ALGEBRE 1

(2020 - 2021)

Table des matières

Chapitre 1

Ensembles

1.1 Définitions, Exemples

Définition 1.1.1.
On appelle ensemble toute collection d'objets bien déterminés dans laquelle les objets sont uniques. Ces objets s'appellent éléments de l'ensemble, ou les points de l'ensemble.

Remarque 1.1.1.
Si x est un point d'un ensemble A, on ecrit $x \in A$ et on lit "x appartient à A" ou "x est élément de A" ou "A contient x".
Si x n'est pas un point d'un ensemble A, on ecrit $x \notin A$ et on lit "x n'appartient pas à A" ou "x n'est pas élément de A" ou "A ne contient pas x".

Remarque 1.1.2.

- *Un ensemble peut être fini ou non.*
- *Les ensembles rencontrés dans la vie courante, si vastes soient-ils sont finis. En mathématiques, nous considérerons des ensembles non finis appelés infinis.*
- *Un ensemble peut être concrêt ou imaginaire.*

Remarque 1.1.3.
Un ensemble E est bien défini lorsqu'on possède un critère permettant d'affirmer pour tout objet a, s'il appartient à l'ensemble E ou n'appartient pas à l'ensemble E.

Remarque 1.1.4.
Un même être mathématique ne peut être à la fois un ensemble et un élément de cet ensemble, c'est-à-dire nous nous interdisons d'écrire $a \in a$.

Exemples 1.1.1.

1. $0, 1, 2, 3, \cdots$ *les entiers naturels forment un ensemble qui est noté* $\mathbb{N}$. $\mathbb{N}$ *n'est pas un ensemble fini.*

2 *L'ensemble des couleurs de l'arc-en-ciel est un ensemble fini.*

3 *L'ensemble de tous les points d'un plan,*

4 *L'ensemble des étudiants de l'UPB inscrits pour cette année universitaire :*

5 $a, b, c, \cdots, z$ *sont lettres de l'alphabet français.*

6 *La collection* $\{*, 1, *\}$ *n'est pas un ensemble.*

Notation 1.1.1.

— *L'ensemble qui n'a aucun élément est dit vide et est noté* $\emptyset$ *ou* $\{\}$.

— *Un ensemble qui n'a qu'un seul élément* x *est noté* $\{x\}$ *et est appelé singleton.*

— *Un ensemble constitue de deux éléments* s, x *est noté* $\{s, x\}$, *ou* $\{x, s\}$ *et est appelé paire.*

1.2 Ecritures d'un ensemble

On peut écrire un ensemble de deux façons :

Définition 1.2.1 (écriture en extension)**.**
Écrire un ensemble en extension veut dire donner une liste de tous ses éléments.

Exemple 1.2.1.

1 *« Dans* A *il y a les éléments 1, 2, 3, 4, 5, 6 et 7 » est une définition en extension. On écrit :*

$$A = \{1; 2; 3; 4; 5; 6; 7\}.$$

2 *l'ensemble E de tous les entiers naturels inferieurs ou egal a 6 est ecrit en extension :*

$$E = \{0, 1, 2, 3, 4, 5, 6\}.$$

Définition 1.2.2 (écriture en compréhension)**.**
Écrire un ensemble en compréhension veut dire donner une propriété caractéristique de ses éléments.

Exemples 1.2.1.

— *« Dans* A *il y a les nombres entiers de 1 à 7 » est une définition en compréhension. on écrit :*

$$A = \{x | x \text{ est un nombre entier de 1 à 7}\}.$$

— *L'ensemble* P *de tous les entiers relatifs pairs est ecrit en comprehension :*

$$P = \{2n,\ n \in \mathbb{Z}\}.$$

— *L'ensemble* S *de toutes les puissances entières de 3 est écrit en comprehension :*

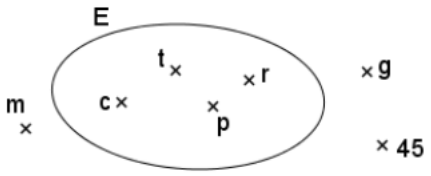
$$S = \{3^n,\ n \in \mathbb{Z}\}.$$

1.3 Diagrammes de Venn

1.3.1 Représentation d'un ensemble

Pour représenter un ensemble on dessine une ligne fermée appelée **diagramme de Venn** et on met les éléments de l'ensemble à l'intérieur de cette ligne, les autres à l'extérieur.

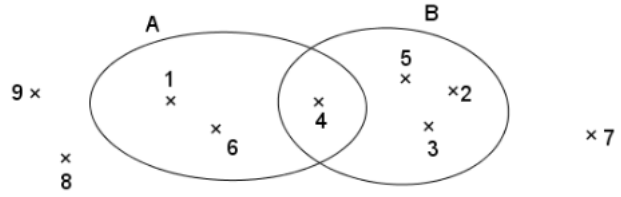
Exemple **1.3.1.** $E = \{c; t; r; p\}$



1.3.2 Représentation de deux ensembles

Pour représenter deux ensembles sur un même diagramme de Venn, il faut prévoir un endroit pour les éléments qui appartiennent aux deux ensembles à la fois, pour les éléments qui n'appartiennent qu'à un seul des deux ensembles et pour ceux qui n'appartiennent à aucun des deux ensembles. Chaque élément ne doit en effet figurer qu'une seule fois sur un diagramme !

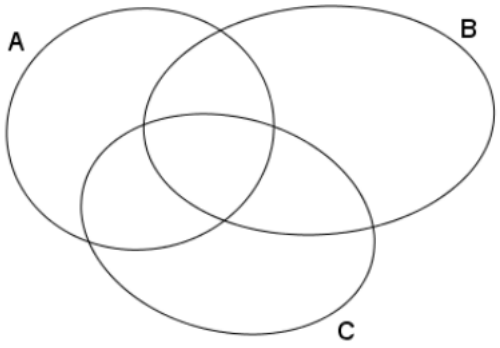
Exemple **1.3.2.** $E = \{1; 2; 3; 4; 5; 6; 7; 8\}$, $A = \{1; 4; 6\}$ *et* $B = \{2; 3; 4; 5\}$



1.3.3 Représentation de trois ensembles

Pour représenter trois ensembles sur un même diagramme, on dessine un « diagramme en trèfle » qui permet de prévoir tous les cas : il y en a 8 en tout ! (essayez de les décrire)

Exemple **1.3.3.** $A = \{1; 2; 5; 7; 9\}$, $B = \{4; 5; 6; 7; 9; 10\}$ *et* $C = \{1; 3; 6; 7; 8; 9; 10\}$
Placez vous-mêmes les entiers de 0 à 12 sur le diagramme suivant :

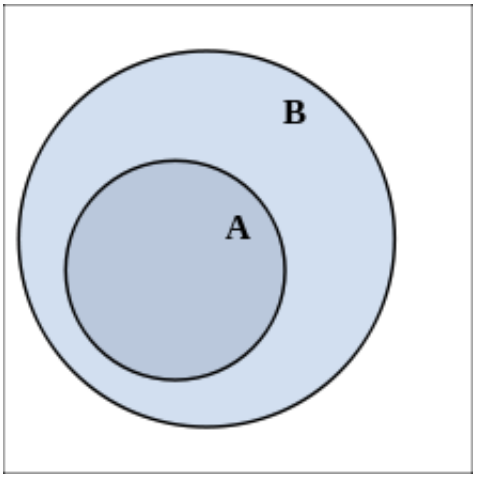


1.4 Inclusion, égalité, ensemble des parties

1.4.1 Inclusion

Définition 1.4.1. *Soient E et F deux ensembles. On dira que E est inclus dans F si tout élément de E est élément de F. On dit encore que E est un sous-ensemble de F ou E est une partie de F. On écrit dans ce cas $E \subset F$ ou $F \supset E$.*

Exemple 1.4.1.



$A \subset B$

Exemples 1.4.1.

— *L'ensemble des poulets est contenu dans celui des oiseaux.*

— *L'ensemble*

$$\left\{ \frac{\cos x}{2+n};\ x \in \mathbb{R},\ n \in \mathbb{N} \right\}$$

est contenu dans $]-1,1[$.

— $\{*\} \subset \{*, \triangle\}$, $\{\triangle\} \subset \{*, \triangle\}$, $\{*, \square\} \not\subseteq \{\square, \triangle, O\}$ *et* $\{\square, \triangle, O\} \not\subseteq \{*, \square\}$.

Remarque 1.4.1.

1. *On convient que l'ensemble vide $\emptyset$ est contenu dans tout ensemble.*
2. *On a bien $E \subset E$.*
3. *Si $E \subset F$ et $F \subset G$, alors $E \subset G$.*

Exercice 1. *Soit E l'ensemble $\{*, \triangle, O\}$. Trouver tous les sous-ensembles de E.*

1.4.2 Ensembles égaux

Définition 1.4.2. *Deux ensembles sont égaux s'ils ont les mêmes éléments.*

Exemple 1.4.2.

— *Les ensembles $A = \{1; 2; 3; 4\}$ et $B =]0; 4] \cap \mathbb{N}$ sont égaux.*

— *Les ensembles $C = \{1; 2; 3; 7\}$ et $D = \{8; 4; 2; 1\}$ ne sont pas égaux*

Proposition 1.4.1. *Deux ensembles A et B sont égaux si et seulement si A est inclus dans B et B est inclus dans A.*

Remarque 1.4.2. *La méthode la plus courante pour montrer que deux ensembles sont égaux est d'ailleurs de procéder par double inclusion, c'est à dire de montrer d'abord que A est inclus dans B, puis que B est inclus dans A.*

1.4.3 Ensemble des parties

Définition 1.4.3. *Toutes les parties d'un ensemble E décrivent un nouvel ensemble appelé ensemble des parties de E et noté $\mathcal{P}(E)$; on a donc :*

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

Remarque 1.4.3.

— *Soit E est un ensemble. Si $card(E) = n$, alors $card(\mathcal{P}(E)) = 2^n$.*

— *si a est élément de E (non vide) :*

$$a \in E \Leftrightarrow \{a\} \subset E \Leftrightarrow \{a\} \in \mathcal{P}(E).$$

1.5 Opérations élémentaires dans les ensembles

1.5.1 Activité

Activité 1.5.1.

1 *Représentez sur un même diagramme de Venn des ensembles :* $A = \{1; 2; 3; 4; 5\}$ *et* $B = \{4; 5; 6; 7\}$*, en ne représentant chaque élément qu'une seule fois.*

2 *Placez sur ce diagramme les éléments 13 et 29,5.*

On constate que sur ce diagramme il y a quatre sortes d'éléments, ceux qui appartiennent :

- *à* A *et à* B *:*$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$
- *à* A *mais pas à* B *:*$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$
- *à* B *mais pas à* A *:*$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$
- *ni à* A*, ni à* B *:*$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

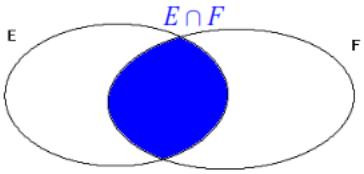
Combien existe-t-il d'éléments qui n'appartiennent ni à A*, ni à* B *?*$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$.
On a aussi ceux qui appartiennent à A *ou à* B *:* $\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$.

1.5.2 Intersection d'ensembles

Définition 1.5.1. *On appelle intersection de 2 ensembles* E *et* F*, le nouvel ensemble constitue des objets* a *tels que* $a \in E$ *et* $a \in F$*. Cet ensemble est note* $E \cap F$*. On définit de la même façon l'intersection de 3 ou de plusieurs ensembles.*

Formellement, $x \in E \cap F \Leftrightarrow (x \in E \quad et \quad x \in F)$.

Exemple 1.5.1.



Exemples 1.5.1. **1** *Pour l' activité 1.5.1 :* $A \cap B = \{\cdots\cdots\cdots\}$.

2 *si* $A = \{2, 5, 7\}$ *et* $B = \{1, 5, 7, 9\}$*, on a* $A \cap B = \{5, 7\}$.

3 *Soit* $A = \{a; b; d; e; f; g\}$, $B = \{a; d; g; i; j; k\}$ *et* $C = \{b; e; f; l; m\}$

$$A \cap B \cap C = \emptyset.$$

Remarque 1.5.1.
— $A \cap B = B \cap A$.
— $A \cap B \subset A$ *et* $A \cap B \subset B$.
— $A \cap A = A$, $\emptyset \cap A = \emptyset$.
— *Si* $A \cap B = \emptyset$*, on dit que* A *et* B *sont disjoints.*

— *Des ensembles* $A_1, A_2, \cdots, A_n$ *sont deux à deux disjoints si pour tous* i *et* j *dans* $\{1, 2, \cdots, n\}$,

$$i \neq j \Rightarrow A_i \cap A_j = \emptyset.$$

— *Notons que* $a \notin A \cap B$ *signifie qu'on est dans l'une des 3 situations suivantes :*

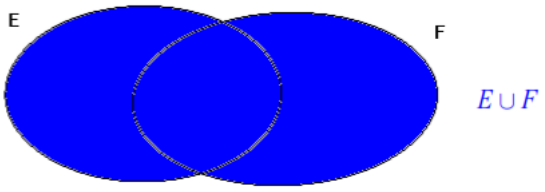
$$(1) \quad a \notin A \quad et \quad a \in B \qquad ou \quad (2) \quad a \notin B \quad et \quad a \in A \qquad ou \quad (3) \quad a \notin A \quad et \quad a \notin B.$$

1.5.3 Réunion d'ensembles

Définition 1.5.2. *On appelle réunion de 2 ensembles* E *et* F*, le nouvel ensemble constitue des objets* a *tels que* $a \in E$ *ou* $a \in F$*. Cet ensemble est note* $E \cup F$*. On définit de la même façon la reunion de 3 ou de plusieurs ensembles.*

Formellement, $x \in E \cup F \Leftrightarrow (x \in E \quad ou \quad x \in F)$.

Exemple 1.5.2.



Exemples 1.5.2.

1 *Pour l' activité 1.5.1 :* $A \cup B = \{\cdots\cdots\cdots\}$.

2 *Si* $A = \{2, 5, 7\}$ *et* $B = \{1, 5, 7, 9\}$*, on a* $A \cup B = \{1, 2, 5, 7, 9\}$.

3 *Soit* $A = \{a; b; d; e; f; g\}$, $B = \{a; d; g; i; j; k\}$ *et* $C = \{b; e; f; l; m\}$

$$A \cup B \cup C = \{a; b; d; e; f; g; i; j; k; l; m\}.$$

Remarque 1.5.2.

— $A \cup B = B \cup A$.

— $A \subset A \cup B$ *et* $B \subset A \cup B$.

— $A \cup A = A$, $\emptyset \cup A = A$.

— $A \cup B = \emptyset$ *que si* $A = \emptyset$ *et* $B = \emptyset$.

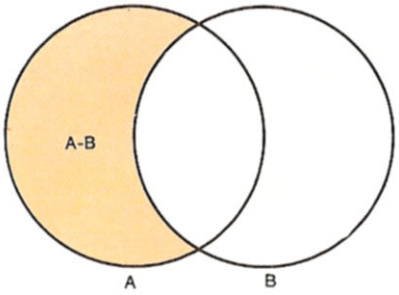
— *Notons que* $a \notin A \cup B$ *signifie que :* $a \notin A$ *et* $a \notin B$.

1.5.4 Différence de deux ensembles

Définition 1.5.3. *Soient A et B deux ensembles. On appelle "A moins B", et on note $A\backslash B$ ou $A - B$, l'ensemble des éléments de A qui ne sont pas dans B. On a donc :*

$$x \in A \setminus B \; ssi \; (x \in A \; et \; x \notin B).$$

Exemple 1.5.3.



Exemples 1.5.3.

- *Pour l' activité 1.5.1 :* $A\backslash B = \{\cdots\cdots\cdots\}$
- *Si* $A = \{2, 5, 7\}$ *et* $B = \{1, 5, 7, 9\}$, *on a* $A \setminus B = \{2\}$ *et* $B \setminus A = \{1, 9\}$.

Remarque 1.5.3.

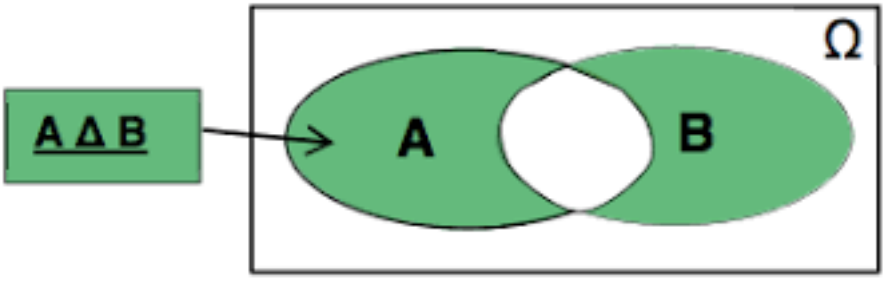
- *Pour tout ensemble A, on a* $A \setminus \emptyset = A$, *et* $A\backslash A = \emptyset$.
- *De plus, pour tous ensembles A et B, on a* $A \subset B$ *ssi* $A \setminus B = \emptyset$.

1.5.5 Différence symétrique entre deux ensembles

Définition 1.5.4. *La différence symétrique entre deux ensembles A et B est l'ensemble des éléments qui n'appartiennent qu'à A ou à B. Cet ensemble est note $A\triangle B$. On a donc :*

$$x \in A\triangle B \; ssi \; (x \in A\backslash B \; ou \; x \in B\backslash A).$$

Exemple 1.5.4.



Exemples **1.5.4.**

— *Pour l' activité 1.5.1 :* $A\triangle B = \{\cdots\cdots\cdots\}$

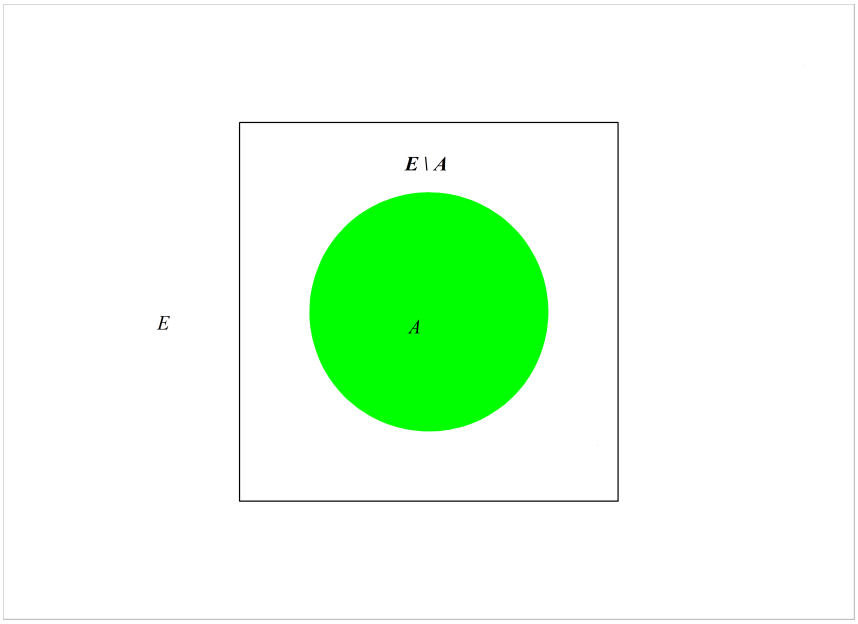
— *Si* $A = \{2, 5, 7\}$ *et* $B = \{1, 5, 7, 9\}$*, on a* $A \setminus B = \{2\}$ *et* $B \setminus A = \{1, 9\}$ *donc* $A\triangle B = \{1, 2, 9\}$.

1.5.6 Le complémentaire d'un ensemble contenu dans un autre

Définition **1.5.5.** *Soient* E *un ensemble et* A *une partie de* E*. On appelle complémentaire de* A *dans* E*, le sous-ensemble de* E *constitue des* $a \in E$ *tels que* $a \notin A$*. Cet ensemble est note* $E - A$ *ou* $E \setminus A$ *ou* $C_E A$ *ou* $\overline{A}$*.*

Formellement, $x \in E \setminus A \Leftrightarrow (x \in E \quad et \quad x \notin A)$.

Exemple **1.5.5.**



Exemples **1.5.5.**

1 *Soit* $E = \{1, 2, 3, 4, 5\}$. *Soit* $A = \{2, 3\}$. *On a* $C_E(A) = \{1, 4, 5\}$. *Soit* $B = C_E(A)$. *On a* $C_E(B) = \{2, 3\} = A$.

2 *Soit* $E = \mathbb{R}$. *Soit* $A = [0, 1]$. *On a*

$$C_{\mathbb{R}}(A) = \{x \in \mathbb{R},\ x \notin [0, 1]\} =]-\infty, 0[\cup]1, +\infty[.$$

Soit $B = C_E(A)$. *On a* $C_E(B) = [0, 1] = A$.

Remarque **1.5.4.** *Si* $A \subset E$, *on a :*

— $A \cap C_E A = \emptyset$ *et* $A \cup C_E A = E$.

— $C_E(C_E A) = A$, $C_E E = \emptyset$ *et* $C_E \emptyset = E$.

1.5.7 Propriétés des opérations élémentaires

Soit E, F et G trois ensembles.

(i) — $E \cup F = F \cup E$,

— $E \cap F = F \cap E$,

— $E \triangle F = F \triangle E$,

on dit que la réunion, l'intersection et la différence symétrique sont des opérations commutatives.

(ii) — $E \cup (F \cup G) = (E \cup F) \cup G$,

— $E \cap (F \cap G) = (E \cap F) \cap G$,
— $E \triangle (F \triangle G) = (E \triangle F) \triangle G$,
on dit que la réunion, l'intersection et la différence symétrique sont des opérations associatives.

(iii) — $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$,
— $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$,
On dit que l'intersection et la réunion sont distributives l'une sur l'autre.

(iv) Si A et B sont deux parties de E, alors $A \cap B$, $A \cup B$, $C_E A$, $C_E B$, $C_E A \cup B$, $C_E A \cap B$ sont toutes des parties de E, et on a

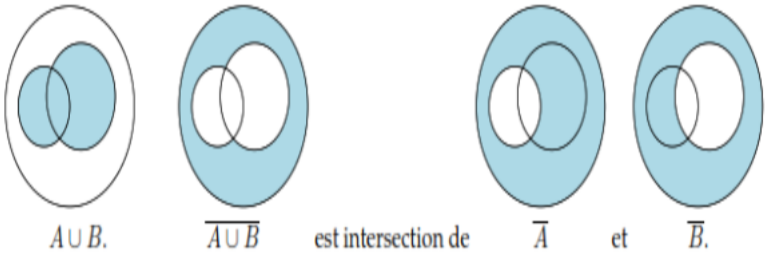
$$C_E(A \cap B) = (C_E A) \cup (C_E B) \qquad C_E(A \cup B) = (C_E A) \cap (C_E B).$$

(v) $E \triangle \emptyset = E$, on dit que la différence symétrique possède un élément neutre.

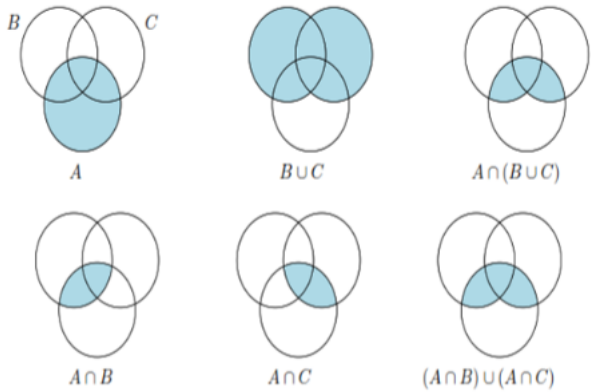
(vi) $A \triangle B = (A \cup B) - (A \cap B)$.

Remarque **1.5.5.** *Ces règles sont faciles à comprendre si on les visualise à l'aide de diagrammes.*

Exemple **1.5.6.** *Illustration de* $\overline{A \cup B} = \overline{A} \cap \overline{B}$



Exemple **1.5.7.** *Illustration de* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



1.5.8 Produit cartésien d'ensembles

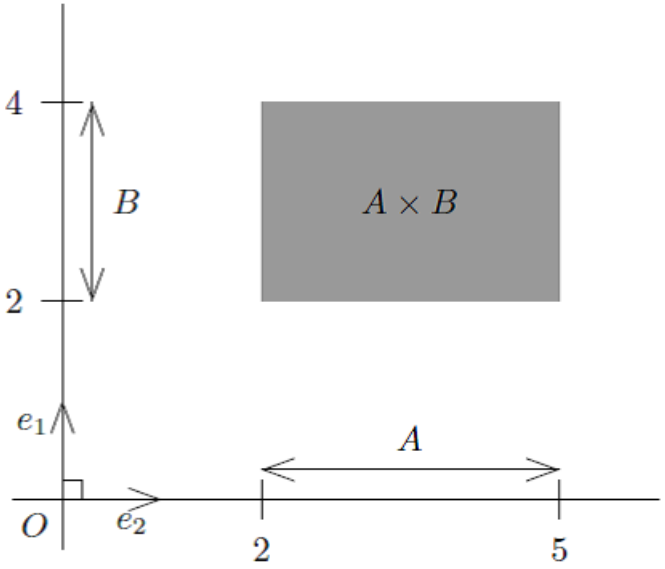
Définition **1.5.6.** *Soient* E *et* F *deux ensembles. On appelle produit cartesien de* E *par* F*, l'ensemble de tous les couples* (x, y) *où* $x \in E$ *et* $y \in F$*. On le note* $E \times F$.

Plus généralement si $E_1, E_2, \cdots, E_n$ sont n ensembles, on appelle prodruit cartesien de $E_1, E_2, \cdots E_n$ l'ensemble de tous les $n-$uplets $(x_1, x_2, \cdots, x_n)$ où $x_1 \in E_1$, $x_2 \in E_2, \cdots, x_n \in E_n$. On le note

$$E_1 \times E_2 \times \cdots \times E_n.$$

Exemple 1.5.8.

• Si $A = [2,5]$ et $B = [2,4]$, le produit $A \times B$ est un sous-ensemble de $\mathbb{R}^2$ qui peut être représenté par le rectangle sur la figure ci-dessous.



Exemples 1.5.6.

— *Si $A = \{1,2,3\}$ et $B = \{1,7\}$, alors*

$$A \times B = \{(1,1),(1,7),(2,1),(2,7),(3,1),(3,7)\}$$

et

$$B \times A = \{(1,1),(1,2),(1,3),(7,1),(7,2),(7,3)\}$$

— *Si $A = \{saumon, poulet\}$ et $B = \{banane, orange\}$, alors*

$A \times B = \{(saumon, banane),(saumon, orange),(poulet, banane),(poulet, orange)\}$.

Remarque 1.5.6.

1 *On convient de noter $E \times E$ par E^2, et plus généralement $\underbrace{E \times E \times \cdots \times E}_{n fois}$ par E^n.*

2 *$E \times F = \emptyset$ ssi $E = \emptyset$ ou $F = \emptyset$.*

3 $A \times B \subset E \times P$ *ssi* $A \subset E$ *et* $B \subset P$.

4 $E \times P \neq P \times E$, $E \nsubseteq E \times P$. *En particulier* $E \nsubseteq E^2$.

5 *Si* E *et* P *sont des ensembles finis, on a*

$$Card(E \times P) = Card(E).Card(P).$$

1.5.9 Partition d'un ensemble

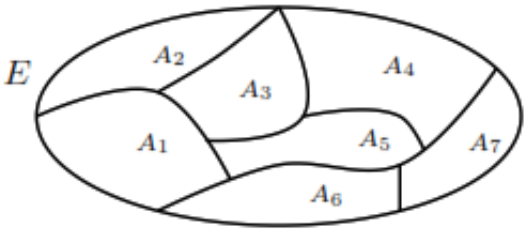
Définition **1.5.7.** *Soit* E *un ensemble. On appelle partition de l'ensemble* E *toute famille* $\{A_i\}_{i \in I}$ *de sous-ensembles de* E *telle que :*

1 $A_i \neq \emptyset$, $\forall i \in I$.

2 *si* $i \neq j$, *on a* $A_i \cap A_j = \emptyset$

3 $E = \bigcup_{i \in I} A_i$

Exemple **1.5.9.**



Exemple **1.5.10.** *Si* $A \subset E$, *la paire* $\{A, C_E A\}$ *est une partition de* E.

Chapitre 2

Eléments de logique

2.1 Opérations logiques dans un ensemble

Soit A un ensemble. Soient P, Q, $R \cdots$ des propriétés que peuvent posséder les éléments de A. Par exemple : A est l'ensemble des etudiants de l'UPB,

— P : avoir le Bac C ;

— Q : avoir moins de 20 ans ;

— R : avoir obtenu la mention assez-bien ;

— S : avoir le Bac D.

Partant de ces propriétés, on peut en construire de nouvelles à l'aide des opérations logiques élémentaires :

2.1.1 Opérations logiques élémentaires

1) $nonP$ **(négation de** P **)** :
Dire que l'élément $x \in A$ possède la propriété $nonP$, c'est dire que x ne possède pas la propriété P.

2) P **et** Q **(conjonction de** P **et** Q**)** :
Dire que l'élément $x \in A$ possède la propriété P et Q, c'est dire que x possède à la fois la propriété P et la propriété Q.

3) P **ou** Q **(disjonction de** P **et** Q**)** :
Dire que l'élément $x \in A$ possède la propriété P ou Q, c'est dire que x possède soit la propriété P , soit la propriété Q, soit les deux à la fois.

2.1.2 L'implication et l'équivalence de deux propriétés

— **L'implication conditionnelle de** P **et** Q.
On dit que la propriété P implique la propriété Q et on ecrit $P \Rightarrow Q$, si tout

élément $x \in A$ possedant la propriété P , possède la propriété Q.

A $\Rightarrow$ B se traduit aussi
A implique B
A entraîne B
si A est vrai alors B est vrai
B est vrai si A est vrai
A est vrai seulement si B est vrai
pour que B soit vrai il suffit que A le soit
A est une condition suffisante pour B
pour que A soit vrai il faut que B le soit
B est une condition nécessaire pour A

— **L'équivalence des propretes P et Q.**
On dit que la propriété P est équivalente à la propriété Q et on écrit $P \Leftrightarrow Q$, si les éléments $x \in A$ possedant la propriété P sont les mêmes que ceux qui possèdent la propriété Q.

A $\Leftrightarrow$ B se traduit aussi
A est équivalent à B A équivaut à B
A entraîne B et réciproquement
si A est vrai alors B est vrai et réciproquement
A est vrai si et seulement si B est vrai
pour que A soit vrai il faut et il suffit que B le soit
A est une condition nécessaire et suffisante pour B

2.2 La table de vérité des différentes propriétés

P	Q	P et Q	P ou Q	$P \Rightarrow Q$	nonP	(nonP) ou Q	$P \Leftrightarrow Q$
V	V	V	V	V	F	V	V
V	F	F	V	F	F	F	F
F	V	F	V	V	V	V	F
F	F	F	F	V	V	V	V

2.3 Les quantificateurs

En mathématiques, il existe deux quantificateurs, le quantificateur **universel** "quel que soit", noté $\forall$, et le quantificateur **existentiel** ou quantificateur **d'existence** "il existe", noté $\exists$.

Exemple 2.3.1.

— *Affirmer que tout élément x dans un ensemble E possède la propriété P s'ecrit :*

$$\forall x \in E \text{ tel que } x \text{ vérifie } P.$$

— *Affirmer qu'il existe un élément x au moins dans un ensemble E qui possède la propriété P s'ecrit :*

$$\exists x \in E \text{ tel que } x \text{ verifie } P.$$

— *Affirmer que pour toute série du Bac, il y a eu au moins un admis, se note :*

$$\forall s \in B, \exists e \in E \text{ tel que e ait obtenu } s,$$

où B est l'ensemble des séries de bac et E l'ensemble des élèves.

— *"Un aliment est bien consomme par tous les hommes", s'ecrit :*

$$\exists r E A \text{ tel que } \forall h \in H,\ h \text{ mange } r.$$

où A est l'ensemble des aliments et H l'ensemble des Hommes.

— *"Tous les hommes mangent tous les aliments" s'ecrit ; $\forall h \in H$, $\forall r \in A$, h mange r.*

où A est l'ensemble des aliments et H l'ensemble des Hommes.

2.4 Correspondance entre sous-ensembles et propriétés

Supposons qu'aux propriétés P et Q correspondent respectivement les sous-ensembles A et B de l'ensemble E. Nous pouvons établir le tableau suivant donnant les correspondances entre parties d'un ensemble E et propriétés définies sur cet ensemble E :

propriété	sous-ensemble correspondant
nonP	$C_E A$
P et Q	$A \cap B$
P ou Q	$A \cup B$
$P \Rightarrow Q$ c-à-d $\left(\forall x \in E, \text{P(x)} \Rightarrow \text{Q(x)}\right)$	$A \subset B$
$P \Leftrightarrow Q$ c-à-d $\left(\forall x \in E, \text{P(x)} \Leftrightarrow \text{Q(x)}\right)$	$A = B$

Les règles de calcul dans les ensembles correspondent aux règles de calcul logique :

Règle de calcul dans les ensembles	Règle de calcul logique correspondante
$A \cup B = B \cup A$	P ou Q $\Leftrightarrow$ Q ou P
$A \cap B = B \cap A$	P et Q $\Leftrightarrow$ Q et P
$A \cap B = \emptyset$	$\forall x \in E$, P(x), Q(x) incompatibles
$A \cap B = \emptyset$ et $A \cup B = E$	$\forall x \in E$, Q(x) $\Leftrightarrow$ non P(x)
$C_E(A \cup B) = (C_E A) \cap (C_E B)$	non(P ou Q) $\Leftrightarrow$ (non P) et (non Q)
$C_E(A \cap B) = (C_E A) \cup (C_E B)$	non(P et Q) $\Leftrightarrow$ (non P) ou (non Q)
$A \subset B \Leftrightarrow C_E B \subset C_E A$	(P $\Rightarrow$ Q) $\Leftrightarrow$ (non Q $\Rightarrow$ non P)
$C_E(C_E A) = A$	$\forall x \in E$, non (non P(x)) $\Leftrightarrow$ P(x)

Définition **2.4.1.** *nonQ $\Rightarrow$ nonP est appelée la contraposée de l'implication P $\Rightarrow$ Q*

2.5 Logique mathématique classique

Définition **2.5.1** (Assertion)**.** *Une assertion est un énoncé dont on peut affirmer sans ambiguïté s'il est vrai ou s'il est faux.*

Exemple **2.5.1.** *Les affirmations suivantes sont des assertions :*

- *Tout polygône regulier de n cotés s'inscrit dans un cercle.*
- *Après la voiture, on inventa l'avion.*
- *un jour un africain inventera une montre.*
- $3 < 10$ *est une assertion vraie.*
- $5 < 2$ *est une assertion fausse.*

Exemple **2.5.2.** *les affirmations suivantes ne sont pas des assertions :*

- *L'algèbre est plus facile que l'analyse*
- *C'est jolie le ciel.*
- *Sur Mars la vie est meilleure.*

Définition **2.5.2** (Proposition)**.** *Une proposition est un énoncé qui contient des variables, qui est vrai pour certaines valeurs attribuées à ces variables.*

Exemples **2.5.1.**

1. $x > 10$ *est une proposition, elle est vraie pour les nombres strictement supérieurs à 10, fausse dans tous les autres cas.*
2. *Une hauteur du triangle T est médiane du triangle T est une proposition vraie pour les triangles T isocèles, fausse dans tous les autres cas.*

Remarque **2.5.1.** *Comme pour les propriétés, à partir d'assertions ou de propositions, on peut definir de nouvelles, par la negation nonP , la conjonction P et Q, la disjonction P ou Q, l'implication $P \Rightarrow Q$ et l'equivalence $P \Leftrightarrow Q$. Ces nouvelles propositions sont definies par la table de verite suivante :*

P	Q	P et Q	P ou Q	$P \Rightarrow Q$	nonP	(nonP) ou Q	$P \Leftrightarrow Q$
V	V	V	V	V	F	V	V
V	F	F	V	F	F	F	F
F	V	F	V	V	V	V	F
F	F	F	F	V	V	V	V

2.6 Quelques méthodes de démonstration

2.6.1 Raisonnement direct

a) Principe

Une démonstration directe de $p \Rightarrow q$ consiste à supposer que p est vraie et étuliser la transitivité de l'implication pour prouver que q est vraie, i.e., en supposant que p est vraie et si les implications $p \Rightarrow r_1$, $r_1 \Rightarrow r_2$, $\cdots$, $r_n \Rightarrow q$ sont vraies, où r_1,$\cdots$, r_n sont des assertions ou des propositions, alors q est vraie.

b) Exemples

Exemple 2.6.1. *Montrer que si $a, b \in \mathbb{Q}$ alors $a + b \in \mathbb{Q}$.*

Démonstration. Prenons $a \in \mathbb{Q}$, $b \in \mathbb{Q}$. Rappelons que les élément de $\mathbb{Q}$ sont les réels s'écrivant $\frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Alors $a = \frac{p}{q}$ pour un certain $p \in \mathbb{Z}$ et un certain $q \in \mathbb{N}^*$. De même $b = \frac{p'}{q'}$ pour un certain $p' \in \mathbb{Z}$ et un certain $q' \in \mathbb{N}^*$. Maintenant $a + b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq'+qp'}{qq'}$. Or le numérateur $pq' + qp'$ est bien un élément de $\mathbb{Z}$; le dénominateur qq' est lui un élément de $\mathbb{N}^*$. Donc $a+b$ s'écrit bien de la forme $a + b = \frac{p''}{q''}$ avec $p'' \in \mathbb{Z}$, $q'' \in \mathbb{N}^*$. Ainsi $a + b \in \mathbb{Q}$. □

Exemple 2.6.2. *Montrer que si $x < 1$ alors $|x - 4| > 3$.*

Démonstration. Si $x < 1$ alors $x - 4 < -3$ et donc $|x - 4| > 3$. □

2.6.2 Raisonnement par double implication

a) Principe

Pour prouver une équivalence, on peut prouver séparément les deux implications, directe et réciproque.

b) Exemples

Exemple 2.6.3. *Soit deux réels a et b. Montrer que :*

$$(\forall n \in \mathbb{N},\ (a \times 2^n + b \times 3^n = 0) \Longleftrightarrow (a = b = 0).$$

Démonstration. (a) Montrons que $(a \times 2^n + b \times 3^n = 0) \Longrightarrow (a = b = 0)$.
Supposons que $\forall n \in \mathbb{N}$, $a \times 2^n + b \times 3^n = 0$. Et montrons qu'alors $a = b = 0$. Comme $a \times 2^n + b \times 3^n = 0$ est vraie pour tout $n \in \mathbb{N}$, l'égalité est en particulier vraie pour $n = 0$ et pour $n = 1$, ce qui donne

$$a \times 2^0 + b \times 3^0 = 0$$

et

$$a \times 2^1 + b \times 3^1 = 0$$

Autrement dit, $a + b = 0$ et $2a + 3b = 0$. La première égalité implique que $a = -b$. En remplaçant a par $-b$ dans la deuxième, on obtient alors $-2b + 3b = 0$, c'est à dire $b = 0$. Comme $a = -b$, on en conclut que $a = b = 0$.

(b) Montrons maintenant que $(a = b = 0) \Longrightarrow (a \times 2^n + b \times 3^n = 0)$.
Supposons donc que $a = b = 0$ et montrons que $\forall n \in \mathbb{N}$, $a \times 2^n + b \times 3^n = 0$.
Soit $n \in \mathbb{N}$. Comme $a = b = 0$, on a

$$a \times 2^n + b \times 3^n = 0 \times 2^n + 0 \times 3^n = 0 + 0 = 0.$$

D'où le résultat. □

Exemple **2.6.4.** *Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction. Montrer que " f est une fonction a la fois paire et impaire" $\Longleftrightarrow$ " f est la fonction nulle".*

Démonstration. □

2.6.3 Cas par cas

a) Principe

Pour montrer que r est vraie, il suffit de montrer que : "p ou q" est vraie et que les implications p⇒ r et q ⇒ r sont vraies.

b) Exemples

Exemple **2.6.5.** *Montrer que pour tout $x \in \mathbb{R}$, $|x - 1| \leq x^2 - x + 1$.*

Démonstration. Soit $x \in \mathbb{R}$. Nous distinguons deux cas. Premier cas : $x > 1$. Alors $|x - 1| = x - 1$. Calculons alors $x^2 - x + 1 - |x - 1|$.

$$\begin{aligned} x^2 - x + 1 - |x - 1| &= x^2 - x + 1 - (x - 1) \\ &= x^2 - 2x + 2 \\ &= (x - 1)^2 + 1 > 0 \end{aligned}$$

Ainsi $x^2 - x + 1 - |x - 1| > 0$ et donc $x^2 - x + 1 > |x - 1|$. Deuxième cas : $x < 1$. Alors $|x - 1| = -(x - 1)$. Nous obtenons $x^2 - x + 1 - |x - 1| = x^2 - x + 1 + (x - 1) = x^2 \geq 0$. Et donc $x^2 - x + 1 \geq |x - 1|$. Conclusion. Dans tous les cas $|x - 1| \leq x^2 - x + 1$. □

Exemple **2.6.6.** *Etude du comportement vers $+\infty$ de la fonction réelle $f_n(x) = x^n sinx$.*

Démonstration. • Si n est strictement positif, alors toutes les fonctions f_n se comportent de la même manière, elles oscillent entre $-\infty$ et $+\infty$.
• si n est strictement négatif, alors les fonctions f_n tendent vers 0.
• si $n = 0$, alors f_0 oscille entre -1 et 1. □

2.6.4 Raisonnement par élimination des cas

a) Principe

Il est parfois utile, quand le nombre de cas est fini, d'étudier toutes les possibilités et de ne retenir que celles qui conviennent. Ce raisonnement très courant en arithmétique, qui est une variante de la ≪ disjonction des cas ≫, est ≪ l'élimination des cas ≫.

b) Exemples

Exemple 2.6.7. *résoudre dans* $\mathbb{Z}$ *:* $\begin{cases} xy = 1 & (1) \\ 3x + y = 4. & (2) \end{cases}$

Démonstration. Dans $\mathbb{Z}$, $3x + y = 4$ revient à étudier une infinité de cas : on ne peut pas faire un raisonnement par ≪ élimination des cas ≫. Par contre, dans $\mathbb{Z}$, $xy = 1$ revient à étudier 2 cas : le cas : $x = -1,\ y = -1$ et le cas : $x = 1,\ y = 1$.
On peut donc faire ici un raisonnement par ≪ élimination des cas ≫. En remplaçant x par -1 et y par -1 dans (2), on obtient $-4 = 4$, ce qui est impossible. $(-1; -1)$ n'est donc pas solution du système. En remplaçant x par -1 et y par -1 dans (2), on obtient $4 = 4$. $(1; 1)$ est solution du système. Le système a donc une solution $(x; y) = (1; 1)$. □

2.6.5 Raisonnement par contraposée

a) Principe

Le raisonnement par contraposition est basé sur l'équivalence suivante : L'assertion ≪ $P \Rightarrow Q$ ≫ est équivalente à ≪ $non(Q) \Rightarrow non(P)$ ≫. Donc si l'on souhaite montrer l'assertion ≪ $P \Rightarrow Q$ ≫, on montre en fait que si $non(Q)$ est vraie alors $non(P)$ est vraie.

b) Exemples

Exemple 2.6.8. *Soit* $n \in \mathbb{N}$. *Montrer que si* n^2 *est pair alors n est pair.*

Démonstration. Nous supposons que n n'est pas pair. Nous voulons montrer qu'alors n^2 n'est pas pair. Comme n n'est pas pair, il est impair et donc il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$. Alors $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2\alpha + 1$ avec $\alpha = 2k^2 + 2k \in \mathbb{N}$. Et

donc n^2 est impair. Conclusion : nous avons montré que si n est impair alors n^2 est impair. Par contraposition ceci est équivalent à : si n^2 est pair alors n est pair. □

Exemple **2.6.9.** *Soit $a \in \mathbb{R}$. Montrer que si $\forall \epsilon > 0$, $|a| \leq 0$, alors, $a = 0$.*

Démonstration. On va procéder par contraposée en prouvant que : Si $a \neq 0$ alors $\exists \epsilon > 0$, tel que $|a| > \epsilon$.
Soit $a \neq 0$. Posons $\epsilon = \frac{|a|}{2}$. Alors $\epsilon > 0$ et on a bien $|a| > \epsilon$.. □

Exemple **2.6.10.** *Montrer que si x et y sont des réels distincts de 1, et si $x \neq y$, alors $\frac{1}{x-1} \neq \frac{1}{y-1}$.*

Démonstration. La contraposée de l'énoncé est : « si x et y sont des réels distincts de 1, et si $\frac{1}{x-1} = \frac{1}{y-1}$ alors $x = y$ ». Ceci est vrai, car

$$\begin{aligned} \frac{1}{x-1} = \frac{1}{y-1} &\implies x - 1 = y - 1 \\ &\implies x = y. \end{aligned}$$

□

Remarque **2.6.1.** *"Si j'ai faim, alors je mange" est logiquement équivalent à la phrase "Si je ne mange pas, alors je n'ai pas faim". Attention! il ne faut jamais dire que la contraposée de $\ll A \Rightarrow B \geq$ est $\ll non(A) \Rightarrow non(B) \gg$. Avec l'exemple précédent, on obtiendrait la proposition "Si je n'ai pas faim alors je ne mange pas" qui ne dit pas la même chose que la proposition "si j'ai faim alors je mange".*

2.6.6 Raisonnement par l'absurde

a) Principe

Le raisonnement par l'absurde est un autre type de raisonnement très utile pour rédiger proprement certains exercices. Afin de montrer qu'une proposition est vraie, on suppose par l'absurde qu'elle est fausse et on raisonne jusqu'à amener une contradiction. On peut alors dire que la proposition que nous avons supposée est vraie.
Autrement dit pour démontrer qu'une proposition P est vraie, on peut supposer que P est fausse et on cherche une contradiction.

b) Exemples

Exemple **2.6.11.** *Montrons que $\forall x \in \mathbb{N}$; $x + 1 \neq x + 2$.*

Démonstration. Supposons par l'absurde que : $\exists x \in \mathbb{N}$ tel que $x + 1 = x + 2$.
Ce qui aboutit à l'absurdité : $1 = 2$ d'où le résultat. □

Exemple **2.6.12.** *Soient $a, b \geq 0$. Montrer que si $\frac{a}{b+1} = \frac{b}{a+1}$ alors $a = b$.*

Démonstration. Nous raisonnons par l'absurde en supposant que $\frac{a}{b+1} = \frac{b}{a+1}$ et $a \neq b$. Comme $\frac{a}{b+1} = \frac{b}{a+1}$ alors $a(1+a) = b(1+b)$ donc $a+a^2 = b+b^2$ d'où $a^2-b^2 = b-a$. Cela conduit à $(a-b)(a+b) = -(a..b)$. Comme $a \neq b$ alors $a-b \neq 0$ et donc en divisant par $a-b$ on obtient $a+b = -1$. La somme des deux nombres positifs a et b ne peut être négative. Nous obtenons une contradiction.
Conclusion : si $\frac{a}{b+1} = \frac{b}{a+1}$ alors $a = b$. □

Exemple **2.6.13.** *Soit $a \in \mathbb{R}^+$. Montrer l'unicité de $\sqrt{a}$.*

Démonstration. Soient x et y deux nombres positifs distincts tels que $x = \sqrt{a}$ et $y = \sqrt{a}$. Ce qui donne $x^2 = a$ et $y^2 = a$ donc $x^2 - y^2 = 0$. Par suite, $(x+y)(x-y) = 0$. Donc $x + y = 0$ soit $x = -y$ ce qui est impossible car x et y sont positifs et distincts ou $x - y = 0$ soit $x = y$: contraire aux hypothèses. D'où l'unicité. □

Exemple **2.6.14.** *Soient a et b deux nombres strictement positifs. Montrer que $\sqrt{a+b} \neq \sqrt{a} + \sqrt{b}$.*

Démonstration. Supposons que $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$. En elevant au carre : On a $a + b = a + b + 2\sqrt{a} * \sqrt{b}$ soit $\sqrt{a} * \sqrt{b} = 0$ donc $\sqrt{a} = 0$ ou $\sqrt{b} = 0$. En elevant au carre, on obtient $a = 0$ ou $b = 0$ ce qui est contraire a l'énonce, d'où $\sqrt{a+b} \neq \sqrt{a} + \sqrt{b}$. □

Exemple **2.6.15.** *Montrer que pour tout nombre réel x différent de -3, on a $\frac{x+1}{x+3} \neq 1$.*

Démonstration. Soit $x \neq -3$ un réel. Par l'absurde, supposons que $\frac{x+1}{x+3} = 1$. On a : $x + 1 = x + 3$, par suite $1 = 3$. Cette dernière égalité est absurde. D'où, on en déduit que $\frac{x+1}{x+3} \neq 1$. □

Remarque **2.6.2.** *Dans la pratique, on peut choisir indifféremment entre un raisonnement par contraposition ou par l'absurde. Attention cependant de bien préciser quel type de raisonnement vous choisissez et surtout de ne pas changer en cours de rédaction.*

2.6.7 Raisonnement par contre-exemple

a) Principe

Pour infirmer une assertion, on peut utiliser un exemple ou un cas particulier qui la contredit, qu'on appelle alors un contre-exemple.
Pour démontrer qu'une proposition du type $\ll \exists x \in E;\ P(x) \gg$ est vraie, il suffit de

donner un exemple de x qui convient. En passant à la négation, pour démonter qu'une proposition du type $\ll \forall x \in E;\ P(x) \gg$ est fausse, il suffit de donner un exemple d'un x qui ne convient pas. On appelle cela un contre exemple de la proposition P.
Le raisonnement par contre-exemple sert a montrer qu'un enoncé de la forme $\forall x \in E,\ P(x)$ est un enoncé faux. Nous cherchons alors a trouver un element x de E qui ne verifie pas $P(x)$.

b) Exemples

Exemple 2.6.16. *Montrer que l'assertion suivante est fausse « Tout entier positif est somme de trois carrés ». (Les carrés sont les* $0^2, 1^2, 2^2, 3^2, ...$ *Par exemple* $6 = 2^2+1^2+1^2$.*)*

Démonstration. Un contre-exemple est 7 : les carrés inférieurs à 7 sont 0, 1, 4 mais avec trois de ces nombres on ne peut faire 7. □

Exemple 2.6.17. *La somme des chiffres de 42 est un multiple de 6 et 42 est un multiple de 6 (idem pour 84). Peut-on en déduire que si la somme des chiffres d'un nombre entier est un multiple de 6, alors ce nombre est un multiple de 6 ?*

Démonstration. Non. Car, la somme des chiffres de 51 est un multiple de 6 et 51 est un multiple de 6. □

Exemple 2.6.18. *Toute fonction* $f : \mathbb{R} \to \mathbb{R}$ *est-elle soit paire, soit impaire ?*

Démonstration. Non. Car, $f(x) = x^3 + x^2$ n'est ni paire ni impaire. □

Exemple 2.6.19. *Soit* $f(x) = x^3 + x^2$. *Montrer que* f *n'est ni paire ni impaire.*

Démonstration. $f(2) = 12$ et $f(-2) = -4$. □

2.6.8 Raisonnement par récurrence

a) Principe

La démonstration par récurrence s'utilise pour prouver des propositions dont l'énoncé dépend d'un entier naturel n. Elle s'appuie sur une propriété (admise) particulière de l'ensemble des entiers naturels $\mathbb{N}$.
Le raisonnement par récurrence est un type de raisonnement très courant en mathématiques. Imaginez que vous êtes tout en bas d'un escalier infini dont les marches sont numérotées, disons à partir de 1. Imaginons que vous pouvez atteindre la marche numéro 1, et que, pour tout $n \geq 1$, une fois arrivés sur la marche n, vous pouvez monter sur la marche $n+1$. Ainsi, vous montez sur la marche 1, puis à partir de la marche 1 vous pouvez aller sur la marche 2, à partir de la marche 2 sur la marche 3, etc. C'est alors assez intuitif

de penser que vous pouvez atteindre toutes les marches, et c'est exactement ce que dit le principe de récurrence !
Plus précisément, pe principe de récurrence permet de montrer qu'une assertion $P(n)$, dépendant de n, est vraie pour tout $n \in \mathbb{N}$. La démonstration par récurrence se déroule en trois étapes : lors de l'initialisation on prouve $P(0)$. Pour l'étape d'hérédité, on suppose $n \geq 0$ donné avec $P(n)$ vraie, et on démontre alors que l'assertion $P(n+1)$ au rang suivant est vraie. Enfin dans la conclusion, on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

b) Exemples

Exemple 2.6.20. *Montrer que pour tout $n \in \mathbb{N}$, $2^n > n$.*

Démonstration. Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion suivante : $2^n > n$. Nous allons démontrer par récurrence que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.
Initialisation : Pour $n = 0$ nous avons $2^0 = 1 > 0$. Donc $P(0)$ est vraie.
Hérédité : Fixons $n \in \mathbb{N}$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie.

$$\begin{aligned} 2^{n+1} &= 2^n + 2^n > n + 2^n \text{ car par } P(n) \text{ nous savons } 2^n > n \\ &> n + 1 \text{ car } 2^n \geq 1. \end{aligned}$$

Donc $P(n+1)$ est vraie. Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$, c'est-à-dire $2^n > n$ pour tout $\in \mathbb{N}$. □

Exemple 2.6.21. *Démontrons par récurrence que, pour tout entier naturel n, l'entier $n^3 - n$ est divisible par 3.*

Démonstration. Soit $P(n)$ l'assertion $\ll n^3 - n$ est divisible par 3 $\gg$.
i) $0 = 0 \times 3$ donc $0^3 - 0 = 0$ est divisible par 3 et $(P(0))$ est vraie.
ii) Soit n un entier naturel tel que $P(n)$. Alors il existe un entier k tel que $n^3 - n = 3k$ et $(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = n^3 - n + 3(n^2 + n) = 3k + 3(n^2 + n)$.
Par suite $(n+1)^3 - (n+1)$ est divisible par 3. On conclut que si $P(n)$ est vraie, alors $P(n+1)$ est vraie.
Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \succeq 0$, c'est-à-dire pour tout entier naturel n, l'entier $n^3 - n$ est divisible par 3. □

Remarque 2.6.3. — *La rédaction d'une récurrence est assez rigide. Respectez scrupuleusement la rédaction proposée : donnez un nom à l'assertion que vous souhaitez montrer (ici $P(n)$), respectez les trois étapes (même si souvent l'étape d'initialisation est très facile). En particulier méditez et conservez la première ligne de l'hérédité « Fixons $n > 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie. »*

— *Si on doit démontrer qu'une propriété est vraie pour tout $n > n_0$, alors on commence l'initialisation au rang n_0.*
— *Le principe de récurrence est basé sur la construction de l'ensemble $\mathbb{N}$. En effet un des axiomes pour définir $\mathbb{N}$ est le suivant : « Soit A une partie de $\mathbb{N}$ qui contient 0 et telle que si $n \in A$ alors $n+1 \in A$. Alors $A = \mathbb{N}$ ».*

2.6.9 Raisonnement par analyse-synthèse

a) Principe

Le raisonnement par analyse-synthèse sert à démontrer l'existence d'un objet. Cette méthode se divise en deux parties.

— **Analyse :** on suppose dans un premier temps l'existence de l'objet souhaité. À l'aide des propriétés qu'il est censé vérifier, on obtient autant d'informations que possible sur la façon de construire un tel objet.
— **Synthèse :** lorsqu'on a suffisamment d'informations sur l'objet recherché, on le construit explicitement et on vérifie qu'il répond au problème.

Bonus : si la phase d'analyse fournit une expression explicite de l'objet recherché sans alternative possible, on a même démontré l'unicité de cet objet.

b) Exemples

Exemple 2.6.22. *Déterminer les réels tels que $\sqrt{2-x} = x$.*

Démonstration. On va raisonner par analyse-synthèse.
Analyse : Imaginons que x soit une solution de cette équation. Alors il est déjà clair que $x \in]-\infty; 2]$, sinon la racine carrée n'aurait pas de sens. On doit aussi avoir $x \geq 0$, car la racine carrée est positive et donc $x \in [0; 2]$. Élevons ensuite l'équation au carré. Si x est solution, alors $2 - x = x^2$ (on a bien ici simplement une implication, pas une condition nécessaire et suffisante !), c'est-à-dire $x^2 + x - 2 = 0$. La résolution de cette équation du second degré donne $x_1 = -2$ et $x_2 = 1$. Seul x_2 est dans l'intervalle souhaité. Donc la seule solution possible est 1.
Synthèse : Prouvons que 1 est solution de l'équation. On sait que $2 - x = x^2$. Prenons la racine carrée de cette inégalité. Alors :

$$x = \sqrt{x^2} = \sqrt{2-x}.$$

(tout est légitime ici car $x \in [0; 2]$). Conclusion : la seule solution de l'équation est 1. □

Exemple 2.6.23. *Soit $a \in \mathbb{R}$ et $I = [-a, a]$. Montrer que toute fonction $f : I \to \mathbb{R}$ s'écrit comme la somme d'une fonction paire et d'une fonction impaire.*

Démonstration. **Analyse :** Soient g une fonction paire et h une fonction impaire telles que $f = g + h$. On a alors que pour tout $x \in I$, $f(x) = g(x) + h(x)$ et $f(-x) = g(-x) + h(-x) = g(x) - h(x)$. On a donc un système de 2 équations à 2 inconnues. Sa résolution nous donne :

$$g(x) = \frac{f(x) + f(-x)}{2}$$

$$h(x) = \frac{f(x) - f(-x)}{2}$$

Bonus : Nous savons ici que nous avons unicité sous réserve d'existence car g et h sont définis de manière unique par f.

Synthèse : Posons

$$g(x) = \frac{f(x) + f(-x)}{2}$$

$$h(x) = \frac{f(x) - f(-x)}{2}$$

On vérifie aisément que g est paire, que h est impaire et que $f = g + h$, ce qui permet de conclure la preuve. □

Chapitre 3

Relations binaires dans un ensemble

3.1 Définitions et exemples

Définition **3.1.1.** *Une relation binaire $\mathcal{R}$ d'un ensemble de départ E vers un ensemble d'arrivée F est définie par une partie G de $E \times F$. Si $(x, y) \in G$, on dit que x est en relation avec y et l'on note*

$$x\mathcal{R}y.$$

Si $E = F$ on dit que $\mathcal{R}$ est une relation binaire sur E ou relation interne sur E.

Remarque **3.1.1.** *La relation binaire « vide » correspond au sous-ensemble $\emptyset$ de $E \times F$.*

Exemples **3.1.1.**

1. *$E = \{*, \clubsuit, \diamondsuit, \heartsuit\}$, la partie*

   $$\mathcal{R} = \{(*, *), (\heartsuit, \diamondsuit), (\diamondsuit, \diamondsuit), (*, \clubsuit), (\heartsuit, \clubsuit)\} \subset E \times E$$

   est une relation binaire sur E.

2. *Sur $\mathbb{Z}$ on définit la relation $\mathcal{S}$ par :*

   $$(a, b) \in \mathcal{S} \quad si \quad a^2 + b \geq 1.$$

3. *Soient $A = \{a; b; c; d; e\}$ l'ensemble des élèves et $B = \{Math; Info; Ang; Phys\}$ l'ensemble des cours. On peut définir les relations suivantes :*

   a. *$\mathcal{R}$ qui décrit si un étudiant suit un cours régulièrement :*

   $$\mathcal{R} = \{(a; Math); (a; Phys); (b; Info); (c; Ang); (d; Ang); (e; Math); (e; Ang)\}.$$

   b. *$\mathcal{S}$ qui décrit si un étudiant a acheté un cadeau à un autre étudiant dé ?nit par*

   $$\mathcal{S} = \{(b; a); (a; a); (c; a); (a; d); (d; c)\}.$$

4. *Ordre strict ou non sur les entiers :* $(0,1)$ *est noté* $0<1$ *ou* $(0,1)$ *est noté* $0\geq 1$.
5. *Relation de divisibilité :* $(12,132)$ *est noté* $12|132$.
6. *Relation d'inclusion sur les ensembles :* $(\emptyset,\{a\})$ *est noté* $\emptyset\subset\{a\}$ $(\{a\},\{a,b,c\})$ *est noté* $\{a\}\subset\{a,b,c\}$.
7. *La droite* $y=2x+1$.

Exemple **3.1.1.** *On a par rapport aux relations ci-dessus :* $*\mathcal{R}*$, $*\mathcal{R}\clubsuit$ *et* $1\mathcal{S}3$, $3\mathcal{S}(-6)$. $(*,\diamondsuit)\notin\mathcal{R}$, *on dira que* $*$ *n'est pas en relation avec* $\diamondsuit$, *et on ecrira* $*\ \not\mathcal{R}\diamondsuit\ \not\mathcal{S}$.

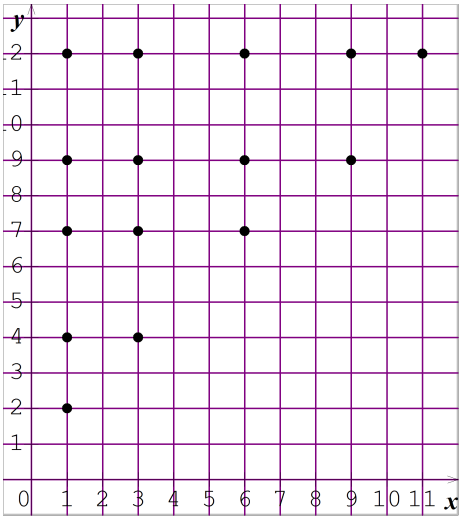
Remarque **3.1.2.** *Une relation binaire* $\mathcal{R}$ *sur un ensemble* E *est definie lorsqu'on sait quand un point x de cet ensemble et en relation avec un autre y de l'ensemble.*

3.2 Mode de représentation

3.2.1 Diagramme cartésien

Définition **3.2.1.** *Grille dans laquelle chaque droite est à égale distance l'une de l'autre autant horizontalement que verticalement. On identifie par un point les couples qui vérifient la relation.*

Exemple **3.2.1.** *Soit* $A=\{1,3,6,9,11\}$, $B=\{2,4,7,9,12\}$ *et la relation "est plus petit que", le graphique cartésien est :*



3.2.2 matrice binaire

Définition **3.2.2.** *Si les ensembles* E *et* F *sont définis par :*

$$E=\{x_1,\cdots,x_n\}\qquad F=\{y_1,\cdots,y_p\}$$

alors la relation $\mathcal{R}$ est définie par la matrice $R = r_{i,j}$ définie par :

$$R = \begin{pmatrix} r_{1,1} & \cdots & r_{1,j} & \cdots & \cdots & r_{1,p} \\ \vdots & & \vdots & & & \vdots \\ r_{i,1} & & r_{i,j} & & & r_{i,p} \\ \vdots & & \vdots & & & \vdots \\ r_{n,1} & \cdots & r_{n,j} & \cdots & \cdots & r_{n,p} \end{pmatrix} \quad avec \quad r_{i,j} = \begin{cases} 1 & si \quad x_i \mathcal{R} y_j \\ 0 & sinon \end{cases}$$

$r_{i,j}$ étant l'élément se trouvant sur la i^{ime} ligne et la j^{ime} colonne, les lignes étant numérotées du haut vers le bas et les colonnes de la gauche vers la droite. La matrice R est appelée la matrice d'adjacence ou d'incidence de la relation $\mathcal{R}$.

Exemple **3.2.2.** *Soit $E = \{e_1, e_2, e_3\}$, $B = \{f_1, f_2, f_3, f_4\}$ et la relation*

$$\mathcal{R} = \{(e_1, f_2); (e_2, f_2); (e_2, f_3); (e_2, f_4); (e_3, f_1); (e_3, f_4)\}.$$

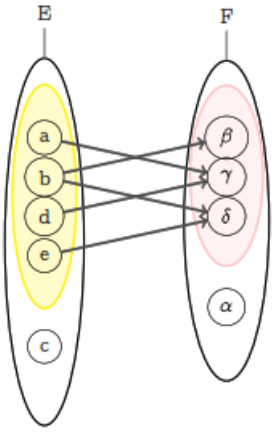
La représentation matricielle de $\mathcal{R}$ est :

$$\begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \end{array} \begin{array}{c} \begin{array}{cccc} f_1 & f_2 & f_3 & f_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

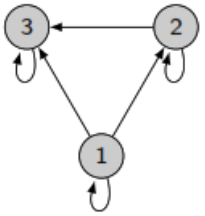
3.2.3 Diagramme sagittal

Définition **3.2.3.** *Un diagramme sagittal représentation graphique d'une relation d'un ensemble fini E vers un ensemble fini F au moyen d'arcs fléchés joignant chaque élément de E et le ou les éléments de F avec lesquels il est en relation.*

Exemple **3.2.3.** *Pour $E = \{a, b, c, d, e\}$, $F = \{\alpha, \beta, \gamma, \delta\}$ et $\mathcal{R} = \{(a; \gamma); (b; \beta); (b; \delta); (d; \gamma); (e; \delta)\}$, on a le diagramme sagittal suivant*



Exemple 3.2.4.
Pour $E = \{1, 2, 3\}$ *et* $\mathcal{R} = \{(1;1); (2;2); (3;3); (1;2); (1;3); (2;3)\}$*, on a le diagramme sagittal suivant*



3.3 Quelques propriétés remarquables des relations binaires

Soit $\mathcal{R}$ une relation binaire definie sur un ensemble non vide E.
Relation Réflexive : On dit que $\mathcal{R}$ est reflexive si on a : $x\mathcal{R}x$ pour tout $x \in E$.
Relation symétrique : $\mathcal{R}$ est dite symétrique si pour tout couple $(x, y) \in E \times E$, la relation $x\mathcal{R}y$ implique la relation $y\mathcal{R}x$:

$$x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

Relation anti-symétrique : $\mathcal{R}$ est dite anti-symétrique si pour tout $(x, y) \in E \times E$, les relations $x\mathcal{R}y$ et $y\mathcal{R}x$ impliquent l'égalité $x = y$:

$$x\mathcal{R}y \quad et \quad y\mathcal{R}x \Rightarrow x = y.$$

Relation transitive : On dit que $\mathcal{R}$ est transitive si pour tout triplet $(x, y, z) \in E \times E \times E$, les relations $x\mathcal{R}y$ et $y\mathcal{R}z$ impliquent la relation $x\mathcal{R}z$:

$$x\mathcal{R}y \quad et \quad y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Exemples 3.3.1. *Sur l'ensemble* $\mathbb{Z}$*, on considère les relations* $\mathcal{R}_1$*,* $\mathcal{R}_2$*,* $\mathcal{R}_3$*,* $\mathcal{R}_4$ *et* $\mathcal{R}_5$ *définies par :*

$$x\mathcal{R}_1 y \; si \; x \geq y; \quad x\mathcal{R}_2 y \; si \; x = y; \quad x\mathcal{R}_3 y \; si \; x = 2y{+}5; \quad x\mathcal{R}_4 y \; si 2x{+}2y \leq 5; \quad x\mathcal{R}_5 y \; si \; x^2 = y^2.$$

Alors,

1. $\mathcal{R}_1$ *est réflexive, antisymétrique et transitive, mais non symétrique.*
2. $\mathcal{R}_2$ *est réflexive, symétrique, transitive et antisymétrique.*
3. $\mathcal{R}_3$ *n'est ni réflexive, ni symétrique, et* $\mathcal{R}_3$ *est antisymétrique.*
4. $\mathcal{R}_4$ *n'est ni réflexive, ni antisymétrique, ni transitive et* $\mathcal{R}_4$ *est symétrique.*
5. $\mathcal{R}_5$ *est réflexive, symétrique et transitive, mais non antisymétrique.*

3.4 Relation d'ordre

3.4.1 Dénitions et exemples

Définition **3.4.1.** *Une relation binaire $\mathcal{R}$ sur un ensemble non vide E est dite relation d'ordre si $\mathcal{R}$ est à la fois* ***reflexive***, ***anti-symétrique*** *et* ***transitive***.

Exemples **3.4.1.**

1) $(\mathbb{R}, \leq)$ *usuel*

2) $\mathbb{R}^2$ *avec la relation* $\prec$ *defini comme suit :*

$$(a, b) \prec (a', b') \quad si \quad a \leq a' \quad et \quad b = b'$$

c'est l'ordre cartesien.

3) Soit $A \neq \emptyset$. *Sur* $\mathcal{P}(A)$ *l'inclusion* $\subset$ *est une relation d'ordre.*

4) Sur $\mathbb{N}^*$ *la relation definie par :* $a\mathcal{R}b$ *si* a *divise* b *est une relation d'ordre.*

Définition **3.4.2** (Ordre total, ordre partiel)**.**

1 *Une relation d'ordre $\mathcal{R}$ sur E est dite totale si pour tout couple x, y de points de E, on a soit $x\mathcal{R}y$, soit $y\mathcal{R}x$.*

2 *Toute autre relation d'ordre est dite partielle.*

Exemple **3.4.1.** *Les exemples 1) et 2) sont des relations d'ordre total.*

3.4.2 Eléments singuliers dans un ensemble ordonné

Soient $(E, \prec)$ un ensemble ordonne et A une partie non vide de E.

Définition **3.4.3** (majorant et minorant)**.**

1 *On appelle majorant de A tout élément $e \in E$ tel que :*

$$\forall a \in A, \qquad a \prec e.$$

2 *On appelle minorant de A tout élément $s \in E$ tel que :*

$$\forall a \in A, \quad s \prec a.$$

3 *On dit que A est majorée (resp. minorée) dans E si A admet un majorant (resp. minorant) dans E.*

.

Remarque **3.4.1.** *Les majorants et minorants n'existent pas toujours, s'ils existent ils ne sont pas uniques.*

Définition **3.4.4** (Elément maximum, Elément minimum)**.**

1. *On dit que M est un plus grand élément ou l'élément maximum de A si*
   - a. $M \in A$,
   - b. $\forall x \in A, \quad x \prec M$.
2. *On dit que M est un plus petit élément ou l'élément minimum de A si*
   - a. $M \in A$,
   - b. $\forall x \in A, \quad M \prec x$.

Remarque **3.4.2.** *Les éléments maximums et minimums n'existent pas toujours, s'ils existent ils sont uniques.*

Exemples **3.4.2.**

1. *Dans $(\mathbb{N}^*, |)$, la partie $A = \{2, 4, 5\}$ est majorée dans $\mathbb{N}^*$ (par exemple, 20 est un majorant de A dans $\mathbb{N}^*$. Aussi, la partie $A = \{2, 6, 10\}$ est minorée dans $\mathbb{N}^*$ (par exemple, 2 est un minorant de A dans $\mathbb{N}^*$.*
2. *Dans $(\mathbb{N}^*, |)$, 2 est le plus petit élément de $A = \{2, 6, 10\}$.*
3. *Dans $(P(E), \subset)$, si $X, Y \in \mathcal{P}(E)$, la partie $A = \{X, Y\}$ est minorée et majorée dans $\mathcal{P}(E)$ ($X \cap Y$ (resp. $X \cup Y$) est un minorant (resp. un majorant) de A dans $\mathcal{P}(E)$).*
4. *La partie $A =]0, 1[$ de $\mathbb{R}$ ordonné par l'ordre usuel est une partie majorée et minorée de $\mathbb{R}$, mais A n'admet ni un plus grand élément ni un plus petit élément.*

Définition **3.4.5** (Borne supérieure, Borne inférieure)**.**

1. *On appelle borne superieure de A le minimum de tous les majorants de A.*
2. *On appelle borne inferieure de A le maximum de tous les minorants de A.*

Définition **3.4.6** (Elément maximal, Elément minimal)**.** *Soit $(E; \preceq)$ un ensemble ordonné, A une partie de E, m et M deux éléments de A.*

1. *On dit que M est un élément maximal de A si $\forall x \in A$; $(M \preceq x \Rightarrow x = M)$. Autrement dit un élément de A est maximal s'il n'y a pas dans A d'éléments qui lui soient strictement supérieurs.*
2. *On dit que m est un élément minimal de A si $\forall x \in A$; $(x \preceq m \Rightarrow x = m)$. Autrement dit un élément de A est minimal s'il n'y a pas dans A d'éléments qui lui soient strictement inférieurs.*

Remarque **3.4.3.** *Il est évident que le plus grand élément M de A, s'il existe, est maximal, c'est d'ailleurs le seul; de même s'il y a dans A un plus petit élément m, il est minimal et c'est le seul.*

Exemples **3.4.3.**

1. *Dans $(\mathbb{N}^*; |)$, on considère $A = \{2; 3; 4; 5; 6; 7; 8; 9\}$, alors, 5 ; 6 ; 7 ; 8 ; 9 sont des éléments maximaux de A et 2 ; 3 ; 5 et 7 sont des éléments minimaux de A.*
2. *Dans $(\mathbb{N}^*; |)$, on considère $A = \mathbb{N}^*\backslash\{1\}$, alors les nombres premiers sont des éléments minimaux de A. ils n'ont pas d'éléments « strictement inférieurs », c'est-à-dire des éléments qui les divisent et en soient différents.*
3. *Dans $\mathcal{P}(E)$ ordonné par $A \subset B$, comme il y a un plus petit élément $\emptyset$ et un plus grand E le seul élément minimal est $\emptyset$ et le seul élément maximal est E, Mais dans $\mathcal{P}(E)\backslash\{\emptyset\}$ il n'y a pas de plus petit élément, les parties $\{x\}$ à un seul élément sont les éléments imnimaux. Dans $\mathcal{P}(E)\backslash\{\emptyset; E\}$ (ensembles des parties propres de E) il y a des éléments minimaux $\{x\}$ et des éléments maximaux $E - \{x\}$.*

3.5 Relation d'équivalence

3.5.1 Dénitions et exemples

Définition **3.5.1.** *Une relation binaire $\mathcal{R}$ est une relation d'équivalence si elle est à fois **reflexive**, **symétrique** et **transitive**.*

Exemples **3.5.1.**

1. *Sur tout ensemble non vide E, la relation $x\mathcal{R}y$ si $x = y$ est une relation d'equivalence. (Cette relation est dite discrette).*
2. *Soit $n \in \mathbb{Z}$. Sur $\mathbb{Z}$ l'entier n permet de définir une relation d'équivalence par :*

$$(p, q) \in \mathbb{Z}^2, \qquad p\mathcal{R}q \quad si \quad q - p \in n\mathbb{Z}$$

   Cette relation est dite de congruence modulo n.
3. *Sur $\mathbb{Z}$, la relation $x\mathcal{R}y$ si $x^2 = y^2$ est une relation d'equivalence.*
4. *La relation $\mathcal{R} = E \times E$ est une relation d'equivalence. Elle est dite grossière.*

3.5.2 Classes d'équivalence

Définition **3.5.2.** . *Soient $\mathcal{R}$ une relation d'équivalence sur E et $a \in E$. On appelle classe d'équivalence de a le sous-ensemble de E constitué des points x qui sont en relation avec a. On note $\dot{a}$ ou $\overline{a}$ ou $Cl(a)$ ce sous-ensemble.*

Exemple **3.5.1.** *Soit $x, y \in \mathbb{R}$ et $\mathcal{R}$ la relation définie sur $\mathbb{R}$ par $x\mathcal{R}y$ si $x^2 = y^2$. $\mathcal{R}$ est une relation d'équivalence et on a : $\overline{x} = \{x, -x\}$*

Lemme **3.5.1.** *Soit $\mathcal{R}$ une relation d'équivalence sur E. On a :*

1. $\forall x \in E$, $x \in \overline{x}$.
2. *Soit $(a, b) \in E^2$. Si $a \in \overline{b}$, alors $b \in \overline{a}$ et $\overline{a} = \overline{b}$.*
3. *Soit $(a, b) \in E^2$. On a soit $\overline{a} = \overline{b}$ soit $\overline{a} \cap \overline{b} = \emptyset$.*
4. *Les différentes classes d'équivalence forment une partition de l'ensemble E.*

3.5.3 Ensemble quotient

Définition **3.5.3.** *. L'ensemble quotient est l'ensemble des classes d'équivalences. On le note $E/\mathcal{R}$ ou $\frac{E}{\mathcal{R}}$.*

Exemple **3.5.2.** *Sur $\mathbb{Z}$ la relation d'équivalence par : $(p, q) \in \mathbb{Z}^2$, $p\mathcal{R}q$ si $q - p \in 5\mathbb{Z}$ a pour classes d'équivalence $\overline{0}$,$\overline{1}$,$\overline{2}$,$\overline{3}$, $\overline{4}$. et pour ensemble quotient*

$$\frac{\mathbb{Z}}{\mathcal{R}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

On a

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}.$$

Remarque **3.5.1.** *Soit $\mathcal{R}$ une relation d'équivalence sur E. L'application $s : E \to E/\mathcal{R}$, $x \mapsto \overline{x}$ est une surjection appelée la **surjection canonique**.*

Chapitre 4

Applications d'un ensemble vers un autre

4.1 Relations d'un ensemble vers un autre

4.1.1 Définitions

Définition 4.1.1. *On appelle relation (ou correspondance) de E vers F tout triplet $f = (E; F; \Gamma)$, où Γ est une partie de $E \times F$.*
Si $(x; y)$ est un élément de Γ, y est appelée une image de x par f et x est dit un antécédent de y par f. On dit aussi que x est en relation avec y. Γ est appelé le graphe de f.

4.1.2 Notation

1. Si $f = (E; F; \Gamma)$ est une correspondance, on écrit xfy si $(x; y) \in \Gamma$.
2. Aussi, une correspondance $f = (E; F; \Gamma)$ est notée :

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

où $f(x)$ est un élément de F tel que $(x; f(x)) \in \Gamma$ La correspondance f est notée aussi $E \overset{f}{\to} F$.

4.1.3 Exemples

Soit $f : \mathbb{R} \to \mathbb{R}\,; x \mapsto y$, avec y est un réel tel que $y^2 = x$. On remarque que 0 possède une unique image et que si $x \in \mathbb{R}_+^*$, x possède deux images distinctes. Cependant, si $x \in \mathbb{R}_-^*$, x n'a pas d'image.

4.2 Applications

4.2.1 Définitions

Définition 4.2.1. *On appelle application de A vers B, toute relation f de A vers B telle que :*
à tout élément $x \in A$ correspond un élément et un seul, bien déterminé y de B. On écrit $f : A \to B$ ou, $A \xrightarrow{f} B$.

1. *A est appelé l'ensemble de départ de f.*
2. *B l'ensemble d'arrivé de f.*
3. *y est l'image de x par f et est noté $f(x)$, et x est un antécédent de y.*

Définition 4.2.2. *Soit $f : A \to B$ une application.*

1. *Si $B \subset \mathbb{R}$, on parle d'application reelle,*
2. *Si $A \subset \mathbb{R}$, on parle d'application variables reelles.*

Remarque 4.2.1.

1. *Si $A' \subset A$, alors f induit une application naturelle $f' : A' \to B$ deflnie par :*
$$\forall a' \in A', \qquad f'(a') = f(a').$$
On dit que f' est restriction de f à A'.
2. *Si $B' \subset B$, f ne deflnit pas necessaire une application de A dans B'.*

4.2.2 Exemples et contre-exemples

1. Les applications constantes
2. L'application identite de A notee id_A.
3. L'application $f : \mathbb{Z} \to \mathbb{N}$, $n \mapsto 2n^2 - n$ est bien deflnie.
4. La relation $g : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto \sin x$ n'est pas une application.
5. La relation $\{(1, \clubsuit), (2, \clubsuit), (4, \diamondsuit), (5, \heartsuit)\}$ n'est pas une application de et $A = \{1, 2, 3, 4, 5, 7\}$ dans $B = \{\clubsuit,\ \diamondsuit,\ \heartsuit,\ \spadesuit\}$.
6. La relation $h : \mathbb{Q} \to \mathbb{Z}$, $\dfrac{p}{q} \to p + q$ n'est pas une application.

4.2.3 Egalité de deux applications

Définition 4.2.3. *Soient $f : A \to B$ et $f' : A' \to B'$ deux applications. On dira que $f = f'$ lorsque : $A = A'$, $B = B'$ et pour tout $x \in A$, on a $f(x) = f'(x)$.*

Exemple 4.2.1. *les applications $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ et $g : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto x^2$ ne sont pas egales.*

Définition **4.2.4** (Suite d'éléments d'un ensemble E)**.** *On appelle suite d'éléments d'un ensemble E toute application de $\mathbb{N}$ ou d'une partie D de $\mathbb{N}$ dans E. On ecrit une suite d'éléments d'un ensemble E sous la forme $(u_n)_{n\in D}$.*

4.2.4 Fonctions caractéristiques

Définition **4.2.5.** *Soient E un ensemble non vide et A une partie de E. On appelle fonction caracteristique (ou indicatrice) de A l'application notee χ_A deflnie comme suit :*

$$\chi_A : E \to \mathbb{R}, \quad x \mapsto 1 \ si \ x \in A \quad et \quad x \mapsto 0 \ si \ x \notin A.$$

Exercice 2. *Deflnir χ_E et $\chi_\emptyset$.*

Propriété 4.2.1 (propriétés remarquables des fonctions caracteristiques)**.**

1. $\chi_A = \chi_B \Leftrightarrow A = B.$
2. $\chi_{A\cap B} = \chi_A\chi_B.$
3. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A\chi_B.$
4. $\chi_A = 1 - \chi_A.$

4.2.5 Image directe, Image réciproque

Définition **4.2.6.** *Soient $f : E \to F$ une application, A une partie de E et B une partie de F.*

1. *L'ensemble de toutes les images des points de A est appele **image directe** de A par f, on le note $f(A)$. On a*

$$f(A) = \{f(a), \quad a \in A\}.$$

   L'image directe de l'ensemble de depart E est appelee image de f, on la note $\mathrm{Im}\, f$.

2. *L'ensemble de tous les points de E dont l'image appartient à B est appele image **reciproque** de B par f, on le note $f^{-1}(B)$. On a*

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

Remarque **4.2.2.**

1. *Notons que $f(A) \subset F$.*
2. *Notons que $f^{-1}(B) \subset E$. Il est clair que $f^{-1}(F) = E$.*

3. *On a $f(A) = \emptyset$ ssi $A = \emptyset$, alors que $f^{-1}(B) = \emptyset$ n'implique pas necessairement que $B = \emptyset$.*

Exemple **4.2.2.** *Soit $f = \sin : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin(x)$; alors $\operatorname{Im} f = [-1, 1]$ et $f([0, \frac{\pi}{2}]) = [0, 1]$.*

Propriété 4.2.2. *Soit A ; B deux parties de E et $f : E \to F$ une application.*

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 $(E_i)_{i\in I}$ est une famille de parties de E, alors $f(\bigcup_{i\in I} E_i) = \bigcup_{i\in I} f(E_i)$.*
4. $f(A \cap B) \subset f(A) \cap f(B)$. *Plus généralement, si $(E_i)_{i\in I}$ est une famille de parties de E, alors $f(\bigcap_{i\in I} E_i) \subset \bigcap_{i\in I} f(E_i)$.*
5. $f^{-1}(\emptyset) = \emptyset$.
6. $f^{-1}(F) = E$.
7. *Si $A \subset B$, alors $f^{-1}(A) \subset f^{-1}(B)$.*
8. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$. *Plus généralement, si $(E_i)_{i\in I}$ est une famille de parties de E, alors $f^{-1}(\bigcup_{i\in I} E_i) = \bigcup_{i\in I} f^{-1}(E_i)$.*
9. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. *Plus généralement, si $(E_i)_{i\in I}$ est une famille de parties de E, alors $f^{-1}(\bigcap_{i\in I} E_i) = \bigcap_{i\in I} f^{-1}(E_i)$.*

4.2.6 Composition des applications

Définition **4.2.7.** *Soient $f : E \to F$ et $g : N \to M$ deux applications. Si $F \subset N$, alors on peut definir une nouvelle application $h : E \to M$ par : $x \mapsto g(f(x))$. h est appele la composee de g par f et est noté $g \circ f$.*
Notons que par definition on a pour tout $x \in E$, $(g \circ f)(x) = g(f(x))$.

Propriété 4.2.3. *Soient $f : E \to F$ et $g : N \to M$ deux applications telles que $F \subset N$.*

1. *Si $s : V \to W$ est une 3e application telle que $M \subset V$, alors*

$$s \circ (g \circ f) = (s \circ g) \circ f.$$

2. *On a $id_F \circ f = f$ et $g \circ id_N = g$.*

Exemples **4.2.1.** *: $s : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ et $v : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 2$, on a $s \circ v : \mathbb{R} \to \mathbb{R}$, $x \mapsto (x + 2)^2$ et $v \circ s : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 2$.*

Remarque **4.2.3.** *La composition des applications n'est pas commutative, c'est-à-dire qu'on a pas toujours $g \circ f = f \circ g$. En effet, soit E est un ensemble contenant deux éléments a et b distincts, $f, g : E \to E$ telles que $f(a) = b$, $f(b) = a$ et $g(a) = b$, $g(b) = b$, alors $(g \circ f)(a) = b$ tandis que $(f \circ g)(a) = a$.*

Théorème **4.2.1.** *Soient E, F deux ensembles non vides et $f : E \to F$, $g : F \to E$ deux applications telles que*

$g \circ f = id_E$ et $f \circ g = id_F$

Alors f et g sont bijectives, et $f^{-1} = g$

Démonstration. A faire en exercice. □

4.2.7 Applications injectives, surjectives, bijectives

a) Définitions et remarques

Définition **4.2.8.** *Soit une application $f : E \to F$. f est dite **injective** si deux éléments distincts quelconques de E ont des images distinctes dans F. Autrement dit, si une égalité d'images $f(x) = f(x')$ où x, $x' \in E$ entraine que $x = x'$, ou encore si tout $y \in F$ a au plus un seul antécédent.*

$$\forall (x, x') \in E^2, \qquad on\ a \quad f(x) = f(x') \Rightarrow x = x'.$$

En particulier f n'est pas injective signifle qu'il existe dans F un élément qui a moins deux antécédents.

Remarque **4.2.4.** *Si les ensembles E et F sont flnis et $f : E \to F$ est injective, alors nécessairement $card(E) \leq card(F)$.*
En particulier toute application $g : \mathbb{N} \to B$ ou B est un ensemble flni non vide est non injective.

Définition **4.2.9.** *f est dite **surjective**, si tout élément de F a au moins un antécédent dans E*

$$\forall y \in F, \quad \forall x \in E : \quad y = f(x).$$

Remarque **4.2.5.** *Si les ensembles E et F sont flnis et $f : E \to F$ est surjective, alors nécessairement $card(E) \geq card(F)$.*

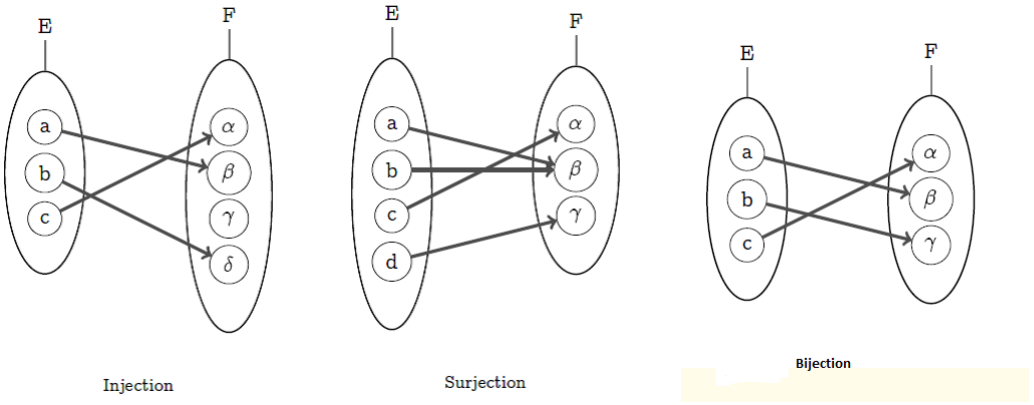
Définition **4.2.10.** *f est dite **bijective**, si f est à la fois injective et surjective , ou encore si tout élément de F a un antécédent et un seul dans E.*

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

Exemple **4.2.3.**

1. *L'application $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto |x|$ n'est ni injective ni surjective tandis que $g : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto |x|$ est surjective.*
2. *id_E est une bijection.*
3. *Soit A une partie de E. L'application $i : A \to E$, $x \mapsto x$ est une application injective appelée **injection canonique** de A dans E. Si $A \neq E$, i n'est pas surjective.*

Exemple **4.2.4.**



Exercice 3. *Soit*

$$\begin{array}{rcl} f : A & \to & B \\ x & \mapsto & x^2. \end{array}$$

Dans chacun des cas suivants, préciser si f est injective, surjective ou bijective :

1. $A = \mathbb{R}, \quad B = \mathbb{R}$;
2. $A = \mathbb{R}_+, \quad B = \mathbb{R}$;
3. $A = \mathbb{R}, \quad B = \mathbb{R}_+$;
4. $A = \mathbb{R}_+, \quad B = \mathbb{R}_+$.

b) Bijection réciproque d'une application bijective

Définition **4.2.11.** *Soit $f : E \to F$ une application bijective. Alors on peut deflnir une application $s : F \to E$ de la façon suivante : à tout $y \in F$, on associe son unique antécédent x dans E.*

$$y \mapsto x \quad si \quad y = f(x)$$

s est appele bijection reciproque de f et on la note f^{-1}.

Proposition **4.2.1.** *Si $f : E \to F$ est une bijection, alors $f^{-1} \circ f = id_E$ et $f \circ f^{-1} = id_F$.*

Proposition **4.2.2.** *Soit $f : E \to F$ et $g : F \to E$ deux applications. Si $f \circ g = id_F$ et $g \circ f = id_E$, alors f et g sont bijectives, $g = f^{-1}$ et $f = g^{-1}$.*

Corollaire 4.2.1. **1** *Si $f : E \to F$ est bijective, alors f^{-1} est bijective et*

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

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

Exemples 4.2.2.

1 *Soit $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. L'application $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$ est bijective et l'application réciproque de f est $f^{-1} : \mathbb{R} \to \mathbb{R}$, $x \mapsto \dfrac{x-b}{a}$.*

2 *L'application réciproque de* $\ln : R_+^* \to \mathbb{R}$, $x \mapsto \ln(x)$ *est l'application* $\exp : \mathbb{R} \to \mathbb{R}_+^*$, $x \mapsto \exp(x)$.

Exemples 4.2.3.

1 id_A *est bijective et* $(id_A)^{-1} = id_A$.

2 $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 2$ *est bijective et* $f^{-1} : \mathbb{R} \to \mathbb{R}$, $x \mapsto x - 2$.

3 $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto -x$ *est bijective et egale a sa propre bijection reciproque.*

4 $\ln : \mathbb{R}* \to \mathbb{R}$ *est une bijection et* $\ln_{-1} = \exp$.

5 $\cos : [0, \pi] \to [-1, 1]$ *est une bijection et* $\cos^{-1} = \arccos$.

6 $\sin : [-\pi, \pi] \to [-1, 1]$ *est une bijection et* $\sin^{-1} = \arcsin$.

4.2.8 Ensembles dénombrables

Définition 4.2.12. *Deux ensembles non vides E et F sont dits equipotents s'il existe une application $f : E \to F$ bijective.*
Un ensemble non vide E est dit denombrable, si E est equipotent à $\mathbb{N}$ ou à une partie de $\mathbb{N}$.

Exemples 4.2.4. **1** *Tout ensemble flni est denombrable.*

2 $\mathbb{N}$ *et* $\mathbb{Z}$ *sont denombrables.*

Propriété 4.2.4. **1** *Toute partie non vide d'un ensemble de- nombrable est encore denombrable.*

2 *La reunion flnie d'ensembles denombrables est denombrable.*

3 *Le produit cartesien de deux ensembles denombrables est denom- brable. En particulier $\mathbb{Q}$ est denombrable.*

4.2.9 Décomposition canonique d'une application

Théorème 4.2.2 (Décomposition canonique d'une application)**.** *Si $f : E \to F$ est une application, alors :*

1. *La relation $\mathcal{R}$ définie sur E par $x\mathcal{R}y$ si $f(x) = f(y)$, où $x, y \in E$, est une relation d'équivalence.*
2. *il existe une, et une seule, application $\overline{f} : E/\mathcal{R} \to \operatorname{Im} f$ telle que f est bijective et $f = i \circ \overline{f} \circ s$, avec $i : \operatorname{Im} f \to F (resp. s : E \to E/\mathcal{R})$ est l'injection canonique (resp. la surjection canonique).*

La décomposition $f = i \circ \overline{f} \circ s$ est appelée la ***décomposition canonique*** *de f.*

Exemple 4.2.5. *Soit $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. La décomposition canonique de f est $f = i \circ \overline{f} \circ s$, avec s est la surjection canonique $s : \mathbb{R} \to \mathbb{R}/\mathcal{R} = \{\{x, -x\}/x \in \mathbb{R}\}$, $x \mapsto \overline{x} = \{x, -x\}$, f est la bijection $f : \mathbb{R}/\mathcal{R} \to \mathbb{R}^+$, $\{x, -x\} \mapsto x^2$ et i est l'injection canonique $i : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto x$.*

Remarque 4.2.6. *Notons que s est une application surjective, et i est injective. $\overline{f}$ est bijective*

Chapitre 5

LOIS DE COMPOSITION INTERNES ET EXTERNES

5.1 Lois de composition internes (LCI)

5.1.1 Définitions et exemples

Définition **5.1.1.** *Soit E ensembles non vide. On appelle loi de composition interne sur E toute application f de $E \times E$ dans E. Le couple constitué par un ensemble et une loi interne sur un ensemble est appelé un magma.*

Notation **5.1.1.** *On note de plusieurs manières les lois de composition. Voici quelques notations utilisées fréquemment*

$$(x,y) \mapsto x+y \qquad (x,y) \mapsto x.y \qquad (x,y) \mapsto x*y$$
$$(x,y) \mapsto x \top y \qquad (x,y) \mapsto x \perp y \qquad (x,y) \mapsto x \times y$$

Remarque **5.1.1.** *Si la loi est notée $\top$, l'image de l'élément $(x,y) \in E \times E$ est désignée par $x \top y$ et non par $\top(x,y)$.*

Exemples **5.1.1.**

1. *Dans $\mathbb{R}$ ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$), l'addition $(x,y) \mapsto x+y$ et la multiplication $(x,y) \mapsto x \times y$ sont des lois de composition internes.*
2. *Dans $\mathbb{R}$ (ou $\mathbb{Z}$, $\mathbb{Q}$), la soustration $(x,y) \mapsto x-y$ est une loi de composition interne.*
3. *Soit E un ensemble. Les applications $(X,Y) \mapsto X \cup Y$ et $(X,Y) \mapsto X \cap Y$ sont des lois de composition internes sur l'ensemble des parties de E.*
4. *Dans l'ensemble $\mathcal{A}(E,E)$ des applications de E vers E, la composition $(f,g) \mapsto g \circ f$ est une loi de composition interne.*

5.1.2 Partie stable par une Loi de composition interne, loi induite

Définition 5.1.2. *Soit E un ensemble non vide, muni d'une loi de composition interne $\top$. Soit A une partie non vide de E. On dit que A est stable pour la loi $\top$ si, et seulement si :*

$$\forall (x,y) \in A^2, \quad x \top y \in A.$$

Exemples 5.1.2.

1. *$\mathbb{R}^+$, $\mathbb{N}$, $\mathbb{Z}^+$ et $\mathbb{Q}^+$, sont stables pour l'addition, et pour la multiplication.*
2. *$\mathbb{R}^-$, $\mathbb{Z}^-$ et $\mathbb{Q}^-$, ne sont pas stables pour la multiplication.*

Définition 5.1.3. *Soit E un ensemble non vide, muni d'une loi de composition interne $\top$. Soit A une partie de E stable pour la loi $\top$.*
L'application $T_A : A \times A \to A$ définie par $(x,y) \mapsto x \top y$ est alors une loi interne sur A; elle est appelée loi induite sur A par la loi $\top$ définie sur E. S'il n'y a pas d'ambiguïté, on la note encore $\top$.

Exemple 5.1.1. *L'application $\mathbb{R}^- \times \mathbb{R}^- \to \mathbb{R}^-$ définie par $(x,y) \mapsto x+y$ est la loi induite sur $\mathbb{R}^-$ par la loi $+$ définie sur $\mathbb{R}$.*

5.1.3 Loi associative

Définition 5.1.4. *Soit E un ensemble muni d'une loi de composition interne $\top$. La loi $\top$ est dite associative si et seulement si :*

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

On dit alors que $(E, \top)$ est un magma associatif appelé semi-groupe.

Exemples 5.1.3.

1. *L'addition et la multiplication des entiers naturels sont des lois de composition associatives sur $\mathbb{N}$.*
2. *L'addition et la multiplication des nombres réels sont des lois de composition associatives sur $\mathbb{R}$;*
3. *Soit E un ensemble. Les lois $\cap$ et $\cup$ sont associatives et commutatives dans $\mathcal{P}(E)$.*

Remarque 5.1.2. *Dans le cas d'une loi associative $\top$, on peut supprimer les parenthèses, et plus généralement associer au $n-$uplet $(x_1, ..., x_n) \in E^n$ l'élément $x_1 \top ... \top x_n$ de E, étant entendu qu'intervient l'ordre dans lequel sont donnés $x_1, ..., x_n$.*

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, l'élément $x_1 \top ... \top x_n$ s'écrit $\overset{n}{\top} x$, et on vérifie par récurrence

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N} \backslash \{0\})^2, \quad (\overset{n}{\top} x) \top (\overset{p}{\top} x) = \overset{n+p}{\top} x.$$

En notation additive, on écrit

$$x_1 + ... + x_n = \sum_{i=1}^{n} x_n.$$

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, $x_1 + ... + x_n$ *s'écrit* nx.

En notation multiplicative, on écrit

$$x_1 \times ... \times x_n = \prod_{i=1}^{n} x_n.$$

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, *l'élément* $x_1 \times ... \times x_n$ *s'écrit* x^n. *On dit que* x^n *est la puissance* n^{ime} *de* x.

On vérifie facilement que pour tout entier p tel que $1 \leq p \leq n$, *on a la relation*

$$x_1 \top ... \top x_n = (x_1 \top ... \top x_p) \top (x_{p+1} \top ... \top x_n).$$

on déduit que :
En notation additive, on a

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N}\backslash\{0\})^2, \quad nx + px = (n+p)x \quad et \quad n(px) = (np)x.$$

En notation multiplicative, on a

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N}\backslash\{0\})^2, \quad x^n \times x^p = x^{n+p} \quad et \quad (x^n)^p = x^{np}.$$

5.1.4 Lois commutatives

Définition 5.1.5. *Soit* $*$ *une loi de composition interne sur* E. *On dit que deux éléments* a *et* b *de* E *sont permutables (ou commutent) pour la loi* $*$ *si*

$$a * b = b * a$$

Définition 5.1.6. *On dit que la loi* $*$ *est commutative si, pour tout* $(x,y) \in E^2$, *on a* $x * y = y * x$ *(en d'autres termes, les éléments de* E *sont permutables 2 à 2).*

Exemples 5.1.4. — $+$, $\times$ *sont des lois commutatives dans* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
— *Les lois* $\cup$ *et* $\cap$ *sont commutatives dans* $\mathcal{P}(E)$.

Il y a cependant des lois qui ne sont pas commutative. par exemple

Exemple 5.1.2. *La composition des applications " ∘ " n'est pas commutative.*

Remarque 5.1.3. *Tout élément* $x \in E$ *permute avec lui même. Si " * " est associative, tout* x *permute avec* x^n, $(n \in \mathbb{N}^*)$.

Définition 5.1.7. *On dit qu'un élément* x *de* E *est central si tout élément de* E *est permutable avec* x. *On appelle centre de* E *l'ensemble des éléments centraux.*

5.1.5 Elément neutre à gauche, élément neutre à droite, élément neutre

Définition 5.1.8. *Soit E un ensemble muni d'une loi de composition interne $*$.*
On dit que l'élément e de E est un élément :

- *neutre à gauche, si : $\forall x \in E,\ e * x = x$;*
- *neutre à droite, si : $\forall x \in E,\ x * e = x$;*
- *neutre si e est neutre à gauche et à droite : $\forall x \in E,\ e * x = x * e = x$.*

Remarque 5.1.4. **1** *Lorsque la loi est notée additivement, l'élément neutre est noté 0 ;*

2 *Lorsque la loi est notée multiplicativement, l'élément neutre est noté 1.*

Exemple 5.1.3. *a) $(\mathbb{R}, +)$ admet 0 comme élément neutre,*

b) $(\mathbb{R}, \times)$ admet 1 comme élément neutre,

c) $(\mathcal{P}(E), \cap)$ admet E comme élément neutre,

d) $(\mathcal{P}(E), \cup)$ admet $\emptyset$ comme élément neutre,

e) $(\mathcal{A}(E, E), \circ)$ admet Id_E comme élément neutre.

Il y a cependant des lois qui n'ont pas d'élément neutre par exemples

Exemple 5.1.4. **1** *La loi $*$ définie sur $\mathbb{R}$ par $x * y = x.y + 3$ n'a pas d'élément neutre.*

2 *La loi $\top$ définie sur $\mathbb{R}$ par : $x \top y = x^2.y$ n'a pas d'élément neutre.*

3 *La multiplication $\times$ définie sur $[2, +\infty[$ n'a pas d'élément neutre.*

Exemple 5.1.5. *On considère la loi $\perp$ définie sur $\mathbb{R}$ par*

$$\forall x, y \in \mathbb{R}, \qquad x \perp y = \frac{1}{2}x^2 \times y.$$

$\perp$ admet $-\sqrt{2}$ et $\sqrt{2}$ comme éléments neutres à gauche.
$\perp$ n'admet pas d'élément neutre à droite.
$\perp$ n'admet pas d'élément neutre.

Proposition 5.1.1. **1** *Si e' est un élément neutre à gauche de $(E, \top)$ et e'' est un élément neutre à droite de $(E, \top)$, alors $e' = e''$.*

2 *Si e_1 et e_2 sont des éléments neutres de $(E, \top)$, alors $e_1 = e_2$.*

Démonstration. **1** Comme e' est un élément neutre à gauche, on a

$$e' \top e'' = e'' \tag{5.1}$$

Comme e'' est un élément neutre à droite, on a

$$e' \top e'' = e' \tag{5.2}$$

(5.1) et (5.2) nous donne $e' = e''$

2 Ce qui précède permet de conclure

□

Remarque **5.1.5.** *Un magma associatif ou semi-groupe admettant un élément neutre s'appelle* ***monoïde****.*

5.1.6 Elément symétrique à gauche, à droite, élément symétrique

Définition **5.1.9.** *Soit E un ensemble muni d'une loi de composition interne $*$. On suppose que $(E,*)$ possède un élément neutre e.*
On dit que l'élément x de E possède :

- *un symétrique à gauche x_g, si $x_g * x = e$. On dit alors que x est symétrisable à gauche·*
- *un symétrique à droite x_d; si $x * x_d = e$. On dit alors que x est symétrisable à droite.*
- *un symétrique x' si $x' * x = x * x' = e$. On dit alors que x est symétrisable .*

Proposition **5.1.2.** *Soit E un ensemble muni d'une loi de composition interne $*$. On suppose que $(E,*)$ possède un élément neutre e et que la loi $*$ est associative.*

1 *Si un élément x de E possède un symétrique à gauche et un symétrique à droite alors ils sont égaux.*

2 *Si un élément x de E est symétrisable alors il admet un unique symétrique.*

Exemples **5.1.5.**

— *Dans $\mathbb{R}$ muni de $+$, tout élément $x \in \mathbb{R}$ admet $-x$ pour symétrique.*
— *Dans $\mathbb{R}$ muni de $\times$, tout les éléments $x \in \mathbb{R}^*$ admet $\frac{1}{x}$ pour symétrique.*
— *Dans $\mathcal{P}(E)$ muni de la loi Δ*

$$X \Delta Y = (X \cap \overline{Y}) \cup (\overline{X} \cap Y).$$

L'ensemble vide $\emptyset$ est élément neutre et tout élément $X \in \mathcal{P}(A)$ s'admet lui-même pour symétrique.

Notation **5.1.2.** *Si $x \in E$ admet un symétrique, et que ce symétrique est unique, on le note x^{-1} (en notation multiplicative) et $-x$ (en notation additive).*

Proposition **5.1.3.** *Soit E un ensemble muni d'une loi de composition interne $*$. Si x et y sont deux éléments de E de symétrique respectif x^{-1} et y^{-1}, alors $x * y$ admet $y^{-1} * x^{-1}$ pour symétrique*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Démonstration. Calculer $(x * y) * (y^{-1} * x^{-1})$ puis $(y^{-1} * x^{-1}) * (x * y)$. □

Corollaire **5.1.1.** *Si x admet un symétrique, alors pour tout $n \in \mathbb{N}^*$, x^n admet $(x^{-1})^n$ pour symétrique :*

$$(x^n)^{-1} = (x^{-1})^n.$$

5.1.7 Homomorphismes

Définition **5.1.10.** *Soient E, F, deux ensembles munis respectivement des lois de compositions internes $*$ et $\bullet$. On dit qu'une application $f : E \mapsto F$ est un homomorphisme si*

$$\forall (x, x') \in E^2, \quad \text{on a} \quad f(x * x') = f(x) \bullet f(x').$$

Exemples **5.1.6.**

1 *$id_E : E \to E$ est un homomorphisme*

2 *Si la loi $*$ admet $e \in F$ comme élément neutre, alors l'application constante $h : E \to F$, $x \mapsto e$ est un homomorphisme.*

3 *$\ln : \mathbb{R}^* \to \mathbb{R}$ est un homomorphisme si on considère la multiplication dans R* et l'addition dans $\mathbb{R}$.*

4 *$f : \mathbb{R}^2 \to \mathbb{R}$, $(a, b) \mapsto 2a + b$ est un homomorphisme avec l'addition dans $\mathbb{R}^2$ et l'addition dans $\mathbb{R}$. $\mathbb{R}^2$ muni de la loi cartésienne $(a, b) + (a', b') = (a + a', b + b')$.*

Définition **5.1.11.**

— *Un homomorphisme bijectif est appelé isomorphisme.*

— *Un homomorphisme de $(E, *)$ dans $(E, *)$ est appelé endomorphisme.*

— *Un endomorphisme bijectif est appelé un automorphisme.*

Proposition **5.1.4.** *Soient $f : E \to F$ et $g : F \to G$ deux homomorphismes, alors $g \circ f$ est un homomorphisme.*

Démonstration. On considère $(E, *)$, $(F, \bullet)$, $(G, \top)$. $g \circ f : (E, *) \to (G, \top)$. $\forall z \in E$, on a $(g \circ f)(z) = g(f(z))$.
$\forall x, y \in E$, on a

$$\begin{aligned} (g \circ f)(x * y) &= g(f(x) \bullet f(y)) \\ &= g(f(x)) \top g(f(y)) \\ &= (g \circ f)(x) \top (g \circ f)(y). \end{aligned}$$

□

Proposition **5.1.5.** *Si $f : E \to F$ est un isomorphisme, alors la bijection réciproque f^{-1} est un isomorphisme.*

5.1.8 Distributivité

Définition **5.1.12.** *Soit E un ensemble muni de deux lois de composition internes $*$ et $\perp$. On dit que la loi $\perp$ est distributive par rapport à la loi $*$ si :*

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

Exemple **5.1.6.** *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

5.2 Lois de composition externes (LCE)

5.2.1 Définitions et exemples

Définition **5.2.1.** *Soient E et Ω des ensembles. On appelle loi de composition externe sur E, à ensemble d'opérateurs Ω, toute application de $\Omega \times E$ dans E.*

Exemple **5.2.1.** *Une application $g : \mathbb{N}^* \times E \to E\,;\ (n,e) \mapsto ne$ est le model de lois externes le plus connu.*

Exemple **5.2.2.** *Soit E un ensemble muni d'une loi de composition interne $\top$. En posant $n\perp x = \overset{n}{\top}\, x$, on définit une loi de composition externe sur E, dont l'ensemble d'opérateurs est, selon les propriétés de $\top$, $\mathbb{N}\backslash\{0\}$, $\mathbb{N}$ ou $\mathbb{Z}$.*

5.2.2 Partie stable par une loi de composition externe, loi induite

Définition **5.2.2.** *Soit E un ensemble muni d'une loi de composition externe $\perp$ à opérateurs dans X. Soit F une partie de E. On dit que F est stable par $\perp$ si :*

$$\forall a \in X, \qquad \forall x \in F, \qquad a\perp x \in F.$$

Si F est une partie stable par $\perp$, alors la restriction de $\perp$ à F est une loi de composition externe sur F dite loi induite par $\perp$ dans F.

5.2.3 Distributivité

Définition **5.2.3.** *Soit E un ensemble muni :*

i) D'une loi de composition interne $*$;

ii) D'une loi de composition externe $\perp$ à opérateurs dans X.

On dit que la loi $\perp$ est distributive par rapport à la loi $*$ si :

$$\forall a \in X, \quad \forall (x,y) \in E^2, \quad a\perp(x*y) = (a\perp x)*(a\perp y).$$

Exemple **5.2.3.** *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

Chapitre 6

STRUCTURES ALGEBRIQUES

6.1 Groupes

6.1.1 Définitions et exemples

Définition 6.1.1. *On appelle groupe tout couple $(G, \top)$ composé d'un ensemble G non vide et d'une loi de composition $\top$ interne sur cet ensemble satisfaisant aux axiomes suivants :*

(G_1) *La loi $\top$ est associative ;*

(G_2) *La loi $\top$ possède un élément neutre ;*

(G_3) *Tout élément de G admet un symétrique pour la loi "$\top$".*

Si de plus la loi $\top$ est commutative, le groupe $(G, \top)$ est appelé ***groupe commutatif*** *ou* ***groupe abélien****.*

Exemples 6.1.1.

1. *$(\mathbb{Z}, +)$ est un groupe abélien. Mais $(\mathbb{Z}, \times)$ n'est pas un groupe.*
2. *$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.*
3. *$(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes.*
4. *$(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.*
5. *Soient E un ensemble non vide et $\mathcal{A}(E)$ l'ensemble des applications de E dans E. On pose $S(E) = \{f \to \mathbb{A}(E) / \quad f$ bijective$\}$. $S(E)$ est une partie stable par la composition des applications "$\circ$".*
   "$\circ$" définit donc une loi de composition interne sur $S(E)$, et muni de cette loi, $S(E)$ est un groupe non abélien. Pour $E = \{1, 2, ..., n\}$, $S(E)$ est noté simplement S_n et est appelé groupe des premutations de n éléments. $Card(S_n) = n!$.
6. *Soit A un ensemble non vide. $\mathcal{P}(A)$ muni de la différence symétrique Δ est un groupe abélien.*

7 *Le produit cartésien de deux groupes $(E, *)$ et $(F, \bullet)$ est un groupe avec la loi cartésienne $\top$:*

$$(e, f)\top(e', f') = (e * e', f \bullet f').$$

En particulier

a *E^2, est un groupe avec la loi cartésienne notée encore $*$*

$$(a, a') * (b, b') = (a * b, a' * b').$$

b *Plus généralement E^n est un groupe avec la loi cartésienne $*$*

$$(x_1, ..., x_n) * (y_1, ..., y_n) = (x_1 * y_1, ..., x_n * y_n).$$

c *$(\mathbb{R}^2, +)$ est un groupe abélien, la loi + étant définie par $\forall (a, b), (c, d) \in \mathbb{R}^2$, $(a, b) + (c, d) = (a + c, b + d)$.*

d *$(\mathbb{R}^3, +)$ est un groupe abélien, la loi + étant définie par $\forall (a_1, a_2, a_3), (b_1, b_2, b_3) \in \mathbb{R}^3$, $(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$.*

e *$\mathbb{R}^n$ est un groupe abélien avec la loi cartesienne +.*

6.1.2 Sous-groupes d'un groupe

a) Définitions et Exemples

Définition 6.1.2. *Soient $(G, *)$ un groupe, d'élément neutre e et H une partie de G. On dit que H est un sous-groupe de $(G, *)$ si les 3 propriétés suivantes sont vérifiées :*

i) $e \in H$

ii) $\forall (x, y) \in H^2$, $x * y \in H$.

iii) $\forall x \in H$, $x^{-1} \in H$

Proposition 6.1.1. *Soient $(G, .)$ un groupe d'élément neutre e et H une partie de G. H est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites :*

(a) $e \in H$,

(b) $\forall x, y \in H, \quad x.y^{-1} \in H$.

Démonstration. Supposons que H est un sous-groupe de G. Alors $e \in H$ d'après la définition 6.1.2 i). Soient $x, y \in H$. On a $y^{-1} \in H$ d'après la définition 6.1.2 iii) et $xy^{-1} \in H$ d'après la définition 6.1.2 ii), d'où la proposition.

Réciproquement, supposons (a) et (b) vraie. Il est clair que $e \in H$. Soit $x \in H$. D'après (b) on a $ex^{-1} \in H$ donc $x^{-1} \in H$ ce qui prouve iii) de la définition 6.1.2.
Soient $x, y \in H$. Alors $x \in H$ et $y^{-1} \in H$, donc $x(y^{-1})^{-1} \in H$, ainsi $xy \in H$. Ce qui prouve ii) de la définition 6.1.2. Par suite, H est un sous-groupe de G. □

Exemples **6.1.2.** — *G lui même et $\{e\}$ où e est l'élément neutre de $(G,*)$ sont des sous-groupes de $(G,*)$. Ces deux sous groupes sont dits triviaux.*

— *$\mathbb{Z}$ est un sous groupe de $(\mathbb{Q},+)$. $\mathbb{Q}$ est un sous groupe de $(\mathbb{R},+)$. $\mathbb{R}$ est un sous groupe de $(\mathbb{C},+)$*

— *$\mathbb{R}^*$, $\{-1,1\}$ sont des sous-groupes de $(\mathbb{R}^*,\times)$.*

— *$U_n=\{z\in\mathbb{C}:\ z^n=1\}$ est un groupe de n éléments de $(\mathbb{C}^*,\times)$.*

— *Pour tout $a\in\mathbb{Z}$, l'ensemble des multiples de a, noté $a\mathbb{Z}$ est un sous groupe de $(\mathbb{Z},+)$.*

— *Plus généralement, si $(G,*)$ est un groupe et $g\in G$, alors l'ensemble des puissances de a : $\{g^n,\ n\in\mathbb{Z}\}$ est un sous-groupe de $(G,*)$.*

$$a^0=e,\quad a^{-2}=(a^{-1})^2,\quad a^{-3}=(a^{-1})^3$$

Remarque **6.1.1.** **1** *Un sous-groupe H n'est pas vide.*

2 *Si H est un sous-groupe de $(G,*)$ alors H est stable pour la loi $*$, et donc $*$ induit une loi de composition interne sur H. Muni de cette loi, H est un groupe, d'où la terminologie "sous - groupe"*

3 *Très souvent pour montrer qu'un ensemble muni d'une loi de composition interne (LCI) est un groupe, on essaie de voir cet ensemble comme un sous-groupe d'un ensemble plus grands.*

4 *Une partie stable d'un groupe n'est pas nécessairement un sous-groupe. Par exemple $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour l'addition, mais ce n'est pas un sous-groupe de $(\mathbb{Z},+)$.*

Théorème **6.1.1** (Caracterisation des sous-groupes de $(\mathbb{Z},+)$)**.** *Soit $H\subset\mathbb{Z}$.*
H un sous-groupe de $(\mathbb{Z},+)$ si et seulement si il existe $a\in\mathbb{N}$ tel que $H=a\mathbb{Z}$.

Démonstration. On montre facilement que pour tous entier n, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$. Si $H=\{0\}$, alors on peut prendre $n=0$ et c'est le seul entier qui convienne.
Si $H\neq\{0\}$, posons, $n=\min(H\cap\mathbb{N}*)$, (n existe dans $\mathbb{N}$, d'après la propriété fondamentale de $\mathbb{N}$), on a $n\in H$, comme H est un sous-groupe de $(\mathbb{Z},+)$, tout multiple de n est dans$H$, c'est-à-dire $n\mathbb{Z}\subset H$. Soit $k\in H$, effectuons la division euclidienne de k par n, $(n\neq 0)$ $k=nq+r$ avec $0\leq r<n$.
On a donc $r=k-nq\in H\cap\mathbb{N}*$, si $r\neq 0$ alors $r\geq n$, ce qui est absurde, donc $r=0$ ce qui donne $k=nq\in\mathbb{Z}$. Par suite, $H=n\mathbb{Z}$. □

b) Intersection de sous-groupes d'un même groupe

Lemme **6.1.1.** *Soient H_1 et H_2 deux sous-groupes d'un même groupe $(G,*)$; $H_1\cap H_2$ est un sous groupe de $(G,*)$.*

Plus généralement si $\{H_i\}_{i\in I}$ est une famille de sous-groupes d'un même groupe $(G,*)$, alors $\bigcap_{i\in I} H_i$ est un sous groupe de $(G,*)$.

Démonstration. **1** $\forall i \in I, \quad e \in H_i$ donc $e \in \bigcap_{i\in I} H_i$.

2 Soient $x, y \in \bigcap_{i\in I} H_i$. $\forall i \in I$ on a $x \in H_i$ et $y^{-1} \in H_i$, donc $xy^{-1} \in H_i$ car H_i est un sous-groupe de G. Ainsi $xy^{-1} \in \bigcap_{i\in I} H_i$.

□

Par suite, $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

c) Sous-groupe engendré par une partie

Définition 6.1.3. *Soit A une partie de G. On appelle sous groupe engendré par A l'intersection de tous les sous-groupes de G contenant A. Ce sous-groupe est le plus petit (au sens de l'inclusion) sous-groupe de $(G,*)$ contenant A. On le note $< A >$.*

Théorème 6.1.2. *Soient G un groupe d'élément neutre e et A une partie de G. Désignons par H l'ensemble des éléments de G qui peuvent s'écrire*

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n} \qquad avec \quad a_i \in A \quad et \quad \varepsilon_i \in \{-1,+1\}, \quad \forall i \in \{1,2,...,n\},$$

en convenant que $H = \{e\}$ si $A = \emptyset$.
Alors H est le sous-groupe de G engendré par A.

Démonstration. — H est non vide, ainsi qu'on le constate en utilisant $A \subset H$ si $A \neq \emptyset$ et $H = \{e\}$ si , $4 = \emptyset$. D'autre part si

$$x = a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n} \qquad et \qquad y = b_1^{\phi_1} b_2^{\phi_2} ... b_n^{\phi_n}.$$

sont deux éléments de H, xy^{-1} s'écrit $a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n} b_1^{-\phi_1} b_2^{-\phi_2} ... b_n^{-\phi_n}$; d'où $xy^{-1} \in H$.
Ainsi H est un sous-groupe de G contenant A.

— Inversement soit L un sous-groupe de G contenant A. Pour toute famille finie $(a_1, ..., a_n)$ d'éléments de A, $a_1^{-1}, ...a_n^{-l}$ sont aussi des éléments de L, et il en est de même de tout produit de la forme $a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n}$; on a donc $H \subset L$,
H est ainsi le plus petit sous-groupe de G contenant A.

□

Exemple 6.1.1. *si $A = \emptyset$, $< \emptyset >= \{e\}$; $A = x$, $< x >= \{x^n,\ n \in \mathbb{Z}\}$.*

d) Réunions de sous-groupes

La réunion de deux sous-groupes d'un même groupe G n'est pas un sous-groupe (en général). Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous groupe de $\mathbb{Z}$.

6.1.3 Classes d'équivalence suivant un sous-groupe

a) Relation de Lagrange

Soient $(G, *)$ un groupe, d'élément neutre e, et H un sous-groupe de $(G, *)$. H permet de définir sur G la relation binaire $\mathcal{R}_H$ suivant :

$$\forall (x, y) \in G^2, \qquad x\mathcal{R}_H y \quad si \quad x^{-1} * y \in H.$$

On a le théorème suivant :

Théorème 6.1.3 (de Lagrange). *i) $\mathcal{R}_H$ est une relation d'équivalence.*

ii) La classe d'équivalence d'un point $a \in G$ est $\overline{a} = \{a * h, \quad h \in H\}$ qu'on note $a * H$.

iii) Il y a une bijection entre $\overline{e} = H$ et $\overline{a} = aH$.

iv) Si G est un groupe fini, on a

$$Card(G) = Card(H).Card(\frac{G}{\mathcal{R}_H}).$$

Démonstration. i) à faire en exercice

ii) $a^{-1} * (a * h) = h \in H$, donc $(a * h)\mathcal{R}_H a$

iii) $\phi : H \to aH$; $h \mapsto a * h$ est une application bijective.

iv) Comme G est fini, l'ensemble des classes d'équivalence est aussi fini on a

$$G = H \cup (x_1 * H) \cup (x_2 * H) \cup .. \cup (x_k * H).$$

d'où $Card(G) = Card(H) + Card(x_1 * H) + ... + Card(x_k * H)$.
Comme $Card(x_i * H) = Card(H)$, on a $Card(G) = Card(H).Card(\frac{G}{\mathcal{R}_H})$.

□

Remarque 6.1.2. *H permet de définir une autre relation binaire $\mathcal{R}'_H$ sur G par :*

$$x\mathcal{R}'_H y, \quad si \quad x * y^{-1} \in H.$$

$\mathcal{R}'_H$ a toutes les propriétés dans le théorème de lagrange, sauf que la classe d'équivalence de $a \in G$ est $H * a = h * a, \ h \in H$. Très souvent, on a

$$a * H \neq H * a$$

b) Sous-groupes distingés dans un groupe

Définition 6.1.4. *Un sous-groupe H de $(G,*)$ est dit distingué dans G si on a :*

$$\forall x \in G, \quad \text{on a} \quad x * H = H * x.$$

On note $H \lhd G$.

Exemple 6.1.2. **1** *$\{e\}$ et G les deux sous groupes triviaux sont distingués.*

2 *Tout sous-groupe d'un groupe abélien est distingué.*

Proposition 6.1.2. *Soit H un sous-groupe de G. Les assertions suivantes sont équivalentes.*

i) H *est un sous-groupe distingué de* G,

ii) $\forall x \in G,\ xHx^{-1} = H$,

iiii) $\forall x \in G, \forall h \in H,\ xhx^{-1} \in H$,

iv) $\forall x \in G,\ xH \subset Hx$,

v) $\forall x \in G,\ Hx \subset xH$..

Démonstration. A faire en exercice. □

6.1.4 Groupes-quotients

Proposition 6.1.3. *Soit H est un sous-groupe distingué de $(G,*)$,*

a) $\mathcal{R}_H = \mathcal{R}'_H$

b) $\mathcal{R}_H$ *est compatible avec la loi* $*$ *c'est à dire :*
si $a\mathcal{R}_H b$ *et* $x\mathcal{R}_H y$, *alors* $(a*x)\mathcal{R}_H(b*y)$.

Démonstration. a) Il faut montrer que $a\mathcal{R}_H b \Leftrightarrow a\mathcal{R}'_H b$
Soit $(a,b) \in G^2$ tel que $a\mathcal{R}_H b$.
Alors $a^{-1} * b \in H$. Comme H est distingué dans G, $a * (a - 1 * b) * a^{-1} \in H$.
c'est-à-dire $b * a^{-1} \in H$, donc $b\mathcal{R}'_H a$ et $a\mathcal{R}'_H b$ (puisque $\mathcal{R}'_H$ est symétrique).

Réciproquement, si $a\mathcal{R}'_H b$, alors $a * b^{-1} \in H$. H étant distingué dans G, on a $b^{-1}(a * b^{-1}) * b \in H$. Ainsi $b^{-1} * a \in H$ et $a\mathcal{R}_H b$.

b) Soient $(a,b) \in G^2$, $(x,y) \in G^2$ tels que $a\mathcal{R}_H b$ et $x\mathcal{R}_H y$. on a :

$$\begin{aligned}(a*x)^{-1} * (b*y) &= x^{-1} * (a^{-1} * b) * y \\ (a*x)^{-1} * (b*y) &= (x^{-1} * (a^{-1} * b) * x) * (x^{-1} * y) \in H.\end{aligned}$$

□

Notation **6.1.1.** *Si H est distingué, l'ensemble quotient $\frac{G}{\mathcal{R}_H}$ est noté $\frac{G}{H}$*

Proposition **6.1.4.** *La loi $*$ induit une loi de composition interne sur $\frac{G}{H}$ par :*

$$(\overline{a}, \overline{b}) \mapsto \overline{a * b}.$$

$\frac{G}{H}$ muni de cette loi (encore notée $*$) est un groupe, appelé groupe quotient.

Exemple **6.1.3.** *$G = \mathbb{Z}$ avec l'addition + et $H = 4\mathbb{Z}$, $\frac{\mathbb{Z}}{4\mathbb{Z}}$ est un groupe avec l'addition $\overline{a} + \overline{b} = \overline{a + b}$.*
La table de + de $\frac{\mathbb{Z}}{4\mathbb{Z}}$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

6.1.5 Homomorphismes de groupes

Définition **6.1.5.** *Soient $(G, *)$, $(H, \top)$ deux groupes et $f : G \to H$ un homomorphisme. L'homomorphisme f est appelé homomorphisme (ou morphisme) de groupes.*
*On appelle **noyau** de f et on note $\ker(f)$, le sous-ensemble de G défini par*

$$\ker(f) = \{x \in G / f(x) = e_H\}$$

où e_H est l'élément neutre du groupe H.
*L'**image** de f, notée $Im(f)$ ou $f(G)$, est le sous-ensemble de H défini par*

$$Im(f) = \{h \in H / \forall x \in G, y = f(x)\}.$$

Exemple **6.1.4.**

1 *L'application $g : (\mathbb{R}_+^*, \times) \to (\mathbb{R}+)$ définie par $x \mapsto \ln(x)$ est un morphisme de groupes.*

2 *Soit $n \in \mathbb{N}^*$. L'application $f : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ définie par $z \mapsto z^n$ est un morphisme de groupes.*

Remarque **6.1.3.** *L'homomorphisme f satisfait la propriété suivante :*

$$\forall x \in G, \qquad f(x^{-1}) = (f(x))^{-} \not\vdash.$$

Théorème **6.1.4.** *Soit $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$ un morphisme de groupes continu en 0, alors :*

$$\forall x \in \mathbb{R}, \qquad f(x) = ax.$$

où $a = f(1)$.

Démonstration. On pose $a = f(1)$, on montre que $\forall n \in \mathbb{N}$, $f(n) = an$ (récurrence), on en déduit que $f(-n) = a(-n)$ car $f(-n) = -f(n)$, d'où : $\forall n \in \mathbb{Z}$, $f(n) = an$. Soit $r = \frac{p}{q}$ un rationnel avec $q \in \mathbb{N}^*$, alors $f(qr) = f(p) = ap = qf(r)$ d'où $f(r) = ar$.
Soit $x \in \mathbb{R}$ et (r_n) une suite de rationnels qui converge vers x, alors $(x - r_n)$ converge vers 0 et donc $f(x - r_n)$ tend vers $f(0) = 0$, or $f(x - rn) = f(x) - f(rn)$ donc $(f(rn))$ converge vers $f(x)$. Or $f(r_n) = ar_n \to ax$, par conséquent $f(x) = ax$. □

Proposition 6.1.5. *Soit $f : G \to H$ un morphisme de groupes. L'image directe par f de tout sous-groupe de G est un sous-groupe de H. En particulier, $Im(f)$ est un sous-groupe de H.*

Démonstration. Soit K un sous-groupe de G. Montrons que $f(K)$ est un sous-groupe de H.

1) Comme $e_G \in K$ alors $f(e_G) \in f(K)$.
2) Soient $a, b \in f(K)$. Alors, il existe $x, y \in K$ tel que $a = f(x)$ et $b = f(y)$. Ainsi

$$ab^{-1} = f(x)f(y^{-1}) = f(xy^{-1}).$$

or $xy^{-1} \in K$ donc $ab^{-1} \in f(K)$. En somme $f(K)$ est un sous-groupe de H. On déduit aussi que $Im(f) = f(G)$ est un sous-groupe de H.

□

Proposition 6.1.6. *Soit $f : G \to H$ un morphisme de groupes. L'image réciproque par f de tout sous-groupe de H est un sous-groupe de G contenant* $\ker f$. *En particulier,* $\ker(f)$ *est un sous-groupe de G.*

Démonstration. A faire en exercice. □

Théorème 6.1.5. *Soit $f : G \to G'$ un morphisme de groupes.*

1 *Si H est un sous-groupe distingué de G, $f(H)$ est un sous-groupe distingué de $f(G)$.*

2 *Si H' est un sous-groupe distingué de G', $f^{-1}(H')$ est un sous-groupe distingué de G.*

Démonstration. **1** Soit $H \lhd G$. Il faut montrer :

$$\forall (a', h') \in f(G) \times f(H) \qquad a'h'(a')^{-1} \in f(H),$$

c'est-à-dire :

$$\forall (a, h) \in G \times H \qquad f(a)f(h)(f(a))^{-1} \in f(H),$$

ce qui résulte de ce que $f(a)f(h)(f(a))^{-1}$ est l'image par f de aha^{-1}, qui est un élément de H (car $(a, h) \in G \times H$).

2 Soit $H' \lhd G'$. Posons $H = f^{-1}(H')$. Il faut montrer : $\forall (a,h) \in G \times H, aha^{-1} \in H$. Cela résulte de ce que $f(aha^{-1})$ qui s'écrit $f(a)f(h)(f(a))^{-1}$, est un élément de H' (car $(f(a), f(h)) \in G' \times H'$).

□

Proposition 6.1.7. *Soit $f : G \to H$ un morphisme de groupes.*

$$f \text{ injective} \Leftrightarrow \ker f = \{e_G\}.$$

Démonstration. ($\Rightarrow$) Supposons f injective. Pour tout $x \in \ker f$ on a $f(x) = f(e_G)$. Le caractère injectif de f implique que $x = e_G$, donc $\ker f = \{eG\}$.
($\Leftarrow$) Supposons $\ker f = \{e_G\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. On a $f(x).(f(y))^{-1} = e_H$. Comme $(f(y))^{-1} = f(y^{-1})$ on a $f(x).f(y^{-1}) = e_H$. Ainsi $f(x.y^{-1}) = e_H$, d'où $x.y^{-1} \in \ker f$ et comme $\ker f = \{eG\}$, on a $x.y^{-1} = e_G$, c'est à dire que $x = y$. Donc f est injective. □

6.2 Anneaux

6.2.1 Définition et exemples

Définition 6.2.1. *On appelle anneau tout triplet $(A, +, .)$, où A est un ensemble dit sous-jacent à l'anneau, où + et . sont des lois de composition internes sur E dites addition et multiplication, satisfaisant aux axiomes suivants :*

(A_1) *$(A, +)$ est un groupe abélien, dit groupe additif de l'anneau ; l'élément neutre est noté 0 et est appelé élément nul ;*

(A_2) *La multiplication est associative et admet un élément neutre, noté 1, (1_A en cas d'ambiguïté), et appelé élément-unité ;*

(A_3) *La multiplication est distributive par rapport à l'addition.*

— *On qualifie de commutatif tout anneau dans lequel la multiplication est commutative.*

— *L'anneau A est dit unitaire si la multiplication admet un élément neutre.*

Notation 6.2.1.

— *L'élément neutre de + deux A est noté 0_A et pour tout $x \in A$, le symétrique de x par rapport à la loi $+$ est noté $-x$. (on dit que $-x$ est l'opposé de x)*

— *Si l'anneau A est unitaire, l'élément neutre de la multiplication " $\cdot$ " dans A est noté 1_A. Un élément $x \in A$ sera dit inversible, s'il admet un symetrique par rapport à la multiplication, dans ce cas le symétrique de x est noté x^{-1}. On note $\mathcal{U}(A)$ l'ensemble de tous les éléments inversibles de A. $\mathcal{U}(A)$ est stable pour la multiplication et $(\mathcal{U}(A), .)$ est un groupe.*

— *Pour tout $a \in A$, et pour tout $n \in \mathbb{N}^*$ on pose :*

$$a^n = \underbrace{a.a \cdot \cdot \cdot a}_{n fois} \qquad et \qquad na = \underbrace{a + a + \cdot \cdot \cdot + a}_{n fois}.$$

Exemples **6.2.1.** **1** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition + et de la multiplication $\times$ sont des anneaux commutatifs et unitaires.*

2 *Soit $(G, +)$ est un groupe abélien. On note $End(G)$ l'ensemble de tous les endomorphisme de G. $(End(G), +, \circ)$ est un anneau en posant :*

$$f, g \in End(G), \quad f + g : x \mapsto f(x) + g(x) \quad et \quad f \circ g : x \mapsto f(g(x)).$$

3 *$(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif unitaire ayant n éléments.*

4 *Si A et A' sont 2 anneaux, il y a sur $A \times A'$ une structure naturelle d'anneau*

$$(a, a') + (b, b') = (a + b, a' + b') \qquad et \qquad (a, a').(b, b') = (a.b, a'.b').$$

En particulier $\mathbb{Z}^2$, $\mathbb{Z}^3$, $\mathbb{Z}^3$, $\mathbb{C}^2$, ... sont des anneaux.

6.2.2 Propriétés remarquables dans l'anneau

i) $0_A.x = 0_A$, $x.0_A = 0_A$ pour tout $x \in A$.

ii) $-(x.y) = (-x).y = x.(-y)$ pour tout $(x, y) \in A^2$

iii) Si A est un anneau unitaire, on a $(-1_A).x = -x$

iv) Si x et y commutent (par rapport à "· ") c'est-à-dire $x.y = y.x$ alors

$$(x.y)^2 = x^2y^2, \quad (x.y)^3 = x^3.y^3 \quad , ..., \quad (x.y)^n = x^n.y^n \quad \forall n \in \mathbb{N}^*,$$

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

Plus généralement

$$(x + y)^3 = x^3 + 3(x^2y) + 3(xy^2) + y^3$$

$$\begin{aligned} (x + y)^n &= \sum_{k=0}^{n} C_n^k x^k y^{n-k} \\ &= x^n + C_n^1 xy^{n-1} + C_n^2 x^2 y^{n-2} + ... + C_n^k x^k y^{n-k} + ... + C_n^{n-1} xy^{n-1} + y^n. \end{aligned}$$

Exercice 4. *Soit $a \in A$. Calculer $(1_A + a)^5$*

Définition **6.2.2.** *Soit A un anneau, on dit que $a \in A$ est un diviseur de zéro dans A si $a \neq 0$ et s'il existe $b \in A$, $b \neq 0$ tel que*

$$ab = 0 \qquad ou \qquad ba = 0.$$

Exemple **6.2.1.** *Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément 3 est un diviseur de 0.*

Exercice 5. *Déterminer tous les diviseurs de 0 de l'anneau $\mathbb{Z}/24\mathbb{Z}$.*

Définition **6.2.3.** *On dit que A est intègre si A est commutatif, non réduit à zéro et dépourvu de diviseur de zéro, c'est à dire que*

$$\forall a, b \in A, \qquad ab = 0 \;\Rightarrow\; a = 0 \quad ou \quad b = 0.$$

Exemple **6.2.2.** **1** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des anneaux intègres.*

2 *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre si et seulement si $n = 0$ ou n est un nombre premier.*

3 *$(\mathbb{Z}, +, \times)$ est intègre.*

6.2.3 Sous-anneaux, Idéaux

a) Sous-anneaux

Définition **6.2.4.** *Soient A un anneau commutatif unitaire et B une partie de A. On dit que B est un sous-anneau de A si :*

i) B est un sous-groupe de $(A, +)$

ii) B contient 1_A et B est stable par le produit $\forall b, b' \in B$, $bb' \in B$.

Exemple **6.2.3.**
- *$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$*
- *$\mathbb{R}$ est un sous-anneau de $\mathbb{C}$*
- *$\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$*

Remarque **6.2.1.** *L'intersection de sous-anneaux est un sous-anneau. On a alors la notion de sous-anneau engendré par une partie quelconque X d'un anneau A.*
Si 1_A est l'élément unité de l'anneau $(A, +, .)$, tous les sous-anneaux contiennent le sous-anneau

$$\mathbb{Z}.1_A.$$

b) Idéaux

Définition **6.2.5.** *On dit que B est un idéal de A si*

1 *B est un sous-groupe de $(A, +)$*

2 *$\forall a \in A$, $\forall b \in B$, on a $ab \in B$.*

Exemple **6.2.4.**
- *$\{0_A\}$, A sont des idéaux de A (dits triviaux)*
- *aA l'ensemble des multiples de a dans A est un idéal (dit principal).*
- *Les idéaux de l'anneau $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$*

Remarque **6.2.2.**
- *L'intersection d'idéaux d'un anneau est un idéal. On a donc la notion de d'idéal engendré par une partie quelconque X d'un anneau A.*
- *Le seul idéal qui contient 1_A l'élément unité de l'anneau $(A, +, .)$ ou tout autre élément inversible est l'idéal A lui-meme.*

Définition **6.2.6.**
- *Un idéal I est dit propre s'il est différent de l'anneau A et de l'idéal $\{0\}$.*
- *Parmi les idéaux propres, un idéal M est dit maximal s'il n'est contenu strictement dans aucun autre idéal propre.*

Exemple **6.2.5.** *dans l'anneau $(\mathbb{Z}, +, .)$ les idéaux $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}$..... sont maximaux.*

Remarque **6.2.3.** *Notons que la réunion de deux idéaux d'un anneau n'est un idéal.*

6.2.4 Anneaux quotients

Proposition **6.2.1.** *Si I est un idéal de A, alors les lois " + " et " $\cdot$ " sont compatibles avec la relation d'équivalences (de Lagrange)*

$$a\mathcal{R}b \qquad si \qquad b - a \in I.$$

Proposition **6.2.2.** *L'ensemble quotient $\dfrac{A}{I}$ muni des lois de composition internes*

$$\overline{a} + \overline{b} = \overline{a + b} \quad ; \quad \overline{a}.\overline{b} = \overline{a.b}.$$

est un anneau commutatif unitaire.

Exercice 6.
1 *Ecrire les tables de l'addition et de la multiplicattion de l'anneau quotient $\dfrac{\mathbb{Z}}{6Z}$.*
2 *Trouver $\mathcal{U}(A)$.*

6.2.5 Morphisme d'anneaux

Définition **6.2.7.** *Soient A, B deux anneaux unitaires, et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux (ou un homomorphisme) de A dans B si*

i) $f(1_A) = 1_B$,

ii) $\forall a, b \in A,\ f(a + b) = f(a) + f(b)$,

iii) $\forall a, b \in A,\ f(ab) = f(a)f(b)$.

On définit de façon évidente les notions d'endomorphisme, d'isomorphisme et d'automorphisme d'anneaux.

Exemples **6.2.2.** **1** *L'application* $z \mapsto \overline{z}$ *est un automorphisme de l'anneau* $\mathbb{C}$.

2 *L'application* $(u_n) \mapsto \lim_{n\to+\infty} u_n$ *est un morphisme de l'anneau des suites convergentes dans* $\mathbb{R}$.

Théorème **6.2.1.** *Soit* $f : A \to B$ *un morphisme d'anneaux.*

i) Si A *est un sous-anneau de* A *alors* $f(A)$ *est un sous-anneau de* B,

ii) Si B *est un sous-anneau de* B *alors* $f^{-1}(B)$ *est un sous-anneau de* A,

iii) Si A et B sont commutatifs, et si I' *est un idéal de* B *alors* $f^{-1}(I')$ *est un idéal de* A.
En particulier, $\ker f = \{x \in A / f(x) = 0\}$ *est un idéal de A.*

Proposition **6.2.3.** *Soit f :* $A \to B$ *un morphisme d'anneaux. On a l'équivalence*

$$f \text{ injectif} \Leftrightarrow ker f = 0.$$

Démonstration. Le morphisme d'anneaux est un morphisme de groupes . D'après la proposition 6.1.7, on a le résultat. □

Théorème **6.2.2.** *Soient* A, B, C *trois anneaux.*

1 *Si* $f : A \to B$ *et* $g : B \to C$ *sont des morphismes d'anneaux alors* $g \circ f : A \to C$ *est un morphisme d'anneaux.*

2 *Si* $f : A \to B$ *est un isomorphisme d'anneaux alors* f^{-1} *est un isomorphisme de* B *sur* A.

3 $(End(A), +, \circ)$ *est un anneau, dont le groupe des unités est* $(Aut(A), \circ)$.

Démonstration. A faire en exercice. □

Théorème **6.2.3** (Transport de structure)**.** *Si* A *est un anneau et* f *une bijection de* A *sur un ensemble* E, *alors on peut définir deux lois sur* E, *de sorte que* f *devienne un isomorphisme d'anneaux.*

Démonstration. A faire en exercice. □

6.3 Corps

6.3.1 Définitions-exemples

Définition **6.3.1.** *On dit qu'un ensemble* $\mathbb{K}$ *muni de deux lois "+" et " × " est un corps si*

i) $(\mathbb{K}, +, \times)$ *est un anneau, et* $1_{\mathbb{K}} \neq 0$,

ii) $\forall x \in \mathbb{K}\backslash\{0\}$, $\exists x' \in \mathbb{K}$, $x'x = 1_{\mathbb{K}} = xx'$.

Si de plus la multiplication est commutative, on dit que $\mathbb{K}$ *est un corps commutatif.*

Remarque **6.3.1.** *Un anneau* $\mathbb{K}$ *est un corps s'il n'est pas réduit à 0 et si tout élément non nul de* $\mathbb{K}$ *est inversible.*

Remarque **6.3.2.** **1** *Si* $\mathbb{K}$ *est un corps alors* $\mathbb{K}\backslash\{0\}$ *est un groupe multiplicatif qui est abélien si et seulement si* $\mathbb{K}$ *est commutatif.*

2 *Un corps est en particulier un anneau sans diviseurs de zéro.*

3 *Si* I *est un idéal du corps* $\mathbb{K}$ *alors* $I = \{0\}$ *ou* $I = \mathbb{K}$.

Exemples **6.3.1.** *1)* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *sont des corps commutatifs pour les lois usuelles.*

2) $\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} / \ \forall a, b \in \mathbb{Q}, \quad x = a + b\sqrt{2}\}$ *est un corps commutatif*

3) $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si* n *est un nombre premier.*

Exemple **6.3.1.** *Tout anneau intègre fini* A *est un corps. En effet :*
On sait que $A \neq \{0\}$. *Soit* $a \in A\backslash\{0\}$ *; associons-lui l'endomorphisme* $x \to ax$ *du groupe* $(A, +)$ *qui est une injection, puisque,* a *étant régulier,* $ax = 0$ *équivaut à* $x = 0$*;* A *étant fini, il s'agit même d'une bijection. Il existe donc un, et un seul* $a' \in A$ *tel que* $aa' = 1$*; par commutativité* $a'a = 1$*;* a *est donc inversible.*

6.3.2 Sous-corps

Définition **6.3.2.** *Soient* $\mathbb{K}$ *un corps et* K *une partie de* $\mathbb{K}$. *On dit que* K *est un sous-corps de* $\mathbb{K}$ *ou que* $\mathbb{K}$ *est un sur-corps de* K *si :*

(i) K *est un sous-anneau de* $\mathbb{K}$,

(ii) $\forall x \in K\backslash\{0\}, \qquad x^{-1} \in K\backslash\{0\}$.

Exemple **6.3.2.** *(a)* $\mathbb{Q}$ *est un sous-corps de* $\mathbb{Q}[\sqrt{2}]$ *qui est lui-même un sous-corps de* $\mathbb{R}$.

(b) $\mathbb{Z}/p\mathbb{Z}$ *(*p *premier) n'a pas de sous-corps propres.*

Proposition **6.3.1.** *Soient* $\mathbb{K}$ *un corps et* K *une partie de* $\mathbb{K}$. *Alors* K *est un sous-corps de* $\mathbb{K}$ *ssi :*

1) $1_{\mathbb{K}} \in K$,

2) $\forall x, y \in K$, $x - y \in K$,

3) $\forall x, y \in K$, $xy \in K$,

4) $\forall x \in K\backslash\{0\}$, $x^{-1} \in K\backslash\{0\}$.

Démonstration. $(\Rightarrow)$ Supposons que K est un sous-corps de $\mathbb{K}$. K est donc un sous-anneau de $\mathbb{K}$ et que l'on a $x^{-1} \in K$ pour tout élément non nul x de K. Par suite, les assertions 1), 2), 3) et 4) sont véréfiés.

$(\Leftarrow)$ Supposons que les assertions 1), 2), 3) et 4) sont véréfiés. Les assertions 1), 2) et 3) expriment que K est un sous-anneau de $\mathbb{K}$. L'assertion 4) exprime que l'inverse de tout élément non-nul de K est dans K. Par suite, K est un sous-corps de $\mathbb{K}$. □

Remarque **6.3.3.** *On montre, comme pour les sous-groupes, que toute intersection d'une famille de sous-corps d'un corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ et que, pour toute partie $X \subset \mathbb{K}$, il existe un plus petit sous-corps de $\mathbb{K}$ contenant X, on dit qu'il s'agit du sous-corps engendré par X.*

Bibliographie

[1] **A. Bodin** : *Algèbre*. Exo 7 (2016).

[2] **B. Calvo, J. Doyen, A. Calvo, F. Boschet** : *Cours d'analyse*. Armand Colin - collection U (1977).

[3] **C. Deschamps, A. Warusfel, F. Moulin, J. François Ruaud, A. AAiquel, J-C Sifre** : *Mathématiques TOUT-EN-UN • I^e année : cours exercices corrigés MPSI-PCSI*. Dunod, Paris, (2003).

[4] **D. Fredon** : *Mathématiques Résumé du cours en fiches MPSI - MP*. Dunod, Paris, (2010).

[5] **M. Allano Chevalier, X. Oudot** : *Maths MPSI*. Hachette, (2008).

[6] **M. K.KOUAKOU** : *Cours de première année : Eléments de Logique*. (2012).

[7] **M. Queysanne** : *ALGÈBRE M. P et Spéciales A-A'*. Cinquième édition revue et corrigée LIBRAIRIE ARMAND COLIN 103, boulevard Saint-Michel, Paris-5e (1964).

[8] **T. Pierron** : *Mathématiques MPSI*. ENS Ker Lann.

[9] **A. Soyeur, F. Capaces, E. Vieillard-Baron** : *Cours de Mathématiques Sup MPSI PCSI PTSI TSI* . sesamath.net (2011).

[10] **E. Ramis, C. Deschamps, J. Odoux** : *Cours de Mathématiques Spéciales Algèbre*. Masson (1993).

[11] **J. Dixmler** : *Cours de Mathématiques du premier cycle* 1^e *année*, Gauthier-villars, (1976).

[12] **N. Bourbaki** : *Éléments de Mathématique : Algèbre*. Springer (1970).

[13] **P. Bornsztein, X. Caruso, P. Nolin, M. Tibouchi** : *Cours d'arithmétique*. (2004).