vocabulaire : les ensembles d'une famille de parties $(A_i)_{i\in I}$ d'un ensemble E sont dits deux à deux disjointes si deux ensembles quelconques et distincts de cette famille sont disjoints.

Autrement dit,

$$\forall i,j \in I,\, i \neq j \Longrightarrow A_i \cap A_j = \emptyset.$$

Par exemple, la famille $(\{x\})_{x\in\mathbb{Z}}$ est une famille de parties de $\mathbb{Z}$ deux à deux disjointes.

Les propriétés des opérations sur les ensembles sont données par les propositions suivantes dont la preuve de chacune d'elles est laissée à titre d'exercice.

Proposition 1.2. *Soient A, B et C des parties d'un ensemble E.*
Les propriétés suivantes sont vérifiées :

1) $A \cup B = B \cup A \quad et \quad A \cap B = B \cap A$;

2) $(A \cup B) \cup C = A \cup (B \cup C) \quad et \quad (A \cap B) \cap C = A \cap (B \cap C)$;

3) $A \cup \emptyset = A$ *et* $A \cap E = A$;

4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad et \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *Plus généralement, si $(B_i)_{i\in I}$ est une famille de parties de E, alors*

$$A \cap (\bigcup_{i\in I} B_i) = \bigcup_{i\in I}(A \cap B_i) \quad et \quad A \cup (\bigcap_{i\in I} B_i) = \bigcap_{i\in I}(A \cup B_i).$$

Proposition 1.3. *Soient A, B, C et D des parties d'un ensemble E.*
Les propriétés suivantes sont vérifiées :

1. $A \cup A = A \cap A = A$;
2. $A \cap B \subset A \subset A \cup B$;
3. *si* $A \subset C$ *et* $B \subset D$ *alors* $A \cup B \subset C \cup D$ *et* $A \cap B \subset C \cap D$.

Proposition 1.4. *Soient A et B deux parties d'un ensemble E.*
Les propriétés suivantes sont vérifiées :

1. $(A^c)^c = A$, $\emptyset^c = E$, $E^c = \emptyset$, $A \cup A^c = E$ *et* $A \cap A^c = \emptyset$;
2. $A \subset B \Longleftrightarrow B^c \subset A^c$;
3. *(Lois de De Morgan)*

$$(A \cup B)^c = A^c \cap B^c \quad et \quad (A \cap B)^c = A^c \cup B^c.$$

Plus généralement, si $(A_i)_{i\in I}$ est une famille de parties de E, alors

$$(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c \quad et \quad (\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c.$$

Proposition 1.5. *Soient A, B et C des parties d'un ensemble E.*
Les propriétés suivantes sont vérifiées :

1. *(a)* $A \setminus B = A \cap B^c$;
   (b) $A \setminus A = \emptyset$ *et* $A \setminus \emptyset = A$;
   (c) $A \setminus B = \emptyset \Longleftrightarrow A \subset B$
2. *(a)* $A\triangle B = B\triangle A$, $A\triangle(B\triangle C) = (A\triangle B)\triangle C$, $A\triangle\emptyset = A$ *et* $A\triangle A = \emptyset$;
   (b) $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$.

Remarque 1.3. En générale, on a $(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$. Par exemple, $(\mathbb{N} \setminus \mathbb{Z}) \setminus \mathbb{R} = \emptyset$ et $\mathbb{N} \setminus (\mathbb{Z} \setminus \mathbb{R}) = \mathbb{N}$.

Exercice 5. Soient A, B, C et D des parties d'un ensemble E. Montrer que :

1. si $A \cap B \subset A \cap C$ et $A \cup B \subset A \cup C$ alors $B \subset C$.
2. Si $A \cap B = A \cap C$ et $B \setminus A = C \setminus A$ alors $B = C$.
3. $(A \setminus B) \cap (C \setminus D) = (A \cap B) \setminus (B \cup D)$.
4. si $A\triangle B = A\triangle C$ alors $B = C$.
5. $(A\triangle B)^c = A^c\triangle B = A\triangle B^c$.
6. si $A\triangle B = \emptyset$ alors $A = B$.

I.4. Produit cartésien

Définition 1.4. Le produit cartésien de deux ensembles E et F (dans cet ordre) est l'ensemble, noté $E \times F$, défini par :

$$E \times F = \{(x,y) \ / \ x \in E \text{ et } y \in F\}.$$

Un élément (x,y) de $E \times F$ s'appelle **un couple**.

On a donc,

$$(x,y) \in E \times F \Longleftrightarrow x \in E \text{ et } y \in F,$$

ou encore,

$$z \in E \times F \Longleftrightarrow (\exists x \in E)(\exists y \in F) \ : \ z = (x,y).$$

Exemple 1.2. Soient $E = \{1,2\}$ et $F = \{3,4,5\}$. On a :
• $E \times F = \{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5)\}$.
• $F \times E = \{(3,1),(3,2),(4,1),(4,2),(5,1),(5,2)\}$.

Remarquons au passage que $E \times F \neq F \times E$ en générale. Ceci découle du fait que

$$(a,b) = (c,d) \Longleftrightarrow a = c \text{ et } b = d.$$

Remarques 1.1. 1. Soit $n \in \mathbb{N}^*$ et $I = \{1,2,\ldots,n\}$, le **produit cartésien** de n ensembles A_1, A_2,..., A_n est :

$$\prod_{i\in I} A_i = \prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n = \Big\{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i \text{ pour } 1 \leq i \leq n\Big\}.$$

Si $A_1 = A_2 = \cdots = A_n = A$, alors le produit cartésien $A_1 \times A_2 \times \cdots \times A_n$ sera noté A^n, c-à-d

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ fois}}.$$

2. $\prod_{i=1}^{n} A_i = \emptyset \Longleftrightarrow (\exists i \in \{1,2,\ldots,n\})\ A_i = \emptyset$.

3. Si pour tout $i \in \{1,2,\ldots,n\}$ on a $A_i \subset B_i$, alors $\prod_{i=1}^{n} A_i \subset \prod_{i=1}^{n} B_i$.

Vocabulaires : Un élément $(x_1, x_2, \ldots, x_n)$ de $\prod_{i=1}^{n} A_i$ est appelé un n**-uplet**. Ainsi, un couple est un 2-uplet, un triplet est un 3-uplet, un quadruplet est un 4-uplet et ainsi de suite.

Proposition 1.6. *Soient A, B et C des ensembles.*

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$ *et* $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

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

Démonstration. À faire à titre d'exercice. □

Exercice 6. Soient A, B, C et D des parties d'un ensemble E. Montrer que :

1. $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$ (en général).

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

3. $\overline{A \times B} = (\overline{A} \times E) \cup (E \times \overline{B})$.

4. $\overline{A \times B} = (\overline{A} \times B) \cup (\overline{A} \times \overline{B}) \cup (A \times \overline{B})$.

I.5. Recouvrement et partition

Définition 1.5. (**Recouvrement d'un ensemble**) **Un recouvrement** d'un ensemble E est une famille d'ensembles $(A_i)_{i\in I}$ telle que $E \subset \bigcup_{i\in I} A_i$.

Remarque 1.4. Si les ensembles A_i, $i \in I$, sont des parties de E alors l'inclusion $E \subset \bigcup_{i\in I} A_i$ est en fait une égalité.

Exemples 1.2.
1. La famille d'ensembles $(I_n)_{n\in\mathbb{N}}$, où $I_n =]-n,n[$, est un recouvrement de $\mathbb{N}$. En effet, pour tout $k \in \mathbb{N}$, $k \in I_{k+1} =]-k-1,k+1[\subset \bigcup_{i\in\mathbb{N}} I_i$.

2. Clairement $\mathbb{N} = \bigcup_{n\in\mathbb{N}} \{n\}$, donc la famille $(\{n\})_{n\in\mathbb{N}}$ est un recouvrement de $\mathbb{N}$.

Définition 1.6. (**Partition d'un ensemble**) Soit E un ensemble non vide. On dit qu'une famille d'ensembles $(A_i)_{i\in I}$ est **une partition** de E si les conditions suivantes sont vérifiées :

1. pour tout $i \in I$, $A_i \subset E$;

2. pour tout $i \in I$, $A_i \neq \emptyset$;

3. pour tous $i \neq j \in I$, $A_i \cap A_j = \emptyset$;

4. $E = \bigcup_{i\in I} A_i$.

Remarque 1.5. Une partition d'un ensemble E est un recouvrement de E par une famille de parties non vides de E qui sont deux à deux disjointes.

Exemples 1.3. 1. Les ensembles $A = \{1,2\}$ et $B = \{3,4,5,6\}$ forment une partition de l'ensemble $E = \{1,2,3,4,5,6\}$.

2. Les intervalles $]-\infty,-1]$, $]-1,2]$ et $]2,+\infty[$ forment une partition de $\mathbb{R}$.

3. Les ensembles $\mathbb{R}_+$ et $\mathbb{R}_-$ ne forment pas une partition de $\mathbb{R}$.

Exercice 7. Soient A et B deux parties non vides d'un ensemble E. On suppose que : $A \cap B \neq \emptyset$, $A \cup B \neq E$, $A \not\subset B$ et $B \not\subset A$. On considère les ensembles $A_1 = A \cap B$, $A_2 = A \cap \overline{B}$, $A_3 = \overline{A} \cap B$ et $A_4 = \overline{A \cup B}$.

Montrer que la famille $(A_i)_{1 \leq i \leq 4}$ est une partition de l'ensemble E.

II. Applications

II.1. Définitions et exemples

Définition 1.7. Soient E et F deux ensembles. On appelle **correspondance** (ou **relation**) de E vers F tout triplet $f = (E, F, G)$ où G est une partie de $E \times F$.

Vocabulaires :

1. L'ensemble E (resp. F) est appelé l'ensemble de départ ou source (resp. l'ensemble d'arrivée ou but) de f.

2. L'ensemble G est appelé le graphe de f.

3. Si (x, y) est un élément du graphe G, y sera appelé une image de x par f et x un antécédent de y.

Exemple 1.3. Soit $f = (\mathbb{R}, \mathbb{R}, G)$, avec

$$G = \Big\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x\Big\}$$

- On a $(0,0) \in G$ (0 admet une seule image).
- Si $x \in \mathbb{R}_+^*$ alors $(x, \sqrt{x})$ et $(x, -\sqrt{x})$ appartiennent au graphe G ($x \in \mathbb{R}_+^*$ admet deux images distinctes).
- Si $x \in \mathbb{R}_-^*$ alors x n'a aucune image (car, pour tout $y \in \mathbb{R}$, $y^2 \neq x$, puisque $y^2 \geq 0$ et $x < 0$).

Définition 1.8. Une correspondance $f = (E, F, G)$ est dite **fonction** de E vers F si tout élément de E admet **au plus** une image par f dans F.

En termes de graphe : pour $x \in E$, il peut arriver qu'il n'y ait aucun élément y de F tel que $(x, y) \in G$; mais si y et y' sont deux éléments de F tels que $(x, y) \in G$ et $(x, y') \in G$, alors $y = y'$.

Vocabulaires et notations : Soit $f = (E, F, G)$ une fonction de E vers F.

1. Si un élément x de E admet une image y dans F, alors l'élément y est unique et sera noté $y = f(x)$. Dans ce cas x est un antécédent de y par f.

2. La fonction $f = (E, F, G)$ sera notée :

$$f : E \longrightarrow F, \quad x \mapsto f(x) \quad \text{ou} \quad \begin{array}{l} f : E \longrightarrow F \\ x \longmapsto f(x) \end{array}$$

Le graphe G de la fonction f est donné par :

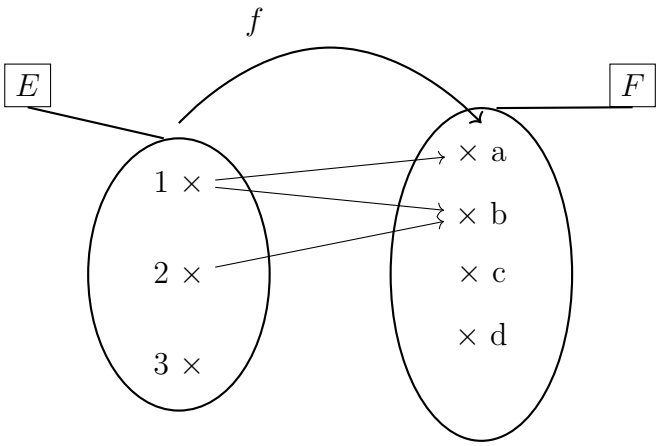
$$G = \{(x, y) \in E \times F \mid y = f(x)\}.$$

Remarque 1.6. Le domaine de définition d'une fonction $f : E \to F$, $x \mapsto f(x)$, noté D_f ou tout simplement D, est défini par :

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

Exemples 1.4. 1)

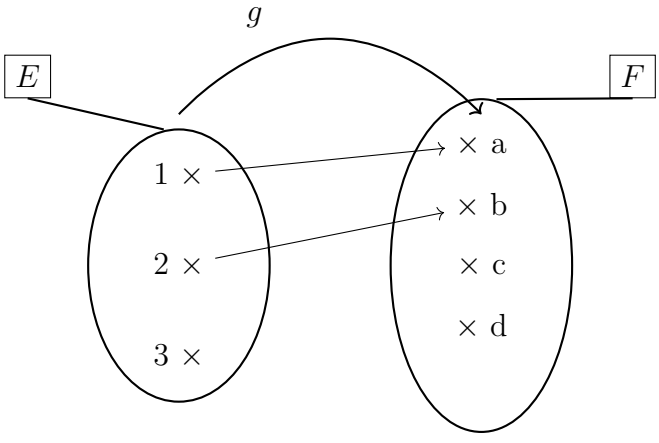
1.



f est une correspondance mais elle n'est pas une fonction, car 1 admet deux images distinctes par f. Son graphe est :

$$G = \{(1, a); (1, b); (2, b)\}$$

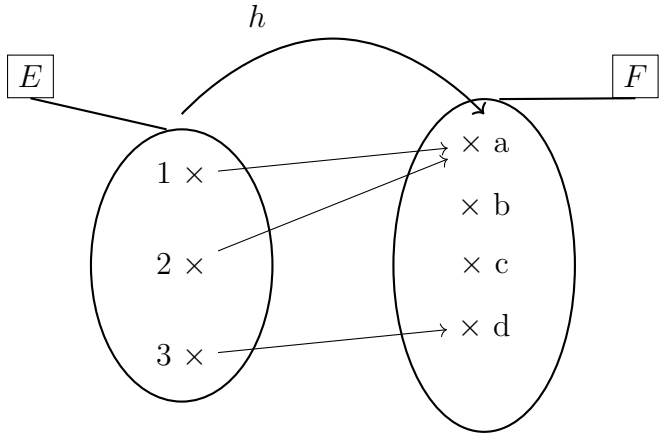
2.



g est une fonction de E vers F. Son graphe est $G = \{(1, a); (2, b)\}$ et son domaine de définition est :

$$D_g = \{1, 2\}$$

3.



h est une fonction de E vers F. Son graphe est $G = \{(1, a); (2, a); (3, d)\}$ et son domaine de définition est :

$$D_h = \{1, 2, 3\} = E.$$

2) La correspondance $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \sqrt{x}$ est une fonction de $\mathbb{R}$ vers $\mathbb{R}$.

- Tout élément $x \in \mathbb{R}_-^*$ n'admet pas d'image.
- Chaque élément $x \in \mathbb{R}_+$ admet une seule image. Le domaine de définition de f est $D_f = \mathbb{R}_+$.

Définition 1.9. Une fonction f de E vers F est dite une **application** si chaque élément de l'ensemble de départ E admet exactement une image dans F par f.

En termes de graphe : si G est le graphe de la fonction f, alors f est une application, si et seulement si :

$$(\forall x \in E)(\exists! y \in F) : (x, y) \in G.$$

Ce qui se traduit par :

$$\forall (x, y), (x', y') \in G \ \ (x = x') \Longrightarrow (y = y') \qquad (\alpha).$$

Remarques 1.2.

1. Le domaine de définition d'une application est égal à son ensemble de départ.
2. Le graphe d'une application f de E vers F est l'ensemble :

$$G = \{(x, f(x)) \mid x \in E\}.$$

3. D'après (α),

$$\Big(f \text{ est une application}\Big) \Longleftrightarrow \Big(\forall (x, x') \in E^2, \quad x = x' \Rightarrow f(x) = f(x')\Big).$$

Attention : L'implication réciproque n'est pas toujours vraie. En effet, si on considère l'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ on a : $f(1) = f(-1)$ mais $1 \neq -1$.

Notation. On note $\mathcal{F}(E, F)$ ou encore F^E l'ensemble des applications de E vers F.

Exemples 1.5.
1. La fonction h de l'exemple 1) 3 de la page 12 est une application de E vers F.
2. La fonction $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2 + 1$ est une application (car $D_f = \mathbb{R}$).
3. La fonction $g : \mathbb{R} \to \mathbb{R}^+, x \mapsto \sqrt{x}$ n'est pas une application (car $D_g = \mathbb{R}^+ \neq \mathbb{R}$).
4. La fonction $T : \mathbb{N} \longrightarrow \mathbb{N}, n \mapsto n - 1$ n'est pas une application, car 0 n'admet pas d'image dans $\mathbb{N}$ par f.

Exemples importants d'applications

1. Une application $f : E \to F$ est dite **constante** s'il existe un $a \in F$ tel que $\forall x \in E, f(x) = a$. Autrement dit, une application $f : E \to F$ est constante si
$$\forall (x, x') \in E^2, \quad f(x) = f(x').$$
Par exemple, les applications :
$$f_1 : \begin{array}{c}\mathbb{R}\longrightarrow\mathbb{R}\\ x\longmapsto 0\end{array}, \quad f_2 : \begin{array}{c}\mathbb{N}\longrightarrow\mathbb{R}\\ n\longmapsto -1\end{array} \text{ et } \quad f_3 : \begin{array}{ccc}\mathcal{P}(E)&\longrightarrow&\mathcal{P}(E)\\ A&\longmapsto&\emptyset\end{array} \quad (E \text{ est un ensemble})$$
sont des applications constantes. En revanche, l'application $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$ n'est pas constante, car $f(0) = 1 \neq 2 = f(1)$.
2. L'application $\mathrm{id}_E : E \to E, x \mapsto x$ est appelée l'application **identique** (ou l'identité) de E. On la note aussi id ou encore Id_E. On a donc
$$(\forall x \in E)\ \mathrm{id}_E(x) = x.$$
3. Soit A une partie de E. L'application
$$\chi_A : E \longrightarrow \{0,1\}$$
$$x \longrightarrow \begin{cases} 1, & \text{si } x \in A, \\ 0, & \text{si } x \notin A \ (i.e., x \in \bar{A}), \end{cases}$$
est appelée l'application **caractéristique** (ou **indicatrice**) de A.

Définition 1.10. Deux applications $f : E \to F$ et $g : E' \to F'$ sont dites **égales** ou **identiques** et on écrit $f = g$, si $E = E'$, $F = F'$ et $\forall x \in E$, $f(x) = g(x)$.

Remarques 1.3.
1. Si $E = E'$ et $F = F'$, alors $f \neq g$ si et seulement s'il existe $x \in E$, tel que $f(x) \neq g(x)$.
2. L'égalité $f = g$ a lieu dans $\mathcal{F}(E, F)$ alors que l'égalité $f(x) = g(x)$ a lieu dans F. Ne pas confondre les deux : $f = g$ entraîne $f(x) = g(x)$, par contre $f(x) = g(x)$ doit être vrai pour tout $x \in E$ pour qu'on puisse en déduire $f = g$.

Exemples 1.6. 1. Les applications : $f : \mathbb{R} \to \mathbb{R}, x \mapsto \cos x$ et $g : \mathbb{R} \to [-1,1], x \mapsto \cos x$ sont différentes ($f \neq g$), car elles n'ont pas le même ensemble d'arrivée.

2. Les applications : $f : [1, +\infty[\to \mathbb{R}, x \mapsto \sqrt{x}$ et $g : \mathbb{R}^+ \to \mathbb{R}, x \mapsto \sqrt{x}$ sont différentes ($f \neq g$), car elles n'ont pas le même ensemble de départ.

3. Les applications : $f : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$ et $g : \mathbb{R} \to \mathbb{R}, x \mapsto x$ sont différentes ($f \neq g$), car $f(-1) \neq g(-1)$.

4. Les applications : $f : \mathbb{R} \to \mathbb{R}^+, x \mapsto \sqrt{x^2}$ et $g : \mathbb{R} \to \mathbb{R}^+, x \mapsto |x|$ sont égales ($f = g$), car elles ont le même ensemble de départ, le même ensemble d'arrivée et pour tout $x \in \mathbb{R}$, on a $f(x) = \sqrt{x^2} = |x| = g(x)$.

Exercice 8. Soient A et B deux parties d'un ensemble E, et χ_A l'application caractéristique de A. Montrer que :

1. $A \subseteq B \iff \chi_A \leq \chi_B$.
2. $A = B \iff \chi_A = \chi_B$.
3. $\chi_{A\cap B} = \chi_A \chi_B$.
4. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \chi_B$.
5. $\chi_{A\setminus B} = \chi_A(1 - \chi_B)$.
6. $\chi_{A\Delta B} = |\chi_A - \chi_B|$.

Définition 1.11 (**Restriction et prolongement**)**.** Soient A une partie non vide d'un ensemble E et $f : E \to F$ une application. Alors :

1. L'application $g : A \to F$ telle que, pour tout $x \in A$, $g(x) = f(x)$ est appelée la **restriction** de f à A. On la note : $g = f\restriction_A$.
2. Soient G un ensemble contenant E ($G \supset E$) et $f : E \to F$ une application. Toute application $h : G \to F$ telle que $h\restriction_E = f$ est appelée **prolongement** de f à G.

Exemples 1.7. 1. Considérons l'application $f : \mathbb{R} \to \mathbb{R}$, définie par $f(x) = |x|$. On a :

$$f\restriction_{\mathbb{R}^+} : \begin{array}{ccc}\mathbb{R}^+ & \to & \mathbb{R} \\ x & \mapsto & |x| = x\end{array} \quad \text{et} \quad f\restriction_{\mathbb{R}^-} : \begin{array}{ccc}\mathbb{R}^- & \to & \mathbb{R} \\ x & \mapsto & |x| = -x\end{array}$$

L'application f est un **prolongement** à la fois de $f\restriction_{\mathbb{R}^+}$ et de $f\restriction_{\mathbb{R}^-}$.

2. Soit f l'application :

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto \begin{cases} x - 1, & \text{si } x \leqslant -1, \\ x^2, & \text{si } -1 < x \leqslant 1, \\ \ln(x), & \text{si } x > 1. \end{cases}$$

On a :

$$f\restriction_{]-\infty,-1]} :]-\infty,-1] \to \mathbb{R},\ x \mapsto x - 1 \quad f\restriction_{]-1,1]} :]-1,1] \to \mathbb{R},\ x \mapsto x^2 \quad \text{et} \quad f\restriction_{]1,+\infty[} :]1,+\infty[\to \mathbb{R},\ x \mapsto \ln(x)$$

sont les **restrictions** de f, respectivement à $]-\infty,-1]$, $]-1,1]$ et $]1,+\infty[$.

3. Considérons l'application $f : \mathbb{R}^+ \to \mathbb{R}^+$, définie par $f(x) = \sqrt{x}$. L'application

$$g : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto \begin{cases} x - 1, & \text{si } x < 0, \\ \sqrt{x}, & \text{si } x \geqslant 0. \end{cases}$$

est un **prolongement** de f à $\mathbb{R}$, car $g\restriction_{\mathbb{R}^+} = f$.

II.2. Image directe et image réciproque

Définition 1.12. Soient $f : E \to F$ une application, $A \subset E$ et $B \subset F$.

1. On appelle **image directe** (ou tout simplement **image**) de A par f, l'ensemble noté $f(A)$, qui est défini par :
$$f(A) = \{f(x) \mid x \in A\} = \{y \in F \mid \exists\, a \in A, f(a) = y\}.$$

2. On appelle **image réciproque** de B par f, l'ensemble noté $f^{-1}(B)$, qui est défini par :
$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

Autrement dit,

- $y \in f(A) \iff \exists a \in A,\ y = f(a)$,
- $x \in f^{-1}(B) \iff f(x) \in B$.

Remarques 1.4. Sous les mêmes hypothèses de la définition ci-dessus, on a :

1. $f(A) \subset F$ et $f^{-1}(B) \subset E$.
2. $f(A)$ est l'ensemble des images des éléments de A, alors que $f^{-1}(B)$ est l'ensemble des antécédents des éléments de B.
3. Si $A = \{a_1, a_2, \ldots, a_n\}$, alors $f(A) = \{f(a_1), f(a_2), \ldots, f(a_n)\}$.
4. L'image $f(E)$ de E par f est appelée **l'image de** f que l'on note : $f(E) = \operatorname{Im} f$.
5. L'ensemble A est dit **stable** par f si $f(A) \subset A$, et il est dit **invariant** par f si $f(A) = A$.

Exemples 1.8. 1. Considérons l'application $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto 2x - 1$. On pose : $A = \{-2, -1, 0, 1, 2\}$ et $B = \{-1, 1, 2\}$.

(∗) on a : $f(-2) = -5, f(-1) = -3, f(0) = -1, f(1) = 1$ et $f(2) = 3$, donc
$$f(A) = \{f(-2), f(-1), f(0), f(1), f(2)\} = \{-5, -3, -1, 1, 3\}$$

(∗) Déterminons $f^{-1}(B)$, c-à-d cherchons les antécédents des éléments de B :
• Si x est un antécédent de -1, alors $x \in \mathbb{Z}$ et $f(x) = -1$, c-à-d $x \in \mathbb{Z}$ et $2x - 1 = -1$. D'où, $x = 0 \in \mathbb{Z}$.
• Si x est un antécédent de 1, alors $x \in \mathbb{Z}$ et $f(x) = 1$, c-à-d $x \in \mathbb{Z}$ et $2x-1 = 1$. D'où, $x = 1 \in \mathbb{Z}$.
• Si x est un antécédent de 2, alors $x \in \mathbb{Z}$ et $f(x) = 2$, c-à-d $x \in \mathbb{Z}$ et $2x - 1 = 2$.D'où, $x = \frac{3}{2}$ mais, $\frac{3}{2} \notin \mathbb{Z}$.
Il en résulte que 2 n'a pas d'antécédent par f. Ainsi, $f^{-1}(B) = \{0, 1\}$.

2. Soit f l'application :
$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto |x| \end{aligned}$$
Déterminons $f([-1,1])$ et $f^{-1}([1,4])$.

(∗)
$$\begin{aligned} y \in f([-1,1]) &\Leftrightarrow \exists\, x \in [-1,1], y = f(x) \\ &\Leftrightarrow \exists\, x \in [-1,1], y = |x| \\ &\Leftrightarrow 0 \leqslant y \leqslant 1 \\ &\Leftrightarrow y \in [0,1]. \text{ Alors } f([-1,1]) = [0,1]. \end{aligned}$$

(∗∗)
$$\begin{aligned} x \in f^{-1}([1,4]) &\Leftrightarrow f(x) \in [1,4] \\ &\Leftrightarrow 1 \leqslant |x| \leqslant 4 \\ &\Leftrightarrow (x \in]-\infty,-1] \cup [1,+\infty[) \text{ et } (x \in [-4,4]) \\ &\Leftrightarrow x \in [-4,-1] \cup [1,4]. \text{ D'où } f^{-1}([1,4]) = [-4,-1] \cup [1,4]. \end{aligned}$$

Proposition 1.7. *Soient A, B deux parties d'un ensemble E et $f : E \to F$ une application. Alors, les assertions suivantes sont vraies :*

1. $f(\emptyset) = \emptyset$.
2. *si $A \subset B$, alors $f(A) \subset f(B)$.*
3. $f(A \cup B) = f(A) \cup f(B)$. *Plus généralement, si $(A_i)_{i\in I}$ est une famille de parties de E, alors*
$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i).$$
4. $f(A \cap B) \subset f(A) \cap f(B)$. *Plus généralement, si $(A_i)_{i\in I}$ est une famille de parties de E, alors*
$$f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i).$$

Démonstration. À faire à titre d'exercice □

Proposition 1.8. *Soient A, B deux parties d'un ensemble F et $f : E \to F$ une application. Alors, les assertions suivantes sont vraies :*

1. $f^{-1}(\emptyset) = \emptyset$.
2. $f^{-1}(F) = E$.
3. *si $A \subset B$, alors $f^{-1}(A) \subset f^{-1}(B)$.*
4. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$. *Plus généralement, si $(B_i)_{i\in I}$ est une famille de parties de F, alors*
$$f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i).$$

5. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. *Plus généralement, si* $(B_i)_{i\in I}$ *est une famille de parties de* F*, alors*

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

Démonstration. À faire à titre d'exercice □

Exercice 9. Soit $f : E \to F$ une application. Montrer que pour toute partie B de F :

$$f^{-1}(\complement_F B) = \complement_E f^{-1}(B).$$

II.3. Composition des applications

Définition 1.13. Soient $f : E \to F$ et $g : F \to G$ deux applications. La **composée** de f par g est l'application $g \circ f : E \to G$ définie par : $(g \circ f)(x) = g(f(x))$, pour tout $x \in E$.

$$E \xrightarrow{f} F \xrightarrow{g} G$$

$$x \longrightarrow f(x) \longrightarrow g(f(x))$$

$$g \circ f$$

Exemple 1.4. Considérons les applications $f : \mathbb{R} \to \mathbb{R}^+, x \mapsto x^2$ et $g : \mathbb{R}^+ \to \mathbb{R}, x \mapsto \sqrt{x}$.

- La composée de f par g est l'application $g \circ f : \mathbb{R} \to \mathbb{R}$ telle que :

$$(\forall x \in \mathbb{R})\ (g \circ f)(x) = g(f(x)) = g(x^2) = \sqrt{x^2} = |x|.$$

D'où, $g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$.

- La composée de g par f est l'application $f \circ g : \mathbb{R}^+ \to \mathbb{R}^+$ telle que :

$$(\forall x \in \mathbb{R}^+)\ (f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = \sqrt{x}^2 = x.$$

D'où, $f \circ g : \mathbb{R}^+ \to \mathbb{R}^+, x \mapsto x$ ou encore, $f \circ g = id_{\mathbb{R}^+}$.

Remarques 1.5. 1. Soient $f : E \to F$ et $g : H \to G$ deux applications. Si on suppose que $f(E) \subset H$, alors $g \circ f$ est bien définie et on a $g \circ f : E \to G, x \mapsto (g \circ f)(x) = g(f(x))$.

$$E \xrightarrow{f} f(E) \subset H \xrightarrow{g} G$$

$$x \longrightarrow f(x) \longrightarrow g(f(x))$$

$$g \circ f$$

2. En général, $f \circ g \neq g \circ f$ lorsque $f \circ g$ et $g \circ f$ sont définies. Parfois $f \circ g$ n'est même pas définie quand $g \circ f$ l'est. Par exemple : Dans l'exemple ci-dessus, on a $f \circ g \neq g \circ f$.

Proposition 1.9. *Soient $f : E \to F$, $g : F \to G$ et $h : G \to H$ des applications. On a :*

1. *$id_F \circ f = f$ et $f \circ id_E = f$.*
2. *$(h \circ g) \circ f = h \circ (g \circ f)$.*

Démonstration. À faire à titre d'exercice □

Exemple 1.5. Considérons les applications suivantes :

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & 1+x^2 \end{array}, \quad g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & \sqrt{x} \end{array} \text{ et } \quad h : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln(1+x) \end{array}$$

On a donc :

$$h \circ g \circ f(x) = h(g(f(x))) = h(g(1+x^2)) = h\left(\sqrt{1+x^2}\right) = \ln\left(1+\sqrt{1+x^2}\right).$$

Proposition 1.10. *Soit $f : E \to F$ une application. On a :*

1. *pour toute partie A de E, $f^{-1}(f(A)) \supseteq A$.*
2. *pour toute partie B de F, $f(f^{-1}(B)) \subset B$.*

Démonstration. 1) Pour tout $x \in A$, on a $f(x) \in f(A)$, donc $x \in f^{-1}(f(A))$. D'où, $A \subset f^{-1}(f(A))$.

2) Soit $y \in f(f^{-1}(B))$, donc il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. Comme $x \in f^{-1}(B)$, alors $f(x) \in B$, c'est-à-dire $y \in B$. D'où, $f(f^{-1}(B)) \subset B$. □

Remarque 1.7. Soit $f : E \to E$ une application. Pour $n \geqslant 2$ un entier, la composée $\underbrace{f \circ f \circ \ldots \circ f}_{n \text{ fois}}$ est bien définie et on la note

$$f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ fois}}.$$

Ainsi, $f^2 = f \circ f$, $f^3 = f \circ f \circ f$, etc.

II.4. Injection, surjection et bijection

Définition 1.14. Soient E et F deux ensembles et soit $f : E \to F$ une application.

1. On dit que f est une application **injective** ou une **injection** si deux éléments quelconques et distincts de E admettent des images distinctes par f.
2. On dit que f est une application **surjective** ou une **surjection** si tout élément de F admet au moins un antécédent par f dans E.
3. On dit que f est une application **bijective** ou une **bijection** si f est à la fois injective et surjective.

Ce qui revient à dire,

1.
$$f \text{ est injective } \Leftrightarrow (\forall x, x' \in E), \quad x \neq x' \Rightarrow f(x) \neq f(x'),$$
ou encore, par contraposée,
$$f \text{ est injective } \Leftrightarrow (\forall x, x' \in E), \quad f(x) = f(x') \Rightarrow x = x'.$$

2.
$$f \text{ est surjectuive } \Leftrightarrow (\forall y \in F)(\exists\, x \in E) \text{ tel que } f(x) = y.$$

Proposition 1.11. *Une application $f : E \to F$ est bijective, si et seulement si, tout élément de F admet un et un seul antécédent dans E par f. Autrement dit,*
$$f \text{ est bijective } \Leftrightarrow (\forall y \in F)(\exists! x \in E) : y = f(x).$$

Démonstration. Supposons que f soit bijective. Alors f est surjective, donc pour tout $y \in F$ il existe au moins un $x \in E$ tel que $y = f(x)$. S'il existe un autre élément $x' \in E$ tel que $y = f(x')$, alors $f(x) = f(x')$. Comme f est bijective, en particulier f est injective, alors $x = x'$. Donc, pour tout $y \in F$, il existe un et un seul $x \in E$ tel que $y = f(x)$.

Réciproquement, Soit $y \in F$ il existe un et un seul (donc au moins) $x \in E$ tel que $y = f(x)$. Cela signifie que f est surjective. Concernant l'injectivité de f, supposons qu'il existe $x \neq x' \in E$ tels que $f(x) = f(x')$. On pose $y = f(x) = f(x')$, alors l'élément $y \in F$ admet deux antécédents distincts x et x', ce qui contredit l'unicité de l'antécédent de tout élément de F par f. Donc, f est injective. □

Exemples 1.9.
1. L'application $f : \mathbb{R}^+ \to \mathbb{R}^+$ définie par $x \mapsto x^2$ est injective et surjective, donc bijective.
2. L'application $f : \mathbb{R} \to \mathbb{R}^+, x \mapsto x^2$ n'est pas injective mais elle est surjective (par conséquent, elle n'est pas bijective).
3. L'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est ni injective ni surjective, car $f(1) = f(-1)$, $1 \neq -1$ et -1 n'admet pas d'antécédent, donc elle n'est pas bijective.

Remarques 1.6.
1. Une application $f : E \to F$ est surjective si et seulement si
$$f(E) = F.$$
2. Pour toute partie non vide A de E, l'application $i : A \to E, x \mapsto x$ est injective. On l'appelle **l'injection canonique**.

Proposition 1.12. *La composée de deux injections (resp. surjections, bijections) est une injection (resp. surjection, bijection).*

Démonstration. Soient $f : E \to F$ et $g : F \to G$ deux applications :
$$E \xrightarrow{f} F \xrightarrow{g} G$$
$$x \longrightarrow f(x) \longrightarrow g(f(x))$$
$$g \circ f$$

1. Supposons que f et g soient des applications injectives. Pour tous $x, x' \in E$, on a :

$$\begin{aligned} g \circ f(x) = g \circ f(x') &\Rightarrow g(f(x)) = g(f(x')) \\ &\Rightarrow f(x) = f(x') \text{ (car } g \text{ est injective)} \\ &\Rightarrow x = x' \text{ (car } f \text{ est injective).} \end{aligned}$$

   Donc $g \circ f$ est injective.

2. Supposons que f et g soient des applications surjectives. Alors,

$$\begin{aligned} g \circ f(E) = g(f(E)) &= g(F) \text{ (car } f \text{ est surjective)} \\ &= G \quad \text{(car } g \text{ est surjective).} \end{aligned}$$

3. Si f et g sont bijectives, alors f et g sont à la fois injectives et surjectives. Par suite, $g \circ f$ est à la fois injective et surjective. Donc $g \circ f$ est bijective.

□

Proposition 1.13. *Soient $f : E \to F$ et $g : F \to G$ deux applications.*

1) *Si $g \circ f$ est injective, alors f est injective.*

2) *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration. 1) Supposons que $g \circ f$ soit injective. Pour tous $x, x' \in E$ tels que $f(x) = f(x')$, on a $g(f(x)) = g(f(x'))$ (car g est une application), ainsi $g \circ f(x) = g \circ f(x')$. Comme $g \circ f$ est injective, alors $x = x'$. Donc, f est injective.

2) Supposons que $g \circ f$ soit surjective. Pour tout $z \in G$, il existe $x \in E$ tel que $g \circ f(x) = z$, or $g(f(x)) = z$. Pour $y = f(x) \in F$, on a $g(y) = z$. Par suite, $(\forall z \in G)(\exists y = f(x) \in F)$ tel que $g(y) = z$. Il s'ensuit que g est surjective.

□

Théorème 1.1. *Soit $f : E \to F$ une application. Pour que f soit bijective, il faut et il suffit qu'il existe une application $g : F \to E$ telle que*

$$g \circ f = id_E \text{ et } f \circ g = id_F.$$

Démonstration. Si f est bijective, alors pour tout $y \in F$, il existe un et un seul $x \in E$ tel que $y = f(x)$. Soit g la correspondance de F vers E telle que $g(y) = x$. Par construction, g est une application de F vers E et pour tout $y \in F$,

$$f \circ g(y) = f(g(y)) = f(x) = y, \quad \text{c'est-à-dire} \quad f \circ g = \mathrm{id}_F.$$

De plus, si $x \in E$, $g(f(x))$ est un antécédent de $f(x)$ par f, mais comme il n'y en a qu'un, $g(f(x)) = x$, pour tout $x \in E$. Il vient que

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

Réciproquement, supposons qu'il existe une application $g : F \to E$ vérifiant $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$, alors $g \circ f$ et $f \circ g$ sont bijectives (car id_E et id_F sont des bijections). En particulier, $g \circ f$ est injective et $f \circ g$ est surjective. La proposition précédente entraîne que f est à la fois injective et surjective. Donc f est bijective. □

Remarques 1.7. 1. Il est facile de déduire que l'application g (du théorème) est unique et est bijective. On l'appelle la bijection réciproque (ou l'application réciproque) de f, et on la note $g = f^{-1}$. De plus,

$$g^{-1} = (f^{-1})^{-1} = f$$

.

2. Si $f : E \to F$ est une bijection, alors $\forall x \in E, \forall y \in F, f(x) = y \Leftrightarrow x = f^{-1}(y)$.

Corollaire 1.1. *Si $f : E \to F$ et $g : F \to C$ sont deux applications bijectives, alors $g \circ f : E \to C$ est une application bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration. Puisque f et g sont des applications bijectives, alors $g \circ f$ est bijective. De plus,

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_F \circ f = f^{-1} \circ f = \mathrm{id}_E.$$

De même,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_E \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_G.$$

□

Remarque 1.8. Toute application $f : E \to E$ telle que $f \circ f = \mathrm{id}_E$ est bijective (appelée une involution sur E). Sa bijection réciproque est $f^{-1} = f$.

Exercice 10. 1. Soit l'application f définie par

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{x(1-x)^2}{(1+x^2)^2}. \end{aligned}$$

(a) Montrer que $f\left(\frac{1}{x}\right) = f(x)$, pour tout $x \in \mathbb{R}^*$. Conclure.

(b) Montrer que $f(x) \leq \frac{1}{4}$, pour tout $x \in \mathbb{R}$. Conclure.

2. Soit E un ensemble non vide et $f : \mathcal{P}(E) \longrightarrow \mathcal{P}(E)$ définie par $A \longmapsto A^c$. Montrer que f est bijective et déterminer sa bijection réciproque f^{-1}.

3. Montrer que l'application $f : [1, +\infty[\to \mathbb{R}^+$ définie par

$$x \longmapsto \sqrt{x-1}$$

est bijective et déterminer sa bijection réciproque.

4. Soit $f : E \to F$ une application.

(a) Montrer que les assertions suivantes sont équivalentes :

(i) f est injective.

(ii) $\forall A, B \in \mathcal{P}(E), f(A \cap B) = f(A) \cap f(B)$.

(iii) $\forall A \in \mathcal{P}(E), A = f^{-1}(f(A))$.

(b) Montrer que f est surjective si et seulement si, pour tout $B \in \mathcal{P}(F), f(f^{-1}(B)) = B$.

5. L'exercice 6 du TD.

III. Relations binaires

III.1. Définitions et exemples

Définition 1.15. Une **relation binaire** sur un ensemble non vide E est une correspondance $\mathcal{R}$ de E vers E, c'est-à-dire, $\mathcal{R} = (E, E, G)$, où G est une partie de $E \times E$.

Notation. Soit $\mathcal{R} = (E, E, G)$ une relation binaire sur E. Si $(x, y) \in G$, avec $x, y \in E$, on dit que l'élément x est **en relation** avec l'élément y (dans cet ordre), et on écrit : $x\mathcal{R}y$.

Exemples 1.10.

1. La relation $\mathcal{R}$ définie sur $\mathbb{R}$ par :
$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x = y.$$
2. La relation $\mathcal{R}$ définie sur $\mathbb{R}$ par :
$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x \leq y.$$
3. La relation $\mathcal{R}$ définie sur $\mathbb{Z}$ par :
$$\forall n, m \in \mathbb{Z}, \quad n\mathcal{R}m \Leftrightarrow n \text{ divise } m.$$
4. La relation $\mathcal{R}$ définie sur $\mathbb{Z} \times \mathbb{N}^*$ par :
$$\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^*, \quad \forall (p', q') \in \mathbb{Z} \times \mathbb{N}^*, \quad (p, q)\mathcal{R}(p', q') \Leftrightarrow pq' = qp'.$$
5. La relation $\mathcal{R}$ définie sur $\mathcal{P} \times \mathcal{P}$ (où $\mathcal{P}$ est un plan) par :
$$\forall (A, B), (C, D) \in \mathcal{P} \times \mathcal{P}, \quad (A, B)\mathcal{R}(C, D) \Leftrightarrow [AD] \text{ et } [BC] \text{ ont même milieu.}$$
6. La relation $\mathcal{R}$ définie sur l'ensemble $\mathcal{D}$ des droites du plan par :
$$\forall (D), (\Delta) \in \mathcal{D}, \quad (D)\mathcal{R}(\Delta) \Leftrightarrow (D) \parallel (\Delta).$$
7. La relation $\mathcal{R}$ définie sur $\mathcal{P}(E)$ par :
$$\forall A, B \in \mathcal{P}(E), \quad A\mathcal{R}B \Leftrightarrow A \subset B.$$

Définition 1.16. Soit $\mathcal{R}$ une relation binaire définie sur un ensemble E. Nous disons que :

1. La relation $\mathcal{R}$ est **réflexive** si
$$\forall x \in E, \quad x\mathcal{R}x.$$
2. La relation $\mathcal{R}$ est **symétrique** si
$$\forall x, y \in E, \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

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

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

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

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

Exemples 1.11. Sur l'ensemble $\mathbb{Z}$, considérons les relations binaires $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4$ et $\mathcal{R}_5$ définies par :

$$\begin{aligned} \forall x, y \in \mathbb{Z}, \quad & x\mathcal{R}_1 y \Leftrightarrow x \leq y, \\ & x\mathcal{R}_2 y \Leftrightarrow x = y, \\ & x\mathcal{R}_3 y \Leftrightarrow x = y + 1, \\ & x\mathcal{R}_4 y \Leftrightarrow x + y \leq 3, \\ & x\mathcal{R}_5 y \Leftrightarrow x^2 = y^2. \end{aligned}$$

On a :

- $\mathcal{R}_1$ est réflexive, antisymétrique et transitive, mais non symétrique (par exemple, $2\mathcal{R}_1 3$ mais 3 n'est pas en relation avec 2 ($3 \not\leq 2$).
- $\mathcal{R}_2$ est réflexive, symétrique, antisymétrique et transitive.
- $\mathcal{R}_3$ n'est ni réflexive, ni symétrique, ni antisymétrique, ni transitive.
- $\mathcal{R}_4$ n'est ni réflexive, ni antisymétrique et ni transitive mais $\mathcal{R}_4$ est symétrique.
- $\mathcal{R}_5$ est réflexive, symétrique et transitive mais elle n'est pas antisymétrique.

III.2. Relations d'équivalence

Définition 1.17. On dit qu'une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'**équivalence** si elle est réflexive, symétrique et transitive.

Exemples 1.12. (1) La relation d'égalité, définie sur $\mathbb{R}$, est une relation d'équivalence. En effet :

(a) Réflexivité : $\forall x \in \mathbb{R}, \quad x = x$.

(b) Symétrie : $\forall x, y \in \mathbb{R}, \quad x = y \Rightarrow y = x$.

(c) Transitivité : $\forall x, y, z \in \mathbb{R}, \quad (x = y \text{ et } y = z) \Rightarrow x = z$.

(2) La relation "$\leqslant$" n'est pas une relation d'équivalence sur $\mathbb{R}$, car elle n'est pas symétrique. Par exemple, bien que $2 \leqslant 3$, il n'est pas vrai que $3 \leqslant 2$.

Exercice 11. Parmi les exemples 1.11 de la sous-section III.1, déterminer les relations qui sont des relations d'équivalence.

Définition 1.18. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Pour un élément a de E, on appelle **classe d'équivalence** de a (modulo $\mathcal{R}$) ou tout simplement classe de a, le sous-ensemble de E, noté $\overline{a}$, défini par : $\overline{a} = \{x \in E \mid x\mathcal{R}a\}$. On la note aussi $\dot{a}$ ou encore $cl(a)$. L'ensemble des classes d'équivalence modulo $\mathcal{R}$, noté $E/\mathcal{R}$, est appelé **l'ensemble quotient** de E par $\mathcal{R}$ ou simplement ensemble quotient, c'est-à-dire,

$$E/\mathcal{R} = \{\overline{a} \mid a \in E\}.$$

Exemples 1.13. 1. Soit $E = \{1, 2, 3, 4\}$ et $\mathcal{R}$ la relation binaire définie sur E par son graphe :

$$G = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4)\}.$$

(a) La relation $\mathcal{R}$ est une relation d'équivalence. On vérifie facilement que :

- $x\mathcal{R}x$ pour tout $x \in E$ (réflexivité),
- Si $x\mathcal{R}y$, alors $y\mathcal{R}x$ pour tous $x, y \in E$ (symétrie),
- Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$ pour tous $x, y, z \in E$ (transitivité).

Les classes d'équivalence de E modulo $\mathcal{R}$ sont $\{\overline{1}, \overline{3}\} = \{\{1,2\}, \{3,4\}\}$, car

$$\overline{1} = \{x \in E \mid x\mathcal{R}1\} = \{1,2\}.$$

$$\overline{2} = \{x \in E \mid x\mathcal{R}2\} = \{1,2\}.$$

$$\overline{3} = \{x \in E \mid x\mathcal{R}3\} = \{3,4\}.$$

$$\overline{4} = \{x \in E \mid x\mathcal{R}4\} = \{3,4\}.$$

2. Soit $\mathcal{R}$ la relation binaire définie sur $\mathbb{R}$ par

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x^2 = y^2.$$

(a) La relation $\mathcal{R}$ est réflexive. En effet, pour tout $x \in \mathbb{R}$, on a $x^2 = x^2$, donc $x\mathcal{R}x$.

(b) La relation $\mathcal{R}$ est symétrique. En effet, pour tous $x, y \in \mathbb{R}$, on a :

$$x\mathcal{R}y \Rightarrow x^2 = y^2$$
$$\Rightarrow y^2 = x^2$$
$$\Rightarrow y\mathcal{R}x.$$

(c) La relation $\mathcal{R}$ est transitive. En effet, pour tous $x, y, z \in \mathbb{R}$, on a :

$$(x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x^2 = y^2 \text{ et } y^2 = z^2$$
$$\Rightarrow x^2 = z^2$$
$$\Rightarrow x\mathcal{R}z.$$

Cette relation est réflexive, symétrique et transitive, donc est une relation d'équivalence. Déterminons l'ensemble quotient. Soit $x \in \mathbb{R}$,

$$y \in \overline{x} \Leftrightarrow y\mathcal{R}x \Leftrightarrow y^2 = x^2 \Leftrightarrow y = x \text{ ou } y = -x \Leftrightarrow y \in \{x, -x\}.$$

D'où, pour tout $x \in \mathbb{R}$, $\overline{x} = \{x, -x\}$ et l'ensemble quotient est

$$\mathbb{R}/\mathcal{R} = \{\{x, -x\} \mid x \in \mathbb{R}\}.$$

3. Soit " $\sim$ " la relation binaire définie sur $\mathcal{P} \times \mathcal{P}$ (où $\mathcal{P}$ est un plan) par :

   $\forall (A,B),(C,D) \in \mathcal{P}\times\mathcal{P}, \quad (A,B) \sim (C,D) \Leftrightarrow$ les milieux de $[AD]$ et $[BC]$ sont identiques.

   Cette relation est réflexive, symétrique, et transitive, formant ainsi une relation d'équivalence sur $\mathcal{P} \times \mathcal{P}$. La classe d'équivalence du bipoint (A,B) est le vecteur $\overrightarrow{AB}$, et l'ensemble quotient $\mathcal{P} \times \mathcal{P}/\sim$ représente le plan vectoriel.

Exercice 12. 1. Soit $\mathcal{R}$ la relation définie sur $\mathbb{C}$ par

$$z\mathcal{R}z' \Leftrightarrow |z| = |z'|$$

   Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{C}$ et déterminer l'ensemble quotient.

2. Soit A une partie non vide d'un ensemble E. On définit sur $\mathcal{P}(E)$ la relation binaire $\mathcal{R}$ par :

$$\forall X, Y \in \mathcal{P}(E), X\mathcal{R}Y \Leftrightarrow A \cap X = A \cap Y.$$

   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathcal{P}(E)$.

   (b) Déterminer $\overline{\emptyset}$, $\overline{E}$, $\overline{A}$ et $\overline{C_E^A}$.

Remarques 1.8. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Alors :

1. Pour tout $x \in E$, $x \in \overline{x}$ (car $x\mathcal{R}x$). Un élément qui appartient à $\overline{x}$ est appelé un représentant de $\overline{x}$.

2. Pour tous $x, y \in E$, on a :

$$x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}.$$

Proposition 1.14. *Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, alors la famille $(\overline{x})_{\overline{x}\in E/\mathcal{R}}$ forme une partition de E.*

Démonstration. (i) On a $\forall \overline{x} \in E/\mathcal{R}$, $\overline{x} \neq \emptyset$ (car $x \in \overline{x}$, pour tout $x \in \overline{x}$).

(ii) Soient $\overline{x}$ et $\overline{y}$ deux éléments distincts de $E/\mathcal{R}$ ($\overline{x} \neq \overline{y}$). Montrons que $\overline{x} \cap \overline{y} = \emptyset$. Supposons qu'il existe $z \in \overline{x} \cap \overline{y}$, alors $z \in \overline{x}$ et $z \in \overline{y}$, c'est-à-dire $\overline{z} = \overline{x}$ et $\overline{z} = \overline{y}$, ce qui contredit $\overline{x} \neq \overline{y}$. Donc $\overline{x} \cap \overline{y} = \emptyset$.

(iii) Montrons que $E = \bigcup\limits_{\overline{x}\in E/\mathcal{R}} \overline{x}$. On a $\forall \overline{x} \in E/\mathcal{R}, \overline{x} \subset E$, donc $\bigcup\limits_{\overline{x}\in E/\mathcal{R}} \overline{x} \subset E$. Pour l'autre inclusion, soit $x \in E$, donc $x \in \overline{x}$, par suite $x \in \bigcup\limits_{\overline{x}\in E/\mathcal{R}} \overline{x}$. Donc $E \subset \bigcup\limits_{\overline{x}\in E/\mathcal{R}} \overline{x}$. Par conséquent, $E = \bigcup\limits_{\overline{x}\in E/\mathcal{R}} \overline{x}$.

□

Exercice 13. (Exercice 10 du TD).

Remarque 1.9. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Par construction, l'application $\pi : E \to E/\mathcal{R}$, $x \mapsto \overline{x}$ est surjective. On l'appelle **la surjection canonique**.

Théorème 1.2 (Décomposition canonique d'une application)**.** *Soit $f : E \to F$ une application.*

(1) *La relation binaire $\mathcal{R}$ définie sur E par :*

$$\forall x, y \in E, \quad x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$$

est une relation d'équivalence.

(2) *Il existe une unique application bijective $\overline{f} : E/\mathcal{R} \to f(E)$ telle que $f = i \circ \overline{f} \circ \pi$, où $i : f(E) \to F$ est l'injection canonique définie par $y \mapsto y$ et $\pi : E \to E/\mathcal{R}$ est la surjection canonique définie par $x \mapsto \overline{x}$.*

Remarque 1.10. La décomposition canonique de f peut être schématisée de la manière suivante :

$$\begin{array}{ccccccc} E & \xrightarrow{\pi} & E/\mathcal{R} & \xrightarrow{\overline{f}} & f(E) & \xrightarrow{i} & F \\ \multicolumn{7}{c}{\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{f = i \circ \overline{f} \circ \pi}} \end{array}$$

ou encore par le digramme commutative suivant :

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ E/\mathcal{R} & \xrightarrow{\overline{f}} & f(E) \end{array}$$

Démonstration. (1) Il est facile de vérifier que $\mathcal{R}$ est une relation d'équivalence sur E.
(2) • La correspondance $\overline{f} : E/\mathcal{R} \to f(E), \overline{x} \mapsto f(x)$ est bien définie (i.e., $\overline{f}$ est une application). En effet, soient $\overline{x}$ et $\overline{y}$ deux éléments de $E/\mathcal{R}$, on a :

$$\overline{x} = \overline{y} \Rightarrow x\mathcal{R}y \Rightarrow f(x) = f(y) \Rightarrow \overline{f}(\overline{x}) = \overline{f}(\overline{y}) \text{ (car } \overline{f}(\overline{x}) = f(x) \text{ et } \overline{f}(\overline{y}) = f(y).$$

Donc, $\overline{f}$ est bien définie.
• De plus, $\overline{f}$ vérifie : $f = i \circ \overline{f} \circ \pi$. En effet, pour tout $x \in E$, on a :

$$i \circ \overline{f} \circ \pi(x) = i \circ \overline{f}(\overline{x}) = i(f(x)) = f(x).$$

Donc, $f = i \circ \overline{f} \circ \pi$.
• Unicité de $\overline{f}$ telle que $f = i \circ \overline{f} \circ \pi$. Supposons qu'il existe une autre application $g : E/\mathcal{R} \to f(E)$ telle que $f = i \circ g \circ \pi$. Puisque $f = i \circ g \circ \pi$ et $f = i \circ \overline{f} \circ \pi$, alors

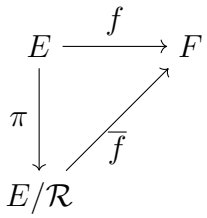
$$\forall x \in E, (i \circ g \circ \pi)(x) = (i \circ \overline{f} \circ \pi)(x).$$

Donc $i(g \circ \pi(x)) = i(\overline{f} \circ \pi(x))$, par suite $g(\overline{x}) = \overline{f}(\overline{x})$ (car i est injective), c'est-à-dire $g = \overline{f}$.
• $\overline{f}$ est injective. En effet, pour tous $x, y \in E$:

$$\overline{f}(\overline{x}) = \overline{f}(\overline{y}) \Rightarrow f(x) = f(y) \Rightarrow x\mathcal{R}y \Rightarrow \overline{x} = \overline{y}.$$

$\overline{f}$ est surjective. En effet, pour tout $y \in f(E)$, il existe $x \in E$ tel que $y = f(x)$, c'est-à-dire $y = \overline{f}(\overline{x})$. Donc, $(\forall\, y \in f(E))(\exists\, \overline{x} \in E/\mathcal{R}) : y = \overline{f}(\overline{x})$. Donc $\overline{f}$ est bijective. □

Remarque 1.11. Si f est une application surjective, alors $f(E) = F$ et l'injection canonique $i : f(E) \to F$ n'est autre que l'application identité $\mathrm{id}_F : F \to F$. Par conséquent, la décomposition canonique de l'application $f : E \to F$ sera $f = \overline{f} \circ \pi$, avec $\pi : E \to E/\mathcal{R}$ la surjection canonique et $\overline{f} : E/\mathcal{R} \to F$ est la bijection telle que $f = \overline{f} \circ \pi$.



Exemple 1.6. On considère l'application $f : \mathbb{R} \to \mathbb{R}$, définie par $f(x) = x^2$. La relation d'équivalence associée à f est définie par :

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x^2 = y^2.$$

On sait que $\forall x \in \mathbb{R}, \overline{x} = \{x, -x\}$ (voir Exemple 2, page 24). La décomposition canonique de f est donnée par $f = i \circ \overline{f} \circ \pi$, où :

- $i : f(\mathbb{R}) = \mathbb{R}^+ \to \mathbb{R}$ est l'injection canonique,
- $\pi : \mathbb{R} \to \mathbb{R}/\mathcal{R} = \{\{x, -x\} \mid x \in \mathbb{R}\}$ est la surjection canonique, définie par

$$\pi(x) = \overline{x} = \{x, -x\},$$

- $\overline{f} : \mathbb{R}/\mathcal{R} \to f(\mathbb{R}) = \mathbb{R}^+$ est la fonction bijective, définie par

$$\overline{f}(\{x, -x\}) = f(x) = x^2.$$

Exercice 14. Soit $\mathcal{R}$ la relation binaire définie sur $\mathbb{Z} \times \mathbb{Z}^*$ par :

$$\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}^*, \forall (x', y') \in \mathbb{Z} \times \mathbb{Z}^*, \quad (x, y)\mathcal{R}(x', y') \Leftrightarrow xy' = yx'.$$

(1) Montrer que $\mathcal{R}$ est une relation d'équivalence.

(2) Montrer que l'ensemble quotient $\mathbb{Z} \times \mathbb{Z}^*/\mathcal{R}$ est en bijection avec $\mathbb{Q}$.

III.3. Relations d'ordre

Définition 1.19. Une relation binaire $\mathcal{R}$ sur un ensemble E est dite une **relation d'ordre** (ou un **ordre**) sur E si $\mathcal{R}$ est réflexive, antisymétrique et transitive.

Notation. En général, une relation d'ordre sera notée " $\leq$ ".

Remarques 1.9. (1) Si $\leq$ est un ordre sur E, le couple $(E, \leq)$ est dit un **ensemble ordonné**.

(2) Une relation binaire sur E qui est réflexive et transitive est dite un **préordre** sur E.

Exemples 1.14. (1) La relation binaire $\leq$ définie sur $\mathbb{R}$ par :

$$\forall x, y \in \mathbb{R}, \quad x \leq y \Leftrightarrow y - x \in \mathbb{R}^+,$$

est une relation d'ordre sur $\mathbb{R}$, donc $(\mathbb{R}, \leq)$ est un ensemble ordonné. De même, $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$ et $(\mathbb{Q}, \leq)$ sont des ensembles ordonnés.

(2) Soit E un ensemble non vide. La relation binaire définie sur $\mathcal{P}(E)$ par :

$$\forall A, B \in \mathcal{P}(E), \quad A \leq B \Leftrightarrow A \subseteq B,$$

est une relation d'ordre sur $\mathcal{P}(E)$. Donc $(\mathcal{P}(E), \subseteq)$ est un ensemble ordonné.

(3) La relation $\leq$ définie sur $\mathbb{C}$ par :

$$\forall z, z' \in \mathbb{C}, \quad z \leq z' \Leftrightarrow |z| \leq |z'|,$$

est un préordre.

(4) La relation $\leq$ définie sur $\mathbb{N}^*$ par :

$$\forall n, m \in \mathbb{N}^*, \quad n \leq m \Leftrightarrow n \mid m \quad (n \text{ divise } m),$$

est une relation d'ordre sur $\mathbb{N}^*$.

Définition 1.20. Soit $\leq$ un **ordre** sur un ensemble E.

(1) On dit que $\leq$ est un **ordre total** si deux éléments quelconques de E sont comparables, c'est-à-dire, $\forall x, y \in E, \quad x \leq y$ ou $y \leq x$. Dans ce cas, on dit que $(E, \leq)$ est un **ensemble totalement ordonné**.

(2) Si l'ordre $\leq$ n'est pas total, on dit que $\leq$ est un **ordre partiel**, c'est-à-dire, il existe $x, y \in E$ tels que $x \not\leq y$ et $y \not\leq x$. Dans ce cas, on dit que $(E, \leq)$ est un **ensemble partiellement ordonné**.

Exemples 1.15. (1) $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ et $(\mathbb{R}, \leq)$ sont des ensembles totalement ordonnés.

(2) Si E contient au moins deux éléments distincts, alors $(\mathcal{P}(E), \subseteq)$ est un ensemble partiellement ordonné. Par exemple, soit $E = \{1, 2, 3\}$. On sait que $(\mathcal{P}(E), \subseteq)$ est un ensemble ordonné, et puisque $\{1\} \not\subseteq \{2\}$ et $\{2\} \not\subseteq \{1\}$, alors $(\mathcal{P}(E), \subseteq)$ est un ensemble partiellement ordonné.

(3) La relation "divise" $(|)$ est un ordre partiel sur $\mathbb{N}^*$, car $2 \nmid 3$ et $3 \nmid 2$.

Exercice 15. Soient deux relations binaires $\mathcal{R}_1$ et $\mathcal{R}_2$ définies sur $\mathbb{R}^2$ de la manière suivante :

$$\begin{aligned} &\forall (x, y), (x', y') \in \mathbb{R}^2, \\ &\quad (x, y)\mathcal{R}_1(x', y') \Leftrightarrow x \leq x' \text{ et } y \leq y', \\ &\quad (x, y)\mathcal{R}_2(x', y') \Leftrightarrow x < x' \text{ ou } (x = x' \text{ et } y \leq y'). \end{aligned}$$

Montrer que :

- $\mathcal{R}_1$ est un **ordre partiel** sur $\mathbb{R}^2$.
- $\mathcal{R}_2$ est un **ordre total** sur $\mathbb{R}^2$.

IV. Arithmétique de $\mathbb{Z}$

IV.1. Divisibilité et division euclidienne

IV.1.1. Divisibilité et Propriétés de base

Définition 1.21. Soient $m \in \mathbb{Z}$ et $n \in \mathbb{Z} \setminus \{0\}$. On dit que m est **divisible** par n ou que n **divise** m s'il existe $k \in \mathbb{Z}$ tel que $m = kn$ (i.e. $\frac{m}{n}$ est un entier). On dit aussi que m est un **multiple** de n et que n est un **diviseur** de m. Si n divise m, on écrit $n \mid m$. Sinon, on écrit $n \nmid m$.

Exemple 1.7. On a $5 \mid 30$, $-12 \mid 48$, $-10 \mid 100$ et $-4 \mid -20$; mais $3 \nmid 4$.

Remarques 1.10.
1. Tout entier a est divisible par 1 et -1, car $a = 1 \cdot a$ et $a = (-1) \cdot (-a)$.
2. 0 est divisible par tous les entiers car $0 = a \cdot 0$, pour tout $a \in \mathbb{Z}$.

Proposition 1.15. *Soient x, y et z des entiers. On a :*

1. *$x \mid x$ (on dit que la relation binaire $\mid$ est réflexive) ;*
2. *Si $x \mid y$ et $y \mid z$ alors $x \mid z$ (on dit que la relation binaire $\mid$ est transitive) ;*
3. *Si $x \mid y$ et $x \mid z$ alors $x \mid \alpha y + \beta z$ pour tous $\alpha, \beta \in \mathbb{Z}$;*
4. *Si $x \mid y$ et $y \mid x$ alors $\mid x \mid = \mid y \mid$;*
5. *Si x et y sont deux entiers tels que $x^n \mid y^n$ pour un entier $n \geq 1$, alors $x \mid y$;*

Démonstration. Pour (1) on a pour tout $x \in \mathbb{Z}$, $x = 1 \cdot x$. Pour les propriétés (2) à (4), la condition $x \mid y$ signifie l'existence d'un entier k tel que $y = k \cdot x$.
Pour (2), on a $y \mid z$ ce qui signifie qu'il existe $k_1 \in \mathbb{Z}$ tel que $z = k_1 y$. Donc $z = (kk_1)x$ et $x \mid z$.
Pour (3), écrivons $z = k_2 x$, $k_2 \in \mathbb{Z}$, il vient $\alpha y + \beta z = (\alpha k + \beta k_2)x$ et x divise $\alpha y + \beta z$.
Pour (4), remarquons que puisque $x \mid y$ et $y \mid x$, x et y sont non nuls. Donc $\mid x \mid \leq \mid y \mid$ et $\mid y \mid \leq \mid x \mid$ i.e. $\mid x \mid = \mid y \mid$.
Pour (5), voir plus tard. □

Exercice 16. Soient x et y des entiers. Montrer que $2x + 3y$ est divisible par 7 si et seulement si $5x + 4y$ l'est.

Exercice 17. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n - 4$ divise $3n - 17$.

Exercice 18. Démontrer que sur la droite $y = \frac{3}{4}x + \frac{1}{8}$ il n'y a pas de points à coordonnées entières.

IV.1.2. Division euclidienne

Théorème 1.3. *Soient a et b deux entiers positifs avec $a \neq 0$. Alors il existe q,$r \in \mathbb{N}$ uniques tels que $b = aq + r$ et $r < a$. L'entier q s'appelle* ***le quotient*** *de la division euclidienne de b par a, et r* ***le reste****.*

Démonstration. Pour montrer l'existence, on distingue trois cas :

(*i*) Si $a > b$, on prend $q = 0$ et $r = b < a$.

(*ii*) Si $a = b$, on prend $q = 1$ et $r = 0 < a$.

(*iii*) Si $a < b$, il existe un entier naturel n tel que $na > b$. Soit q le plus petit entier positif vérifiant $(q + 1)a > b$. Alors $qa \leq b$. Posons $r = b - aq$; il est alors clair que $a = bq + r$ et $0 \leq r < b$.

Pour montrer l'unicité, supposons qu'il existe deux couples (q,r) et (q',r') de nombres entiers naturels vérifiant

$$b = aq + r = aq' + r',$$

avec $0 \leq r,r' < a$, alors $a(q - q') = r' - r$ et donc $a \mid r' - r$. D'où $\mid r' - r \mid \geq a$ ou $\mid r' - r \mid = 0$. Mais $0 \leq r,r' < a$ entraîne que $\mid r' - r \mid < a$. Il s'ensuit $r = r'$ et $q = q'$. □

Le théorème ci-dessus admet la généralisation sur $\mathbb{Z}$ comme suit :

Théorème 1.4. *Soient a, b deux entiers avec $a \neq 0$. Alors il existe un unique couple (q,r) d'entiers tel que $b = aq + r$ et $0 \leq r < \mid a \mid$.*

Démonstration. À titre d'exercice. □

Exemple 1.8.
1. On prend $b = 145$ et $a = 13$. On a $145 = 13 \times 11 + 2$ donc $q = 11$ et $r = 2$ $(0 \leq r = 2 < \mid a \mid = 13)$.
2. On prend $b = 145$ et $a = -13$. On a $145 = -13 \times (-11) + 2$ donc $q = -11$ et $r = 2$ $(0 \leq r = 2 < \mid a \mid = 13)$.

Proposition 1.16. *Un entier a divise un entier b si et seulement si le reste de la division euclidienne de b par a est 0.*

Démonstration. À titre d'exercice. □

Exercice 19. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. On note q le quotient de la division euclidienne de $a-1$ par b. Déterminer pour tout $n \in \mathbb{N}$, le quotient de la division euclidienne de $(ab^n - 1)$ par b^{n+1}.

IV.2. Nombres Premiers et le Théorème Fondamental de l'Arithmétique

IV.2.1. Nombres Premiers

Définition 1.22. Un entier $p > 1$ est dit **premier** s'il est différent de 1 et s'il n'admet aucun diviseur positif différent de 1 et n. Un nombre qui n'est pas premier est appelé nombre **composé**.

par définition 1 n'est pas premier. les entiers 2,3,5,7,11 sont les premiers nombres premiers. Le nombre 12 est composé car on peut écrire $12 = 4 \times 3$.

Remarque 1.12. Tous les nombres premiers sont impaires sauf 2.

Proposition 1.17. *Soit $n > 1$ un entier. Son plus petit diviseur $d > 1$ est un nombre premier. Si de plus n est composé, alors $d \leq \sqrt{n}$.*

Démonstration. Supposons que d ne soit pas premier. Alors par définition, il existe un diviseur strict d' de d. Mais alors d' divise n, $d' > 1$ et $d' < d$, ce qui contredit la minimalité de d.
Comme d divise n, on peut écrire $n = dd'$. On a $d > 1$ et comme n n'est pas premier, $d < n$. Ainsi d' est un diviseur de n strictement supérieur à 1. Par minimalité de d, on obtient $d' > d$ et donc $n > d^2$ puis finalement $d \leq \sqrt{n}$. □

Théorème 1.5. *Il existe une infinité de nombres premiers.*

Démonstration. Procédons par l'absurde. Supposons qu'il existe un nombre fini de premiers positifs $p_1 < p_2 < \cdots < p_n$. Soit $P = p_1 \cdots p_n + 1$, P est un nombre composé (sinon P serai supérieur à tous les p_i), donc il doit admettre un diviseur premier parmi les p_i, ce qui est impossible car le reste de la division de P par tous les p_i est 1. □

Exercice 20. Montrer que le nombre $n^4 - n^2 + 16$, avec $n \in \mathbb{Z}$, est composé.

Exercice 21. Soit $n \geq 2$ un entier tel que $2^n - 1$ est premier. Montrer que n est un nombre premier.

IV.2.2. Le Théorème Fondamentale de l'Arithmétique

Théorème 1.6. *Tout nombre entier $n > 1$ se décompose de façon unique (à permutation près) en produit de nombres premiers.*

Démonstration. (Voir tout livre d'arithmétique). □

Ainsi tout entier $n > 1$ s'écrit de façon unique sous la forme

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

où $p_1, \cdots, p_k$ sont des nombres premiers distincts et $\alpha_1, \cdots, \alpha_k$ sont des entiers positifs non nuls. C'est la factorisation canonique de n. Grâce à l'unicité de cette factorisation, on voit que la factorisation canonique d'un produit mn est le produit des factorisations de m et n respectivement. On en déduit en particulier :

Corollaire 1.2. *Soient a et b deux entiers et soit p un nombre premier. Alors*

$$p \mid ab \text{ si et seulement si } p \mid a \text{ ou } p \mid b.$$

Exercice 22. Soient a,$b \in \mathbb{N}^*$ tels que $a^2 \mid b^2$. Montrer que $a \mid b$.

Exercice 23. Montrer qu'un entier naturel qui est à la fois un carré et un cube est aussi un entier à la puissance 6.

IV.3. PGCD, PPCM, Identité de Bézout et lemme de Gauss

IV.3.1. PGCD et PPCM

Définitions 1.1. Soient m et n deux entiers non nuls.

1. Le plus grand nombre strictement positif parmi les diviseurs communs de m et de n est appelé **le plus grand commun diviseur** de m et n. On le note $pgcd(m,n)$ ou $m \wedge n$.

2. Le plus petit entier strictement positif parmi les multiples communs de m et de n est appelé **le plus petit commun multiple** de m et n. On le note $ppcm(m,n)$ ou $m \vee n$.

Exemples 1.16. $pgcd(12,8) = 4$, $pgcd(-12,8) = 4$ et $pgcd(-12,-8) = 4$.

$ppcm(12,8) = 24$, $ppcm(-12,8) = 24$ et $ppcm(-12,-8) = 24$.

Remarques 1.11. 1. Pour tous $a,b \in \mathbb{Z}$, $pgcd(a,b) = pgcd(|\,a\,|\,,|\,b\,|)$.

2. On définit de la même manière le PGCD et le PPCM d'un nombre fini d'entiers non nuls.

Proposition 1.18. *Soient m et n deux entiers non nuls.*

1. Si p est un nombre premier alors $pgcd(p,m) = p$ ou $pgcd(p,m) = 1$.

2. Si $d = pgcd(m,n)$, $m = dm'$ et $n = dn'$ alors $pgcd(m',n') = 1$.

3. Si $m = nq + r$, alors $pgcd(m,n) = pgcd(n,r)$.

4. Si $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $\alpha_i, \beta_i \geq 0$, $i = 1, \cdots, k$, alors

$$ppcm(m,n) = p_1^{max(\alpha_1,\beta_1)} \cdots p_k^{max(\alpha_k,\beta_k)} \text{ et } pgcd(m,n) = p_1^{min(\alpha_1,\beta_1)} \cdots p_k^{min(\alpha_k,\beta_k)}.$$

5. $|\,mn\,| = pgcd(m,n) \cdot ppcm(m,n)$.

Démonstration. À titre d'exercice. □

La proposition (3) nous fournit un algorithme pour déterminer le PGCD de deux entiers, c'est ce qu'on appelle **l'algorithme d'Euclide**.

Exercice 24. Déterminer tous les couples $(x,y) \in \mathbb{N}$ tels que $x \wedge y + x \vee y = x + y$.

IV.4. Nombres premiers entre-eux, Identité de Bézout et lemme de Gauss

Définition 1.23. On dit que deux entiers non nuls m et n sont premiers entre-eux si $pgcd(m,n) = 1$.

Remarque 1.13. Pour un nombre fini (≥ 3) d'entiers non nuls, on a la notion des nombres deux à deux premiers entre-eux et celle des nombres premiers entre-eux dans leur ensemble.

Théorème 1.7. *(Identité de Bézout) Soient m et n des entiers non nuls. Si D est le PGCD de m et n, alors il existe $u,v \in \mathbb{Z}$ tels que $mu + nv = D$.*

Formellement,

$$D = pgcd(m,n) \Longrightarrow (\exists u,v \in \mathbb{Z})\ mu + nv = D.$$

Démonstration. Soit $A = \{mu + nv \in \mathbb{N}^* \ / \ u,v \in \mathbb{Z}\}$. Clairement, $A \neq \emptyset$ (car $\mid m \mid \in A$) et $A \subset \mathbb{N}$. Soit $d = mu_0 + nv_0 \geq 1$ le minimum de A et notons $D = pgcd(m,n)$.
D'une part, on a D divise m et n, donc D divise $d = mu_0 + nv_0$. En particulier, $D \leq d$.
D'autre part, par la division euclidienne de m par d, on a $m = dq + r$ avec $0 \leq r < d$. Par suite,

$$r = m - dq = m - (mu_0 + nv_0)q = m(1 - u_0) + n(-qv_0).$$

Si $r \neq 0$ alors $r \in A$, or $r < d$ ce qui contredit la minimalité de d. Par suite, $r = 0$ et $d \mid m$.
De la même manière on montre que $d \mid n$, donc $d \mid D$. En particulier $d \leq D$. D'où, $D = d = mu_0 + nv_0$. □

Remarque 1.14. La réciproque est fausse en général car si, par exemple, on prend $m = 6$, $n = 3$, $u = 3$ et $v = 2$, on a $mu + nv = 24$ mais $24 \neq m \wedge n = 3$.

Corollaire 1.3. *Soient m et n des entiers non nuls. Tout diviseur commun de m et n est un diviseur du PGCD de m et n.*

C'est-à-dire

$$d \mid m \text{ et } d \mid n \Longrightarrow d \mid m \wedge n.$$

Démonstration. Soit $D = pgcd(m,n)$, alors il existe $u_0,v_0 \in \mathbb{Z}$ tels que $D = mu_0 + nv_0$. Soit d' un diviseur commun de m et n, donc d' divise $mu_0 + nv_0$, c-à-d d' divise D. □

Corollaire 1.4. *Deux entiers m et n sont premiers entre-eux si et seulement s'il existe $u,v \in \mathbb{Z}$ tels que $mu + nv = 1$.*

Démonstration. On a $m \wedge n = 1$, il existe alors $u,v \in \mathbb{Z}$ tels que $mu + nv = 1$ (d'après le théorème ci-dessus). Réciproquement, supposons qu'il existe $u,v \in \mathbb{Z}$ tels que $mu+nv = 1$. Soit d un diviseur commun de m et n, donc $d \mid mu + nv = 1$ et le résultat en découle. □

Corollaire 1.5. *(Gauss) Soient a, b et c des entiers. Si $a \mid bc$ et $pgcd(a,b) = 1$ alors $a \mid c$.*

Démonstration. On a $pgcd(a,b) = 1$, donc il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$. Comme $c = acu + bcv$ et $a \mid bc$, alors $a \mid c$. □

Corollaire 1.6. *Si un nombre premier divise un produit d'entiers $a_1 \cdots a_n$, alors il divise l'un des a_i.*

Démonstration. À faire comme exercice. □

Corollaire 1.7. *Soient a et b deux entiers premiers entre-eux. Si c est un entier tel que $a \mid c$ et $b \mid c$ alors $ab \mid c$.*

Démonstration. On a $a \mid c$ et $b \mid c$, donc $c = aa' = bb'$ et par suite $a \mid bb'$. Comme $(a,b) = 1$, alors $a \mid b'$ c-à-d $b' = ka$. D'où $c = bb' = abk$ et le résultat en découle. □

Exercice 25. Soit $n \in \mathbb{N}$. Montrer que $6 \mid n^3 - n$.

Exercice 26. Montrer que pour tout $n \in \mathbb{N}^*$ $(n^2 + n) \wedge (2n + 1) = 1$.

Exercice 27. Montrer que si x et y sont des entiers premiers entre eux, il en est de même de $x + y$ et xy.

IV.5. Arithmétique modulaire

IV.5.1. Congruence - Définition et propriétés

Définition 1.24. Soient a, b et n des entiers avec $n \geq 1$. On dit que a est **congru** à b **modulo** n et on note $a \equiv b \pmod{n}$, si n divise $a - b$.

Autrement dit,

$$a \equiv b \pmod{n} \Longleftrightarrow n \mid a - b.$$

Ainsi, on a défini une relation sur $\mathbb{Z}$ appelée **relation de congruence**. Si n ne divise pas $a - b$, on dit que a n'est pas congru à b modulo n et on écrit $a \not\equiv b \pmod{n}$.

Les propriétés de la relation de divisibilité dans $\mathbb{Z}$ permettent de déduire les résultats suivants sur la compatibilité de la congruence modulo n avec l'addition et la multiplication dans $\mathbb{Z}$.

Propriétés 1.1. Soient a, b, c, d et n des entiers avec $n \geq 1$.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a + c \equiv b + d \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$.

Conséquences 1.1. Soient a, b, c, d et n des entiers avec $n \geq 1$.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a - c \equiv b - d \pmod{n}$. En particulier, si $a \equiv b \pmod{n}$, alors pour tout entier k, on a : $ka \equiv kb \pmod{n}$.
2. Si $a \equiv b \pmod{n}$, alors pour tout entier naturel k, on a : $a^k \equiv b^k \pmod{n}$.

Proposition 1.19. *Soient m un entier positif et a un entier premier avec m. Pour tous x,$y \in \mathbb{Z}$, on a :*

$$\textit{si } ax \equiv ay \pmod{m} \textit{ alors } x \equiv y \pmod{m}.$$

Démonstration. Il suffit d'appliquer le lemme de Gauss. □

Exercice 28. Soit m un entier positif et soient a et b deux entiers premier avec m. Pour tous x,$y \in \mathbb{N}$, montrer que

$$\text{si } a^x \equiv b^x \pmod{m} \text{ et } a^y \equiv b^y \pmod{m} \text{ alors } a^{x \wedge y} \equiv b^{x \wedge y} \pmod{m}.$$

Il est facile de prouver le résultat suivant :

Proposition 1.20. *La relation de congruence sur $\mathbb{Z}$ est une relation d'équivalence.*

Soit $n \geq 1$ un entier. Pour $a \in \mathbb{Z}$, on note $\overline{a}$ la classe d'équivalence pour cette relation d'équivalence. Ainsi, la classe de a modulo n est l'ensemble

$$\overline{a} = \{b \in \mathbb{Z} \,/ a \equiv b \pmod{n}\}.$$

Tout élément de $\overline{a}$ est appelé **un représentant** de cette classe.

Proposition 1.21. *Soient a, b et n des entiers avec $n \geq 1$.*

1. $\overline{a} = \overline{b} \Longleftrightarrow a \equiv b \pmod{n}$.

2. Si r *est le reste de la division de* a *par* n*, alors* $\overline{a} = \overline{r}$*, c-à-d* $a \equiv r \pmod{n}$.

Démonstration. 1. D'après 2 de la remarque 1.8 (page 25).

2. Il suffit d'écrire $a = nq + r$, c-à-d $a - r = nq$, puis conclure.

□

L'ensemble quotient $(\mathbb{Z}/\equiv)$ sera noté $\mathbb{Z}/n\mathbb{Z}$, donc

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \,/\, a \in \mathbb{Z}\}.$$

D'après l'assertion (2) de la proposition précédente, on a :

Proposition 1.22. *Soit* $n \geq 1$ *un entier.*
L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ *est fini de cardinal* n*. En fait,*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\ldots,\overline{n-1}\}.$$

L'addition et la multiplication définies sur $\mathbb{Z}$ permettent de définir deux opérations sur $\mathbb{Z}/n\mathbb{Z}$ $(n \geq 1)$, à savoir

- l'addition, notée aussi $+$, définie par $\overline{a} + \overline{b} = \overline{a+b}$, pour tous $a,b \in \mathbb{Z}$;
- la multiplication, notée aussi $\times$, définie par $\overline{a} \times \overline{b} = \overline{a \times b}$, pour tous $a,b \in \mathbb{Z}$. On écrit aussi, $\overline{a} \times \overline{b} = \overline{a}\overline{b} = \overline{a} \cdot \overline{b}$

Proposition 1.23. *Soit* p ***un nombre premier****. Pour tous* $a,b \in \mathbb{Z}$*, on a :*

$$\overline{a} \times \overline{b} = \overline{0} \Longrightarrow \overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0}.$$

Démonstration. Supposons que $\overline{a} \neq \overline{0}$, c-à-d p ne divise pas a, donc $p \wedge a = 1$ (car p est premier). Par suite et d'après Bézout, il existe $u,v \in \mathbb{Z}$ tels que $pu + av = 1$, donc $av \equiv 1 \pmod{p}$. D'autre part, on a $\overline{a} \times \overline{b} = \overline{0}$, c-à-d $ab \equiv 0 \pmod{p}$, donc $vab \equiv 0 \pmod{p}$. Par suite, $b \equiv 0 \pmod{p}$ ou encore $\overline{b} = \overline{0}$. □

Théorème 1.8. *(Le petit théorème de Fermat) Soit* $a \geq 0$ *un entier et soit* p *un nombre premier. alors*

$$a^p \equiv a \pmod{p}.$$

En particulier, si $pgcd(p,a) = 1$ *alors* $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration. À titre d'exercice. □

Chapitre 2

Structures algébriques
Groupes, anneaux et corps

I. Groupes

I.1. Lois de composition internes

I.1.1. Définition et exemples

Définition 2.1. Soit E un ensemble. **Une loi de composition interne** ($\ell.c.i$) sur E est une application de $E \times E$ vers E. On dit aussi **une loi interne** ou tout simplement **une loi** sur E. On parlera parfois **d'opération** sur E.

Notation. Souvent une $\ell.c.i$ sera notée par : $+$, $\times$, $*$, $\cdot$, $\top$ (truc), $\perp$ (anti-truc), $\circ$, etc.

Remarque 2.1. 1) Une $\ell.c.i$ est la donnée d'un couple $(E,*)$ où E est un ensemble et $*$ est une application de $E \times E$ vers E. On dit que l'ensemble E est muni de la loi "$*$".

2) Soit E un ensemble muni d'une $\ell.c.i$ $*$. L'image d'un élément $(x, y) \in E \times E$ se note $x * y$ et on l'appelle **le composé** de x et y (dans cet ordre). Ainsi, la loi $*$ sur E est l'application :

$$* : E \times E \longrightarrow E, \quad (x, y) \longmapsto x * y.$$

Exemples 2.1. 1) L'addition "$+$" et la multiplication "$\times$" sont des lois de composition internes sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

2) La soustraction ("$-$") est une loi sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, mais elle ne l'est pas sur $\mathbb{N}$ (car, par exemple, $(2, 3) \in \mathbb{N} \times \mathbb{N}$ et $2 - 3 \notin \mathbb{N}$).

3) L'intersection ("$\cap$"), la réunion ("$\cup$"), la différence ("$\setminus$") et la différence symétrique ("$\triangle$") sont des lois de composition internes sur l'ensemble des parties $P(E)$ d'un ensemble E.

4) La composition ("$\circ$") des applications est une loi de composition interne sur $\mathcal{F}(E, E)$ (E étant un ensemble).

5) L'addition ("+") et la multiplication ("×") sont des lois de composition internes sur $\mathcal{F}(\mathbb{R},\mathbb{R})$. Elles sont définies comme suit :

$$\begin{aligned} + : \mathcal{F}(\mathbb{R},\mathbb{R}) \times \mathcal{F}(\mathbb{R},\mathbb{R}) &\longrightarrow \mathcal{F}(\mathbb{R},\mathbb{R}) \\ (f,g) &\longmapsto f+g \\ \times : \mathcal{F}(\mathbb{R},\mathbb{R}) \times \mathcal{F}(\mathbb{R},\mathbb{R}) &\longrightarrow \mathcal{F}(\mathbb{R},\mathbb{R}) \\ (f,g) &\longmapsto f \times g = fg = f \cdot g \end{aligned}$$

telles que : $\forall x \in \mathbb{R}, (f+g)(x) = f(x) + g(x)$ et $(f \times g)(x) = f(x) \times g(x)$.

6) Le produit scalaire n'est pas une $\ell.c.i$ sur $\mathbb{R}^2$ (le plan vectoriel) du fait que $\forall \vec{u}, \vec{v} \in \mathbb{R}^2$, on a $\vec{u} \cdot \vec{v} \in \mathbb{R}$.

Remarque 2.2. D'après les exemples ci-dessus, on remarque qu'un ensemble peut être muni de plusieurs l.c.i.

I.1.2. Parties stables et lois induites

Définition 2.2. Soit E un ensemble muni d'une $\ell.c.i$ $*$. On dit qu'une partie non vide A de E est **stable** par la loi $*$ si, pour tous $x, y \in A$, on a $x * y \in A$.

Ainsi, la restriction de la loi $*$ à $A \times A$ définit une $\ell.c.i$ sur A qu'on appelle **loi induite** sur A par $*$.

Autrement dit, étant donné une partie non vide A de E, A est stable par la loi $*$ si et seulement si pour tous $x, y \in A$, on a $x * y \in A$.

Exemples 2.2. 1) Les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des parties stables de $\mathbb{C}$ par les lois $+$ et $\times$.

2) L'ensemble des entiers pairs est une partie stable de $\mathbb{Z}$ par les lois $+$ et $\times$.

3) L'ensemble des entiers impairs est une partie stable de $\mathbb{Z}$ par la loi $\times$, mais il ne l'est pas pour la loi $+$ (car on a, par exemple, 1 et 3 sont impairs mais $1+3=4$ qui n'est pas impair).

4) L'ensemble $\mathbb{R} \setminus \mathbb{Q}$ n'est pas une partie stable de $\mathbb{R}$ par la loi $\times$ (car on a, par exemple, $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ mais $\sqrt{2} \times \sqrt{2} = 2 \notin \mathbb{R} \setminus \mathbb{Q}$).

5) L'ensemble $i\mathbb{R} = \{ib \mid b \in \mathbb{R}\}$ n'est pas une partie stable de $\mathbb{C}$ pour la loi $\times$. En effet, $i \in i\mathbb{R}$ et $2i \in i\mathbb{R}$, mais $i \times 2i = -2 \notin i\mathbb{R}$.

6) Soit $\mathcal{F}(E,E)$ l'ensemble des applications d'un ensemble E vers lui-même. L'ensemble $\mathcal{B}(E)$ des bijections de E sur E est une partie stable de $\mathcal{F}(E,E)$ par la loi $\circ$. Il en est de même pour l'ensemble des injections et l'ensemble des surjections.

I.1.3. Propriétés d'une $\ell.c.i$

Soit E un ensemble muni d'une $\ell.c.i$ $*$.

a) La loi $*$ est **commutative** si pour tous $x, y \in E$, on a $x * y = y * x$.

b) La loi $*$ est **associative** si pour tous $x, y, z \in E$, on a $(x * y) * z = x * (y * z)$.

c) (i) Un élément $e \in E$ est un **élément neutre à droite** si pour tout $x \in E$, on a

$$x * e = x.$$

(ii) Un élément $e \in E$ est un **élément neutre à gauche** si pour tout $x \in E$, on a

$$e * x = x.$$

(iii) Un élément $e \in E$ est un **élément neutre** si pour tout $x \in E$, on a

$$x * e = x \text{ et } e * x = x.$$

d) Supposons que la loi $*$ admet un élément neutre $e \in E$.

(i) Un élément $x \in E$ est dit **symétrisable à gauche** s'il existe $x' \in E$, appelé symétrique à gauche de x, tel que $x' * x = e$.

(ii) Un élément $x \in E$ est dit **symétrisable à droite** s'il existe $x'' \in E$, appelé symétrique à droite de x, tel que $x * x'' = e$.

(iii) Un élément $x \in E$ est dit **symétrisable** s'il existe $x' \in E$, appelé symétrique de x, tel que $x' * x = x * x' = e$.

e) (a) Un élément $a \in E$ est dit **régulier** ou **simplifiable à gauche** si pour tous $x, y \in E$, on a

$$a * x = a * y \Rightarrow x = y$$

(b) Un élément $a \in E$ est dit **régulier** ou **simplifiable à droite** si pour tous $x, y \in E$, on a

$$x * a = y * a \Rightarrow x = y.$$

(c) Un élément de E est dit **régulier** ou **simplifiable** s'il est régulier à la fois à gauche et à droite.

Remarques 2.1. 1) Si la loi $*$ est commutative, alors :

- Les notions d'élément neutre à gauche et à droite coïncident.
- Les notions de symétrique à gauche et à droite coïncident.
- Les notions d'élément régulier à gauche et à droite coïncident.

2) Si la loi $*$ est associative, on omet généralement les parenthèses et on écrit :

$$\forall (x, y, z) \in E^3 \ \ (x * y) * z = x * (y * z) = x * y * z, \forall x, y, z \in E.$$

3) L'élément neutre, lorsqu'il existe, commute avec tous les éléments de E. De plus, il est symétrisable et son symétrique est lui-même.

4) Si x' est un symétrique de $x \in E$, alors x est aussi un symétrique de x'. On dit qu'ils sont symétriques l'un de l'autre.

Exemples 2.3. 1) Les lois "+" et "×" sont commutatives et associatives dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ et admettent respectivement 0 et 1 comme éléments neutres.

2) Tout élément x de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ est symétrisable pour la loi "+" de symétrique $(-x)$, appelé **l'opposé** de x (car $x + (-x) = (-x) + x = 0$).

3) Tout élément x de $\mathbb{Q}^*$, $\mathbb{R}^*$ ou $\mathbb{C}^*$ est symétrisable pour la loi "×" de symétrique $x^{-1} = \frac{1}{x}$, appelé **l'inverse** de x (car $x \cdot x^{-1} = x^{-1} \cdot x = 1$).

4) Soit E un ensemble.

- Les lois "$\cap$", "$\cup$" et "Δ" sont commutatives et associatives dans $\mathcal{P}(E)$.
- L'élément neutre de la loi "$\cap$" dans $\mathcal{P}(E)$ est E. En effet,

$$\forall A \in \mathcal{P}(E),\ A \cap E = E \cap A = A.$$

- L'élément neutre de la loi "$\cup$" dans $\mathcal{P}(E)$ est $\emptyset$. En effet,

$$\forall A \in \mathcal{P}(E),\ A \cup \emptyset = \emptyset \cup A = A.$$

- L'élément neutre de la loi "Δ" dans $\mathcal{P}(E)$ est $\emptyset$. En effet,

$$\forall A \in \mathcal{P}(E),\ A\Delta\emptyset = \emptyset\Delta A = A.$$

- Le seul élément symétrisable dans $\mathcal{P}(E)$ pour la loi "$\cap$" (resp. la loi "$\cup$") est E (resp. $\emptyset$).

5) La soustraction "$-$" n'est ni commutative, ni associative dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. En effet, on a par exemple :

$$1 - 2 \neq 2 - 1 \text{ et } (1 - 2) - 3 \neq 1 - (2 - 3).$$

6) Soit E un ensemble.

- La loi "$\circ$" sur $\mathcal{F}(E, E)$ est associative mais elle n'est pas commutative (car $f \circ g \neq g \circ f$ en général). De plus, l'application identité id_E est l'élément neutre de la loi "$\circ$" dans $\mathcal{F}(E, E)$.
- Les applications bijectives $f \in \mathcal{F}(E, E)$ sont symétrisables et ont pour symétriques leurs bijections réciproques f^{-1} (car $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}_E$).

7) Tout élément $a \in \mathbb{C}$ est régulier pour la loi "+" dans $\mathbb{C}$, car

$$\forall z, z' \in \mathbb{C}, \quad a + z = a + z' \Rightarrow z = z' \quad \text{et} \quad z + a = z' + a \Rightarrow z = z'.$$

8) De même, tout élément $a \in \mathbb{C}^*$ est régulier pour la loi "×" dans $\mathbb{C}^*$.

9) 0 n'est pas régulier pour la multiplication dans $\mathbb{C}$. En effet, on a : $0 \times 1 = 0 \times 2$ mais $1 \neq 2$.

10) Soit $E = \{1, 2, 3, 4\}$; $A = \{1\}, B = \{1, 2, 3\}$ et $C = \{1, 2, 4\}$. On a : $A \cap B = A \cap C$ mais $B \neq C$. Donc A n'est pas simplifiable pour la loi "$\cap$" dans $\mathcal{P}(E)$.

Proposition 2.1. *Une $\ell.c.i$ sur un ensemble admet au plus un élément neutre.*

Démonstration. Soit E un ensemble muni d'une $\ell.c.i$ $*$. Supposons qu'il existe deux éléments neutres e_1 et e_2. On a :

$$e_1 * e_2 = e_1 \quad \text{car } e_2 \text{ est un élément neutre,}$$

et

$$e_1 * e_2 = e_2 \quad \text{car } e_1 \text{ est un élément neutre.}$$

Donc $e_1 = e_2$. □

Définition 2.3. Un **monoïde** est la donnée d'un couple $(E, *)$ où E est un ensemble et $*$ est une $\ell.c.i$ associative sur E. Si en plus la loi $*$ est commutative (resp. possède un élément neutre), alors $(E, *)$ est dit un monoïde commutatif (resp. unitaire).

Exemples 2.4. 1) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des monoïdes commutatifs unitaires.

2) $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ sont des monoïdes commutatifs unitaires.

3) L'ensemble $\mathbb{Z}$ muni de la $\ell.c.i$ "$-$" n'est pas un monoïde, car la loi "$-$" n'est pas associative.

Proposition 2.2. *Soit $(E, *)$ un monoïde unitaire.*

1) Le symétrique à gauche et le symétrique à droite, lorsqu'ils existent, d'un élément de E coïncident.

2) Si deux éléments x et y de E sont symétrisables de symétriques respectifs x' et y', alors le composé $x * y$ est symétrisable et son symétrique est $(x * y)' = y' * x'$.

3) Si un élément de E est symétrisable à gauche (resp. à droite), alors il est régulier à gauche (resp. à droite).

Démonstration. Notons e l'élément neutre de $(E, *)$.

1) Soit $x \in E$ et x' (resp. x'') son symétrique à gauche (resp. à droite). On a :

$$\begin{aligned} x' &= x' * e \quad (\text{car } e \text{ est le neutre pour } *) \\ &= x' * (x * x'') \quad (\text{car } x'' \text{ est le symétrique à droite de } x) \\ &= (x' * x) * x'' \quad (\text{car } * \text{ est associative}) \\ &= e * x'' \quad (\text{car } x' \text{ est le symétrique à gauche de } x) \\ &= x'' \quad (\text{car } e \text{ est le neutre pour } *). \end{aligned}$$

Donc $x' = x''$.

2) On a :

$$\begin{aligned} (x * y) * (y' * x') &= x * (y * y') * x' \quad (\text{car } * \text{ est associative}) \\ &= x * e * x' \quad (\text{car } y' \text{ est le symétrique de } y) \\ &= x * x' \quad (\text{car } e \text{ est le neutre pour } *) \\ &= e \quad (\text{car } x' \text{ est le symétrique de } x). \end{aligned}$$

Donc $y' * x'$ est le symétrique à droite de $x * y$. De manière similaire, on trouve :

$$(y' * x') * (x * y) = e,$$

c'est-à-dire que $y' * x'$ est le symétrique à gauche de $x * y$. Donc $x * y$ est symétrisable et son symétrique est

$$(x * y)' = y' * x'.$$

Une autre méthode : Soit $z \in E$ le symétrique à droite de $x * y$. On a :

$$\begin{aligned}
&(x * y) * z = e \\
&\iff x * (y * z) = e \quad (\text{car } * \text{ est associative}) \\
&\iff x' * (x * (y * z)) = x' * e \\
&\iff (x' * x) * (y * z) = x' \quad (\text{car } x' \text{ est le symétrique de } x) \\
&\iff e * (y * z) = x' \\
&\iff y * z = x' \\
&\iff y' * (y * z) = y' * x' \\
&\iff e * z = y' * x' \quad (\text{car } y' \text{ est le symétrique de } y) \\
&\iff z = y' * x'.
\end{aligned}$$

On vérifie facilement que pour $z = y' * x'$, on a aussi $z * (x * y) = e$. Donc $z = y' * x'$ est le symétrique de $x * y$.

3) Soit $a \in E$ symétrisable à gauche, donc il existe $a' \in E$ tel que $a' * a = e$.

Pour tous $x, y \in E$, on a :

$$\begin{aligned}
a * x = a * y &\Rightarrow a' * (a * x) = a' * (a * y) \\
&\Rightarrow (a' * a) * x = (a' * a) * y \\
&\Rightarrow e * x = e * y \\
&\Rightarrow x = y
\end{aligned}$$

donc a est régulier à gauche. □

Le cas où a est symétrisable à droite peut être traité de la même manière.

Remarque 2.3.

1. Dans un monoïde unitaire, le symétrique, s'il existe, d'un élément est unique.

2. La réciproque de (3) dans la proposition 1.2 est fausse en général. En effet, dans $(\mathbb{Z}, \times)$, on a :

$$\begin{aligned}
&\forall x, y \in \mathbb{Z}, \\
&2 \times x = 2 \times y \Rightarrow 2x - 2y = 0 \\
&\Rightarrow 2(x - y) = 0 \\
&\Rightarrow x - y = 0 \quad (\text{car } 2 \neq 0) \\
&\Rightarrow x = y
\end{aligned}$$

donc $2 \in \mathbb{Z}$ est régulier, mais 2 n'est pas symétrisable dans $(\mathbb{Z}, \times)$ (car le symétrique de 2 serait $\frac{1}{2}$ mais $\frac{1}{2} \notin \mathbb{Z}$).

Lorsqu'un ensemble est muni de deux lois de composition internes, on a la notion suivante :

Définition 2.4. Soit A un ensemble muni des $\ell.c.i$ $*$ et $\top$.

1. La loi $\top$ est distributive à gauche par rapport à la loi $*$ si
$$\forall x, y, z \in A, \quad x\top(y * z) = (x\top y) * (x\top z).$$
2. La loi $\top$ est distributive à droite par rapport à la loi $*$ si
$$\forall x, y, z \in A, \quad (y * z)\top x = (y\top x) * (z\top x).$$
3. La loi $\top$ est distributive par rapport à la loi $*$ si elle est distributive à la fois à gauche et à droite.

Remarques 2.2. 1. Si la loi $\top$ est commutative, alors la distributivité à gauche et à droite désignent la même chose.

2. Si la loi $\top$ est distributive par rapport à la loi $*$, cela n'implique pas, en général, que $*$ est distributive par rapport à $\top$.

Exemples 2.5. 1. La loi "$\times$" est distributive par rapport à la loi "$+$" dans $\mathbb{C}$. Mais la loi "$+$" n'est pas distributive par rapport à la loi "$\times$" dans $\mathbb{C}$ (car $1 + (2 \times 3) \neq (1 + 2) \times (1 + 3)$).

2. Soit E un ensemble :
   - L'intersection est distributive par rapport à la réunion dans $\mathcal{P}(E)$.
   - La réunion est distributive par rapport à l'intersection dans $\mathcal{P}(E)$.

I.1.4. Loi produit

Définition 2.5. Soient E_1 et E_2 deux ensembles munis respectivement des lois de composition interne $\top_1$ et $\top_2$. On peut définir une loi de composition interne $\top$ sur $E_1 \times E_2$ de la manière suivante :

$$\forall (x_1, x_2) \in E_1 \times E_2, \quad \forall (y_1, y_2) \in E_1 \times E_2, \quad (x_1, x_2)\top(y_1, y_2) = (x_1\top_1 y_1, x_2\top_2 y_2).$$

La loi $\top$ est appelée **la loi produit** des lois $\top_1$ et $\top_2$.

Proposition 2.3. *Sous les hypothèses ci-dessus, on a :*

1) Si $\top_1$ et $\top_2$ sont commutatives, alors la loi produit $\top$ est commutative.

2) Si $\top_1$ et $\top_2$ sont associatives, alors la loi produit $\top$ est associative.

3) Si e_1 (resp. e_2) est l'élément neutre de $(E_1, \top_1)$ (resp. $(E_2, \top_2)$), alors le couple (e_1, e_2) est l'élément neutre de $(E_1 \times E_2, \top)$.

4) Si de plus $x_1 \in E_1$ et $x_2 \in E_2$ sont symétrisables de symétriques respectifs $x_1' \in E_1$ et $x_2' \in E_2$, alors le couple $(x_1, x_2) \in E_1 \times E_2$ est symétrisable pour la loi produit $\top$ de symétrique le couple (x_1', x_2').

Remarques 2.3. 1) Si $(E_1, \top_1), \ldots, (E_n, \top_n)$ sont des ensembles munis de lois de composition interne, la loi produit $\top$ définie sur $E_1 \times \ldots \times E_n$ par :
$\forall (x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n, \quad \forall (y_1, \ldots, y_n) \in E_1 \times \ldots \times E_n,$

$$(x_1, \ldots, x_n) \top (y_1, \ldots, y_n) = (x_1 \top_1 y_1, \ldots, x_n \top_n y_n).$$

est une loi produit.

2) Si $(E, *)$ est un ensemble muni d'une loi de composition interne $*$, alors la loi produit, notée aussi $*$, définie sur $E^n = \underbrace{E \times \ldots \times E}_{n \text{ fois}} (n \geq 2)$ est donnée par :

$$\forall (x_1, \ldots, x_n) \in E^n, \quad \forall (y_1, \ldots, y_n) \in E^n, \quad (x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 * y_1, \ldots, x_n * y_n).$$

Exemples 2.6. 1) La loi produit, notée aussi $+$, sur $\mathbb{R}^n$ lorsque $\mathbb{R}$ est muni de la loi $+$, est donnée par :

$$\forall (x_1, \ldots, x_n) \in \mathbb{R}^n, \quad \forall (y_1, \ldots, y_n) \in \mathbb{R}^n, \quad (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Notez que $(\mathbb{R}^n, +)$ est un groupe abélien car $(\mathbb{R}, +)$ l'est.

- L'élément neutre de $(\mathbb{R}^n, +)$ est $0_{\mathbb{R}^n} = (0, \ldots, 0)$.
- L'opposé de $(x_1, \ldots, x_n) \in \mathbb{R}^n$ est $(-x_1, \ldots, -x_n)$.

2) La loi produit, notée aussi $\times$, sur $\mathbb{R}^n$ lorsque $\mathbb{R}$ est muni de la loi $\times$, est donnée par :

$$\forall (x_1, \ldots, x_n) \in \mathbb{R}^n, \quad \forall (y_1, \ldots, y_n) \in \mathbb{R}^n, \quad (x_1, \ldots, x_n) \times (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

- L'élément neutre de $(\mathbb{R}^n, \times)$ est $1_{\mathbb{R}^n} = (1, \ldots, 1)$.
- L'inverse de $(x_1, \ldots, x_n) \in \mathbb{R}^n$ tel que $x_i \neq 0 \ \forall i \in \{1, \ldots, n\}$ est le n-uplet $(x_1^{-1}, \ldots, x_n^{-1})$.

I.2. Groupes

I.2.1. Définition et exemples

Définition 2.6. Un groupe est la donnée d'un couple $(G, *)$, où G est un ensemble et $*$ est une loi de composition interne sur G vérifiant les conditions suivantes :

(a) La loi $*$ est associative.

(b) La loi $*$ admet un élément neutre.

(c) Tout élément de G est symétrisable.

Autrement dit, un groupe est un monoïde unitaire dont tous les éléments sont symétrisables, c'est-à-dire

$$(G, *) \text{ est un groupe } \iff \begin{cases} (a)\ \forall x, y, z \in G, \quad (x * y) * z = x * (y * z) \\ (b)\ \exists e \in G, \quad \forall x \in G, \quad x * e = e * x = x \\ (c)\ \forall x \in G, \quad \exists x' \in G, \quad x * x' = x' * x = e \end{cases}$$

Remarques 2.4. 1) Si $(G, *)$ est un groupe et si la loi $*$ est commutative, alors le groupe $(G, *)$ est dit **groupe commutatif** ou **groupe abélien**.

2) Un groupe n'est jamais vide, il contient au moins son élément neutre.

3) Si la loi du groupe G est l'addition ("+"), on dit que le groupe G est **additif**. Dans ce cas :

- L'élément neutre sera noté "0_G" ou tout simplement "0".
- Le symétrique d'un élément $x \in G$ sera noté $-x$ et on l'appelle l'**opposé** de x.

4) Si la loi du groupe G est la multiplication ("$\cdot$"), on dit que le groupe G est **multiplicatif**. Dans ce cas :

- L'élément neutre sera noté "1_G" ou tout simplement "1".
- Le symétrique d'un élément $x \in G$ sera noté x^{-1} et on l'appelle l'**inverse** de x.

Exemples 2.7. 1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes abéliens. Il en est de même pour $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$.

2) $(\mathcal{P}(E), \Delta)$ est un groupe abélien.

3) $(\mathbb{N},+)$, $(\mathbb{Z}, \times)$, $((\mathcal{P}(E), \cup)$ et $(\mathcal{P}(E), \cap)$ ne sont pas des groupes (dans les deux derniers exemples, on suppose que $\text{card}(E) \geqslant 2$).

Proposition 2.4. *1. L'élément neutre d'un groupe est unique.*

2. Le symétrique d'un élément d'un groupe est unique.

3. Tout élément d'un groupe est régulier.

Démonstration. Conséquences des résultats de la sous-section précédente. □

Exercice 29. 1) Montrer que $\forall x, y \in \mathbb{R} \setminus \{1\}, \quad x \top y = x + y - xy$ définit une loi de groupe abélien sur $(\mathbb{R} \setminus \{1\}, \top)$.

2) Montrer que $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un groupe abélien pour la loi $+$.

I.2.2. Sous-groupes d'un groupe

Définition 2.7. Soit $(G, *)$ un groupe. Une partie H de G est dite un **sous-groupe** de G si :

i) H est une partie stable de G pour la loi $*$.

ii) $(H, *)$ est un groupe.

Exemples 2.8. 1) $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.

2) $(\mathbb{R}^*, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

3) $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, mais $\mathbb{R}_-^*$ ne l'est pas car $\mathbb{R}_-^*$ n'est pas stable par la loi $\times$ (par exemple,$(-1) \in \mathbb{R}_-^*$ et $(-2) \in \mathbb{R}_-^*$, mais $(-1) \times (-2) = 2 \notin \mathbb{R}_-^*$).

Proposition 2.5 (Caractérisation d'un sous-groupe)**.** *Soit $(G, *)$ un groupe d'élément neutre e et H un sous-ensemble de G. H est un sous-groupe de G si et seulement si les trois conditions suivantes sont satisfaites :*

i) $H \neq \emptyset$ (on vérifie que $e \in H$).

ii) Pour tous $x, y \in H$, on a $x * y \in H$ (stabilité par la loi $*$).

iii) Pour tout $x \in H$, le symétrique x' de x dans $(G, *)$ est un élément de H (stabilité par passage au symétrique).

Démonstration. À faire à titre d'exercice. □

Remarques 2.5. 1) Un sous-groupe H est aussi un groupe muni de la loi induite par celle de G.

2) Un critère pratique et plus rapide pour prouver que H est un sous-groupe de G est donné par :

$$H \text{ est un sous-groupe de } (G,*) \Leftrightarrow \begin{cases} (i)\ H \neq \emptyset, \\ (ii)\ \forall x, y \in H, \quad x * y' \in H, \\ \text{où } y' \text{ est le symétrique de } y \text{ dans } (G,*). \end{cases}$$

3) Si G est un groupe additif, alors

$$H \text{ est un sous-groupe de } (G,+) \Leftrightarrow \begin{cases} (i)\ H \neq \emptyset\ (0 \in H), \\ (ii)\ \forall x, y \in H, \quad x - y \in H, \\ \text{où } (-y) \text{ est l'opposé de } y \text{ dans } (G,+). \end{cases}$$

4) Si G est un groupe multiplicatif, alors

$$H \text{ est un sous-groupe de } (G,\cdot) \Leftrightarrow \begin{cases} (i)\ H \neq \emptyset\ (1 \in H), \\ (ii)\ \forall x, y \in H, \quad xy^{-1} \in H, \\ \text{où } y^{-1} \text{ est l'inverse de } y \text{ dans } (G,\cdot). \end{cases}$$

5) Si $(G,*)$ un groupe d'élément neutre e alors, $\{e\}$ et G sont des sous-groupes de G appelés **sous-groupes triviaux** de G. Tout autre sous-groupe non trivial est appelé un **sous-groupe propre** de G.

Exercice 30. 1) Soit $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Montrer que $(\mathbb{U}, \times)$ est un groupe abélien.

2) Soit $(G, \cdot)$ un groupe. On pose :

$$Z(G) = \{g \in G \mid g \cdot x = x \cdot g, \forall x \in G\},$$

appelé **centre** de G. Montrer que $Z(G)$ est un sous-groupe de $(G, \cdot)$.

Théorème 2.1. *(Sous-groupes de $\mathbb{Z}$) Les seules sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.*

Rappelons que $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ est l'ensemble des multiples de $n \in \mathbb{N}$.
Par exemple, $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$, $2\mathbb{Z} = \{\ldots, -4, -2,0,2,4, \ldots\}$, etc.

Démonstration. À faire à titre d'exercice. □

Proposition 2.6. *L'intersection de deux sous-groupes d'un groupe est un sous-groupe de ce groupe.*

Démonstration. Soit H et K deux sous-groupes d'un groupe $(G,*)$ d'élément neutre e.

(*i*) Clairement $H \cap K \subset G$.

(*ii*) On a $e \in H \cap K$, car H et K sont deux sous-groupes d'un groupe G, en particulier $e \in H$ et $e \in K$.

(*iii*) Soient $x,y \in H \cap K$ et y' le symétrique de y dans G. Comme H et K sont deux sous-groupes d'un groupe G, alors $x*y' \in H$ et $x*y' \in K$. Par conséquent, $x*y' \in H \cap K$.

D'où $H \cap K$ est un sous-groupe de G. □

Remarques 2.6. 1) Cette proposition se généralise à une famille quelconque de sous-groupes. C'est-à-dire l'intersection d'une famille de sous-groupes d'un groupe G est aussi un sous-groupe de G.

2) La réunion de deux sous-groupes n'est pas en général un sous-groupe. En effet, considérons les sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ du groupe additif $\mathbb{Z}$. On a 2 et 3 sont des éléments de $2\mathbb{Z} \cup 3\mathbb{Z}$ mais $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

I.3. Homomorphismes

I.3.1. Définitions et propriétés

Définition 2.8. Soient E et F deux ensembles non vides munis respectivement des lois internes $*$ et $\top$. On appelle **homomorphisme** ou **morphisme** de $(E,*)$ vers (F,T) toute application $f : E \longrightarrow F$ vérifiant :

$$\forall x, y \in E, \quad f(x * y) = f(x) \top f(y).$$

Exemples 2.9. 1) L'application $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$ est un morphisme. En effet, $\forall x, y \in \mathbb{R}_+^*, \quad \ln(xy) = \ln(x) + \ln(y)$.

2) L'application $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$ est un morphisme. En effet, $\forall x, y \in \mathbb{R}, \quad \exp(x + y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$.

3) L'application $f : (\mathbb{C}, \times) \longrightarrow (\mathbb{R}_+, \times)$ définie par $f(z) = |z|$ est un morphisme. En effet, $\forall z, z' \in \mathbb{C}, \quad f(z \times z') = |z \times z'| = |z| \times |z'| = f(z)f(z')$.

4) L'application $g : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+, +)$ définie par $g(x) = |x|$ n'est pas un morphisme. En effet, $g(2 + (-3)) = g(-1) = 1$ et $g(2) + g(-3) = 5$, donc $g(2 + (-3)) \neq g(2) + g(-3)$.

5) L'application $h : (\mathbb{R}_+, +) \longrightarrow (\mathbb{R}_+, +)$ définie par $h(x) = \sqrt{x}$ n'est pas un morphisme. En effet, $h(16 + 9) \neq h(16) + h(9)$.

Remarques 2.7. 1) **Un endomorphisme** est un homomorphisme de $(E, *)$ vers $(E, *)$.

2) **Un isomorphisme** est un homomorphisme bijectif.

3) **Un automorphisme** est un endomorphisme bijectif.

Proposition 2.7. *Soit $f : (E,*) \longrightarrow (F,\top)$ un homomorphisme.*

1. *Si H est une partie stable de E par $*$ alors $f(H)$ est une partie stable de F par $\top$. En particulier, l'image $f(E)$ de E par f est une partie stable de F par $\top$.*
2. *Si la loi $*$ est commutative (resp. associative) dans E, alors la loi $\top$ est commutative (resp. associative) dans $f(E)$.*
3. *Si $e \in E$ est l'élément neutre de $(E,*)$, alors $f(e)$ est l'élément neutre de $\top$ dans $f(E)$.*
4. *Si un élément $x \in E$ est symétrisable pour la loi $*$ de symétrique x', alors $f(x)$ est symétrisable pour la loi T de symétrique $f(x')$ dans $f(E)$ (i.e.,$(f(x))' = f(x')$).*

Démonstration. 1. Soient $y_1,y_2 \in f(H)$, donc il existe $x_1,x_2 \in H$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. On a :

$$\begin{aligned} y_1 \top y_2 &= f(x_1) \top f(x_2) \\ &= f(x_1 * x_2) \quad (\text{car } f \text{ est un morphisme }). \end{aligned}$$

Comme $x_1,x_2 \in H$ et H est stable par la loi $*$, alors $x_1 * x_2 \in H$. Par suite, $y_1 \top y_2 = f(x_1 * x_2) \in f(H)$. D'où, $f(H)$ est une partie stable de F par $\top$.

2. Soient $y_1,y_2 \in f(E)$, donc il existe $x_1,x_2 \in E$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. On a :

$$\begin{aligned} y_1 \top y_2 &= f(x_1) \top f(x_2) \\ &= f(x_1 * x_2) \quad (\text{car } f \text{ est un morphisme }) \\ &= f(x_2 * x_1) \quad (\text{car } * \text{ est commutative }) \\ &= f(x_2) \top f(x_1) \quad (\text{car } f \text{ est un morphisme }) \\ &= y_2 \top y_1. \end{aligned}$$

D'où la commutativité de $\top$ dans $f(E)$.
D'une manière similaire, on montre que l'associativité de $*$ dans E entraîne l'associativité de $\top$ dans $f(E)$.

3. (Exercice).

4. (Exercice).

□

Théorème 2.2. *La composée de deux homomorphismes est un homomorphisme.*

Démonstration. Soient $f : (E,*) \longrightarrow (F,\top)$ et $g : (F,\top) \longrightarrow (G,\perp)$ deux homomorphismes. La composée $g \circ f$ est une application de E vers G. Pour $x, y \in E$, on a :

$$g \circ f(x * y) = g(f(x * y)) = g(f(x) \top f(y)) = g(f(x)) \perp g(f(y)) = g \circ f(x) \perp g \circ f(y).$$

Donc, $g \circ f$ est un homomorphisme. □

Comme conséquence, on a le résultat suivant :

Corollaire 2.1. *La composée de deux isomorphismes (resp. automorphismes) est un isomorphisme (resp. un automorphisme).*

Théorème 2.3. *Soient E et F deux ensembles munis respectivement des lois $*$ et $\top$. Si f est un isomorphisme de $(E,*)$ vers $(F,\top)$, alors la bijection réciproque f^{-1} est un isomorphisme de $(F,\top)$ vers $(E,*)$.*

Démonstration. Puisque f est un isomorphisme, f est bijectif et donc f^{-1} est aussi bijective. Maintenant, soient $y_1, y_2 \in F$ il existe donc x_1,$x_2 \in E$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. On a

$$f^{-1}(y_1 \top y_2) = f^{-1}(f(x_1) \top f(x_2)) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2 = f^{-1}(y_1) * f^{-1}(y_2).$$

Donc, f^{-1} est un isomorphisme. □

I.3.2. Morphismes de groupes

Lorsque l'ensemble de départ et l'ensemble d'arrivée d'un homomorphisme sont des groupes, on parle d'homomorphisme de groupes.

Théorème 2.4. *Soit $f : (G,*) \longrightarrow (G',\top)$ un homomorphisme de groupes.*

1. *Si H est un sous-groupe de G, alors l'image $f(H)$ de H par f est un sous-groupe de G'.*

2. *Si H' est un sous-groupe de G', alors l'image réciproque $f^{-1}(H')$ de H' par f est un sous-groupe de G.*

Démonstration. Soit e (resp. e') l'élément neutre de $(G,*)$ (resp. $(G',\top)$).

1. • On a $e' = f(e) \in f(H)$.
   • Soient $y_1, y_2 \in f(H)$, donc il existe $x_1, x_2 \in H$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. Notons $(y_2)'$ (resp. $(x_2)'$) le symétrique de y_2 dans $(G',\top)$(resp. de x_2 dans $(G,*)$). On a : $y_1 \top (y_2)' = f(x_1) \top (f(x_2))' = f(x_1) \top f((x_2)') = f(x_1 * (x_2)')$. Comme $x_1, x_2 \in H$ et H est un sous-groupe de G alors $x_1 * (x_2)' \in H$, donc

   $$y_1 \top y_2 = f(x_1 * (x_2)') \in f(H).$$

   D'où, D'où $f(H)$ est un sous-groupe est un sous groupe de $(G',\top)$.

2. • On a $e \in f^{-1}(H')$ car $f(e) = e' \in f(H)$.
   • Soient x_1,$x_2 \in f^{-1}(H')$ et $(x_2)'$ le symétrique de x_2 dans $(G,*)$.
   On a x_1,$x_2 \in f^{-1}(H')$ donc $f(x_1)$,$f(x_2) \in H'$. Comme H' est un sous-groupe de $(G',\top)$, alors $f(x_1) \top (f(x_2))' \in H'$, c-à-d $f(x_1 * (x_2)') \in H'$. Par conséquent, $x_1 * (x_2)' \in f^{-1}(H')$. D'où, $f^{-1}(H')$ est un sous-groupe de $(G,*)$.

□

Corollaire 2.2. *Soit $f : (G, *) \longrightarrow (G', T)$ un morphisme de groupes. Alors, $f(G)$ est un sous-groupe de (G', T) et $f^{-1}(\{e'\})$ est un sous-groupe de $(G, *)$, où e' est l'élément neutre de (G', T).*

Démonstration. Application directe du théorème précédent. □

Définition 2.9. Soit $f : (G, *) \longrightarrow (G', \top)$ un homomorphisme de groupes et soit e' l'élément neutre du groupe (G', T).

1) **Le noyau** de l'homomorphisme f est l'ensemble noté $\mathrm{Ker}(f)$ et qui est défini par :

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e'\}.$$

2) **L'image** de l'homomorphisme f est l'ensemble noté $\mathrm{Im}(f)$ et qui est défini par :

$$\mathrm{Im}(f) = f(G) = \{f(x) \mid x \in G\}.$$

Autrement dit,

$$x \in \mathrm{Ker}(f) \Longleftrightarrow f(x) = e' \quad \text{et} \quad y \in \mathrm{Im}(f) \Longleftrightarrow \exists x \in G,\ y = f(x).$$

Remarques 2.8. 1) Le noyau $\mathrm{Ker}(f)$ n'est jamais vide, car il contient au moins l'élément neutre e de $(G, *)$, puisque $f(e) = e'$.

2) L'image $\mathrm{Im}(f)$ n'est jamais vide, car $e' = f(e) \in \mathrm{Im}(f)$.

3) D'après le corollaire ci-dessus, le noyau $\mathrm{Ker}(f)$ est un sous-groupe de $(G, *)$ et l'image $\mathrm{Im}(f)$ est un sous-groupe de $(G', \top)$.

Théorème 2.5. *Un homomorphisme de groupes $f : (G, *) \longrightarrow (G', T)$ est injectif si et seulement si $\mathrm{Ker}(f) = \{e\}$, où e est l'élément neutre de $(G,*)$.*

Démonstration. Supposons que f est injectif et montrons que $\mathrm{Ker}(f) = \{e\}$.
Soit $x \in \mathrm{Ker}(f)$, donc $f(x) = e'$, où e' est l'élément neutre de (G', T).
Or, $e' = f(e)$, donc $f(x) = f(e)$ implique $x = e$ (car f est injectif). Il en résulte que $\mathrm{Ker}(f) \subseteq \{e\}$ et donc $\mathrm{Ker}(f) = \{e\}$.
Réciproquement, supposons que $\mathrm{Ker}(f) = \{e\}$ et montrons que f est injectif.
Soient $a, b \in G$ tels que $f(a) = f(b)$. Alors, $f(a)\top(f(b))' = e'$, $(f(b))'$ est le symétrique de $(f(b))$, donc $f(a * b') = e'$, b' est le symétrique de b.
Par définition, cela signifie que $a * b^{-1} \in \mathrm{Ker}(f) = \{e\}$, donc $a = b$. □

Définition 2.10. Deux groupes sont dits **isomorphes** s'il existe un isomorphisme de groupes entre eux.

Exercice 31. On définit sur $]1, +\infty[$ la loi de composition interne $*$ par :

$$\forall x, y \in]1, +\infty[, \quad x * y = \sqrt{(x^2 - 1)(y^2 - 1) + 1}.$$

On considère l'application $f : \mathbb{R}_+^* \longrightarrow]1, +\infty[$ définie par :

$$x \longmapsto \sqrt{x + 1}.$$

1. Montrer que $(]1,+\infty[,*)$ est un groupe abélien.
2. Montrer que f est un morphisme de $(\mathbb{R}_+^*,\times)$ vers $(]1,+\infty[,*)$.
3. Déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$, puis conclure.
4. Montrer que $A=\left\{\sqrt{1+2^m} \mid m\in\mathbb{Z}\right\}$ est un sous-groupe de $(]1,+\infty[,*)$.

II. Anneaux

II.1. Définitions et exemples

II.1.1. Définition et règles de calcul dans un anneau

Définition 2.11. Un **anneau** est la donnée d'un triplet $(A,+,\times)$, où A est un ensemble muni des lois de composition internes "$+$" et "$\times$" vérifiant les conditions suivantes :

(i) $(A,+)$ est un groupe abélien dont l'élément neutre est noté 0_A ou simplement 0 ;

(ii) la loi "$\times$" est associative ;

(iii) la loi "$\times$" possède un élément neutre noté 1_A ou simplement 1 ;

(iv) La loi "$\times$" est distributive par rapport à la loi "$+$".

Si de plus la loi "$\times$" est commutative, l'anneau $(A,+,\times)$ est appelé **anneau commutatif**.

Autrement dit :

$$(A,+,\times) \text{ est un anneau } \Leftrightarrow \begin{cases} (i)\ (A,+) \text{ est un groupe abélien ;} \\ (ii)\ (A,\times) \text{ est un monoïde unitaire ;} \\ (iii) \text{ La loi } \times \text{ est distributive par rapport à la loi } +, \text{c-à-d :} \\ \forall x,y,z\in A, \text{on a} \\ x\times(y+z)=(x\times y)+(x\times z) \text{ et } (y+z)\times x=(y\times x)+(z\times x). \end{cases}$$

Remarques 2.9. 1) Si aucune confusion n'est à craindre, on confond souvent un anneau $(A,+,\times)$ avec l'ensemble A (sans préciser les lois "$+$" et "$\times$").

2) Un anneau est toujours non vide.

3) Un anneau est en fait un triplet $(A,+,\times)$ qui vérifie les conditions (i), (ii) et (iv) de la définition (mais pas forcément la condition (iii)). Si de plus la condition (iii) est vérifiée, l'anneau A est dit unitaire.

4) Dans cette section, un anneau désigne un anneau unitaire.

5) L'élément neutre 0_A de $(A,+)$ (resp. 1_A) est appelé **le zéro** (resp. **l'unité**) de l'anneau A.

Exemples 2.10. 1) $(\mathbb{Z},+,\times)$ est un anneau commutatif. Il en est de même pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

2) Soit E un ensemble. $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif ($\mathcal{P}(E)$ désigne l'ensemble des parties de E).
   - L'élément neutre de $(\mathcal{P}(E), \Delta)$ est $\emptyset$.
   - L'élément neutre de $(\mathcal{P}(E), \cap)$ est E.

3) $(\mathbb{N}, +, \times)$ n'est pas un anneau, car $(\mathbb{N}, +)$ n'est pas un groupe.

4) $(2\mathbb{Z}, +, \times)$ n'est pas un anneau, car $1 \notin 2\mathbb{Z}$ (la condition (iii) de la définition d'un anneau n'est pas satisfaite).

Proposition 2.8 (Règles de calcul dans un anneau)**.** *Soit $(A, +, \times)$ un anneau.*

1) *Pour tout $x \in A$, $0 \times x = x \times 0 = 0$, on dit que 0 est un élément **absorbant**.*

2) *Pour tous $x, y \in A$, $x \times (-y) = (-x) \times y = -(x \times y)$ et $(-x) \times (-y) = x \times y$.*

3) *Pour tous $x, y, z \in A$, on a :*

$$x \times (y - z) = (x \times y) - (x \times z) \quad et \quad (y - z) \times x = (y \times x) - (z \times x).$$

Démonstration. 1) Montrons que $0 \times x = 0$ pour tout $x \in A$. En effet, on a :

$$0 \times x = (0 + 0) \times x = 0 \times x + 0 \times x.$$

En soustrayant $0 \times x$ des deux côtés de l'égalité, on obtient :

$$0 = 0 \times x.$$

Par un raisonnement similaire, on montre que $x \times 0 = 0$.

2) On a :

$$(x \times (-y)) + (x \times y) = x \times (-y + y) = x \times 0 = 0.$$

Ainsi, on en déduit que $x \times (-y) = -(x \times y)$.
De même, on obtient :

$$(-x) \times y = -(x \times y).$$

Comme application, on a : $(-x) \times (-y) = x \times y$.

3) Montrons maintenant que $x \times (y - z) = x \times y - x \times z$. On a :

$$x \times (y - z) = x \times (y + (-z)) = (x \times y) + (x \times (-z)),$$

on en déduit :

$$(x \times y) + (-(x \times z)) = x \times y - x \times z.$$

□

Remarque 2.4. Soit $(A,+, \times)$ un anneau. On a : $A = \{0_A\} \iff 0_A = 1_A$. En effet, si $A = \{0_A\}$, alors $1_A = 0_A$ car $1_A \in A$.

Réciproquement, supposons que $0_A = 1_A$ et montrons que $A = \{0_A\}$. Soit $x \in A$, donc $x = x \times 1_A = x \times 0_A = 0_A$. Par conséquent, $A \subseteq \{0_A\}$, ce qui implique $A = \{0_A\}$.

L'anneau $A = \{0_A\}$ est appelé **l'anneau nul** ou **l'anneau trivial**.

Dans toute cette section, nous ne considérons que les anneaux non triviaux, c'est-à-dire ceux pour lesquels $1_A \neq 0_A$.

Soit $(A, +, \times)$ un anneau. Pour tout $a \in A$,

1. les **multiples** de a sont définis par :
   (a) $0a = 0$ et $1a = a$;
   (b) pour tout entier $n \geq 2$, $na = \underbrace{a + a + \cdots + a}_{n\ fois}$;
   (c) pour tout $n \in \mathbb{N}^*$, $(-n)a = n(-a)$

   (a) les **puissances** de a sont définies par :
   (b) $a^0 = 1$ $(a \neq 0)$ et $a^1 = a$;
   (c) pour tout entier $n \geq 2$, $a^n = \underbrace{a \times a \times \cdots \times a}_{n\ fois}$;
   (d) si de plus a est inversible d'inverse a^{-1} alors, pour tout $n \in \mathbb{N}^*$, $a^{-n} = (a^{-1})^n$.

Proposition 2.9 (Autres règles de calcul dans un anneau)**.** *Soit $(A, +, \times)$ un anneau.*

1) *Pour tous $x, y \in A$ et tout $n \in \mathbb{Z}$, on a : $x \times (ny) = (nx) \times y = n(x \times y)$.*

2) *Pour tout $a \in A$ et pour tous $n, m \in \mathbb{Z}$, on a :*

$$(n + m) \times a = n \times a + m \times a \quad et \quad (n \times m) \times a = n \times (m \times a).$$

3) *Pour tout $a \in A$ et pour tous $n, m \in \mathbb{N}^*$, on a :*

$$a^n \times a^m = a^{n+m} \quad et \quad (a^n)^m = a^{n \times m},$$

4) *Si a et b sont deux éléments de A qui commutent, c'est-à-dire $a \times b = b \times a$, alors :*

   (i) Pour tout $n \in \mathbb{N}$, on a :

$$(a + b)^n = \sum_{k=0}^{n} C_n^k \, a^k \, b^{n-k} \quad \textit{(binôme de Newton)},$$

   où $C_n^k = \frac{n!}{k!(n-k)!}$.

   (ii) On a également :

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

   (iii) Pour tout $n \in \mathbb{N}^*$, on a :

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \cdots + a\,b^{n-2} + b^{n-1}\right).$$

   En particulier, on a :

$$1 - b^n = (1 - b)\left(1 + b + b^2 + \cdots + b^{n-1}\right).$$

Démonstration. À faire à titre d'exercice. □

Exercice 32. Soit $(A, +, \times)$ un anneau tel que $x^6 = x$, pour tout $x \in A$. Montrer que l'anneau A est commutatif.

Démonstration. Soit $x \in A$. On a $x^6 = (-x)^6$, donc $x = -x$ $(*)$, ou encore $2x = 0$ $(**)$. D'autre part, comme $1 \in A$, on a aussi $1 + x \in A$. Par hypothèse :

$$(1 + x)^6 = 1 + x.$$

Or, en développant le binôme de Newton, on a :

$$(1 + x)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1.$$

Ainsi, on obtient :

$$1 + x = x + 0 + x^4 + 0 + x^2 + 0 + 1 \text{ (par application de } (**)).$$

Par suite, on a :

$$1 + x = x + x^4 + x^2 + 1.$$

Il en résulte que $x^4 + x^2 = 0$, ce qui implique que $x^4 = -x^2 = x^2$. On en déduit que :

$$x^6 = x^4 \times x^2 = x^2 \times x^2 = x^4 = x^2.$$

Ainsi, $x^2 = x$ (d'après $(*)$).
Finalement, pour tous $x, y \in A$, on a :

$$(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2.$$

Donc :

$$x + y = x + xy + yx + y,$$

c'est-à-dire que $xy + yx = 0$.
Si $xy = -yx$, alors $yx = xy$ (d'après $(*)$). □

II.1.2. Anneaux produits et anneaux de fonctions

(1) **Anneaux produits :** Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On définit sur le produit cartésien $A \times B$ les lois produits notées aussi "+" et "×" par :
pour tout $(x, y) \in A \times B$ et tout $(x', y') \in A \times B$,

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y) \times (x', y') = (x \times x', y \times y').$$

On vérifie facilement que $(A \times B, +, \times)$ est un anneau. Si de plus les anneaux A et B sont commutatifs, alors l'anneau $A \times B$ est aussi commutatif.

Définition 2.12. L'anneau $(A \times B, +, \times)$ est appelé l'**anneau produit** des anneaux A et B.

Remarques 2.10. 1) Si $(A_1, +, \times), \ldots, (A_n, +, \times)$ sont des anneaux, alors $(A_1 \times A_2 \times \cdots \times A_n, +, \times)$ est l'anneau produit des anneaux $A_i, i = 1, \ldots, n$.

En particulier, si $(A, +, \times)$ est un anneau et $n \geq 2$ est un entier, alors $(A^n, +, \times)$ est un anneau produit.

2) L'élément neutre de $(A \times B, +)$ est $0_{A\times B} = (0_A, 0_B)$ et pour tout couple $(a, b) \in A \times B$, on a : $-(a, b) = (-a, -b)$.

3) L'élément neutre de $(A \times B, \times)$ est $1_{A\times B} = (1_A, 1_B)$.

Exemples 2.11. 1. $(\mathbb{Z} \times \mathbb{Q}, +, \times)$ est l'anneau produit (qui est commutatif) des anneaux $\mathbb{Z}$ et $\mathbb{Q}$.

2. $(\mathbb{Z}^2, +, \times)$ est un anneau commutatif, c'est l'anneau produit des anneaux $\mathbb{Z}$ et $\mathbb{Z}$.

(2) **Anneaux de fonctions** Soit I un ensemble non vide et $(A, +, \times)$ un anneau. On considère l'ensemble $\mathcal{F}(I, A)$ des fonctions définies sur I et à valeurs dans l'anneau A.

On définit sur $\mathcal{F}(I, A)$ les lois de composition internes (faciles à vérifier) notées également "+" et "×" par : Pour tous $f, g \in \mathcal{F}(I, A)$ et tout $x \in I$:

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (f \times g)(x) = f(x) \times g(x).$$

On vérifie sans peine que $(\mathcal{F}(I, A), +, \times)$ est un anneau, appelé **anneau des fonctions définies sur I et à valeurs dans** A. Si de plus l'anneau A est commutatif, alors $\mathcal{F}(I, A)$ est un anneau commutatif.

- L'élément neutre de $(\mathcal{F}(I, A), +)$ est la fonction nulle :

$$\theta : I \longrightarrow A, \quad x \longmapsto \theta(x) = 0_A.$$

Pour tout $f \in \mathcal{F}(I, A)$, on a :

$$(-f)(x) = -f(x), \quad \forall x \in I.$$

- L'élément neutre de $(\mathcal{F}(I, A), \times)$ est la fonction constante égale à 1_A :

$$1_{\mathcal{F}(I,A)} : I \longrightarrow A, \quad x \longmapsto 1_{\mathcal{F}(I,A)}(x) = 1_A.$$

Exemple 2.1. L'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un anneau, où $\mathcal{F}(\mathbb{R}, \mathbb{R})$ désigne l'ensemble des fonctions définies sur $\mathbb{R}$ et à valeurs dans $\mathbb{R}$.