COURS DE MATHÉMATIQUES: ALGEBRE 1 2022 - 2023

UTA

Table des matières

1 Ensembles **5**

1.1 Définitions, Exemples 5
1.2 Ecritures d'un ensemble 6
1.3 Diagrammes de Venn 7
1.4 Inclusion, égalité, ensemble des parties 8
1.4.1 Inclusion 8
1.4.2 Ensembles égaux 8
1.4.3 Ensemble des parties 9
1.5 Opérations élémentaires dans les ensembles 9
1.5.1 Activité 9
1.5.2 Intersection, réunion, différence, Différence symétrique, complémentaire, produit cartésien 10
1.5.3 Propriétés des opérations élémentaires 13

2 Logique **17**

2.1 Définitions 17
2.2 Des symboles à connaître 18
2.2.1 Implication, réciproque et équivalence 18
2.2.2 Les quantificateurs pour tout $\forall$ et il existe $\exists$ 19
2.3 Opérations logiques dans un ensemble 20
2.3.1 Opérations logiques élémentaires 20
2.3.2 L'implication et l'équivalence de deux propriétés 20
2.4 Logique mathématique classique 21

3 Raisonnements Mathématiques **23**

3.1 Raisonnement direct 23
3.1.1 Principe 23
3.1.2 Exemples 23
3.2 Raisonnement par double implication 24
3.2.1 Principe 24

3.2.2 Exemples 24
3.3 Raisonnement par disjonction de cas ou Raisonnement cas par cas 26
3.3.1 Principe 26
3.3.2 Exemples 26
3.4 Raisonnement par élimination des cas 27
3.4.1 Principe 27
3.4.2 Exemples 27
3.5 Raisonnement par contraposée 28
3.5.1 Principe 28
3.5.2 Exemples 28
3.6 Raisonnement par l'absurde 29
3.6.1 Principe 29
3.6.2 Exemples 29
3.7 Raisonnement par contre-exemple 30
3.7.1 Principe 30
3.7.2 Exemples 31
3.8 Raisonnement par récurrence 31
3.8.1 Principe de la récurrence classique 31
3.8.2 Exemples 32
3.8.3 Principe de la récurrence forte 33
3.8.4 Exemples 34
3.9 Raisonnement par analyse-synthèse 34
3.9.1 Principe 34
3.9.2 Exemples 34

4 Relations binaires dans un ensemble 36
4.1 Définitions et exemples 36
4.2 Mode de représentation 37
4.2.1 Diagramme cartésien 37
4.2.2 Matrice binaire 37
4.2.3 Diagramme sagittal 38
4.3 Quelques propriétés remarquables des relations binaires 39
4.4 Relation d'ordre 40
4.4.1 Dénitions et exemples 40
4.4.2 Eléments singuliers dans un ensemble ordonné 40
4.5 Relation d'équivalence 42
4.5.1 Dénitions et exemples 42
4.5.2 Classes d'équivalence 43

5 Applications d'un ensemble vers un autre **44**
5.1 Relations d'un ensemble vers un autre 44
5.1.1 Définitions 44
5.1.2 Notation 44
5.1.3 Exemple 44
5.2 Applications 45
5.2.1 Définitions 45
5.2.2 Exemples et contre-exemples 45
5.2.3 Egalité de deux applications 45
5.2.4 Fonctions caractéristiques 46
5.2.5 Image directe, Image réciproque 46
5.2.6 Composition des applications 47
5.2.7 Applications injectives, surjectives, bijectives 48
5.2.8 Ensembles dénombrables 50

6 Lois de composition internes et externes **51**
6.1 Lois de composition internes (LCI) 51
6.1.1 Définitions et exemples 51
6.1.2 Partie stable par une Loi de composition interne, loi induite . . . 51
6.1.3 Loi associative 52
6.1.4 Lois commutatives 52
6.1.5 Elément neutre à gauche, élément neutre à droite, élément neutre . 53
6.1.6 Elément symétrique à gauche, à droite, élément symétrique 54
6.1.7 Distributivité 55
6.2 Lois de composition externes (LCE) 55
6.2.1 Définitions et exemples 55
6.2.2 Partie stable par une loi de composition externe, loi induite 55
6.2.3 Distributivité 56

7 Structures algébriques **57**
7.1 Groupes 57
7.1.1 Définitions et exemples 57
7.1.2 Sous-groupes d'un groupe 58
7.2 Anneaux 59
7.2.1 Définition et exemples 59
7.2.2 Propriétés remarquables dans l'anneau 60
7.2.3 Sous-anneaux, Idéaux 61
7.3 Corps 62
7.3.1 Définitions-exemples 62

7.3.2 Sous-corps 63

BIBLIOGRAPHIE **64**

Chapitre 1

Ensembles

1.1 Définitions, Exemples

Définition 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.
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 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 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 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 $a \in a$.

Exemple 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'UIST inscrits pour cette année universitaire :*
5. $a, b, c, \cdots, z$ *est l'ensemble des lettres de l'alphabet français.*
6. *La collection* $\{*, 1, *\}$ *n'est pas un ensemble.*

Notation 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 2 (écriture en extension)**.**
Écrire un ensemble en ***extension*** *veut dire donner une liste de tous ses éléments.*

Exemple 2.
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 inférieurs ou égal a 6 est écrit en extension :*
$$E = \{0, 1, 2, 3, 4, 5, 6\}.$$

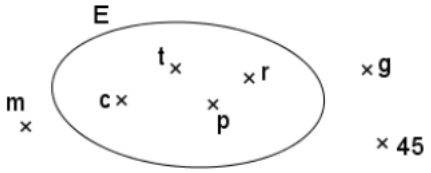
Définition 3 (écriture en compréhension)**.**
Écrire un ensemble en ***compréhension*** *veut dire donner une propriété caractéristique de ses éléments.*

Exemple 3.
- *« 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 impairs est ecrit en comprehension :*
$$P = \{2n + 1,\ n \in \mathbb{Z}\}.$$
- *L'ensemble* S *de toutes les puissances entières de 5 est écrit en comprehension :*
$$S = \{5^n,\ n \in \mathbb{Z}\}.$$

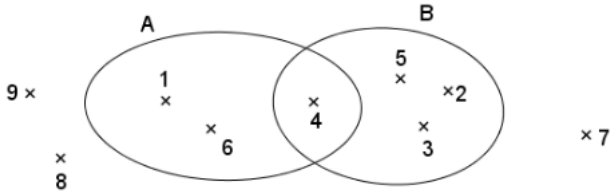
1.3 Diagrammes de Venn

- 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.
- 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 !
- 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)

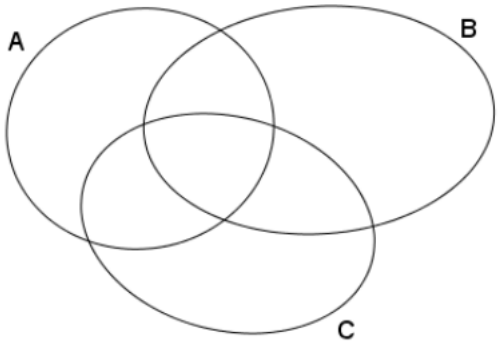
Exemple **4.** $E = \{c; t; r; p\}$



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



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

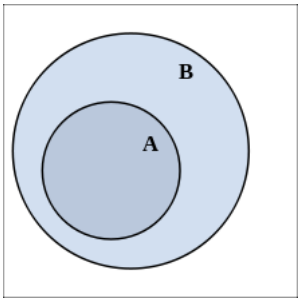


1.4 Inclusion, égalité, ensemble des parties

1.4.1 Inclusion

Définition 4.
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 7.



$$A \subset B$$

Exemple 8.

- *L'ensemble des poulets est contenu dans celui des oiseaux.*
- *L'ensemble*
$$\left\{ \frac{\sin x}{2+n};\ x \in \mathbb{R},\ n \in \mathbb{N} \right\}$$
est contenu dans $]-1,1[$.
- $\{*\} \subset \{*, \triangle\}$, $\{\triangle\} \subset \{*, \triangle\}$, $\{*, \square\} \not\subseteq \{\square, \triangle, O\}$ *et* $\{\square, \triangle, O\} \not\subseteq \{*, \square\}$.

Remarque 5.

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 5.
Deux ensembles sont égaux s'ils ont les mêmes éléments.

Exemple 9.

- *Les ensembles $A = \{1; 2; 3; 4; 5; 6; 7\}$ et $B =]0; 7] \cap \mathbb{N}$ sont égaux.*

– *Les ensembles* $C = \{1; 2; 3; 7\}$ *et* $D = \{9; 5; 2; 1\}$ *ne sont pas égaux*

Proposition 1.
Deux ensembles A *et* B *sont égaux si et seulement si* A *est inclus dans* B *et* B *est inclus dans* A.

Remarque 6.
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.

Remarque 7.
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 6.
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 8.
- *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 *:* $\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

- *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 :* $\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

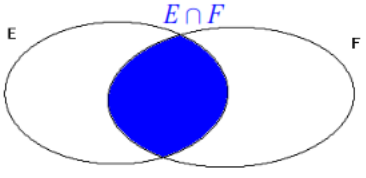
Combien existe-t-il d'éléments qui n'appartiennent ni à A, ni à B ? $\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$.
On a aussi ceux qui appartiennent à A ou à B : $\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$.

1.5.2 Intersection, réunion, différence, Différence symétrique, complémentaire, produit cartésien

Soit E, F et G trois ensembles et A une partie de E.

Opérations	Notations	Définitions
Intersection	$E \cap F$	$\{x \in E \quad et \quad x \in F\}$
Réunion	$E \cup F$	$\{x \in E \quad ou \quad x \in F\}$
Différence	$E - F$ *ou* $E \backslash F$	$\{x \in E \quad et \quad x \notin F\}$
Différence symétrique	$A \triangle B$	$\{x \in A \backslash B \; ou \; x \in B \backslash A\}$
Complémentaire	$E - A$ *ou* $E \backslash A$ *ou* $C_E A$ *ou* $\overline{A}$	$\{x \in E \quad et \quad x \notin A\}$
Produit cartésien	$E \times F$	$\{(x; y)/x \in E \; et \; x \in F\}$

Exemple 10 (Intersection)**.**



Exemple 11 (Intersection)**.**

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 **9.**

- $A \cap B = B \cap A$.
- $A \cap B \subset A$ *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* $\{1, 2, \cdots, n\}$,

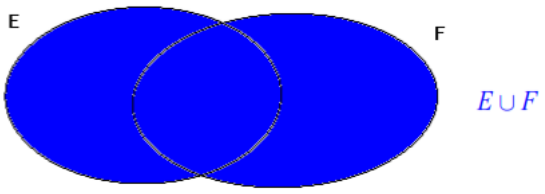
$$i \neq j \Rightarrow A_i \cap A_j = \emptyset.$$

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

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

$$ou \quad (3) \quad a \notin A \quad et \quad a \notin B.$$

Exemple **12** (Réunion)**.**



Exemple **13** (Réunion)**.**

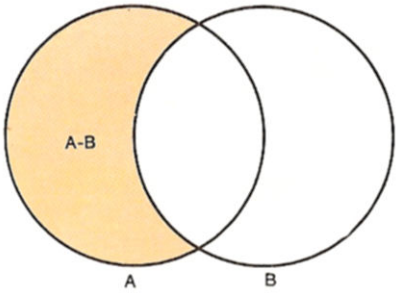
1. *Pour l' activité 1.5.1 :* $A \cup B = \{\cdots\cdots\cdots\}$.
2. *Si* $A = \{2, 5, 7\}$ *et* $B = \{1, 5, 7, 9\}$, *on a* $A \cup B = \{1, 2, 5, 7, 9\}$.
3. *Soit* $A = \{a; b; d; e; f; g\}$, $B = \{a; d; g; i; j; k\}$ *et* $C = \{b; e; f; l; m\}$

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

Remarque **10.**

- $A \cup B = B \cup A$.
- $A \subset A \cup B$ *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* $a \notin B$.

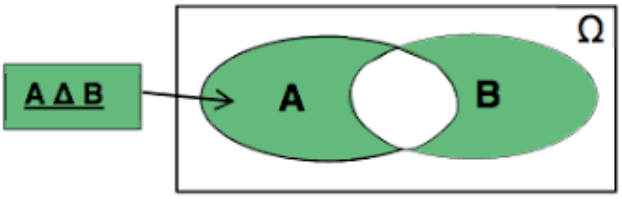
Exemple **14** (Différence de deux ensembles)**.**



Exemple **15** (Différence de deux ensembles)**.**

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

Exemple **16** (Différence symétrique)**.**



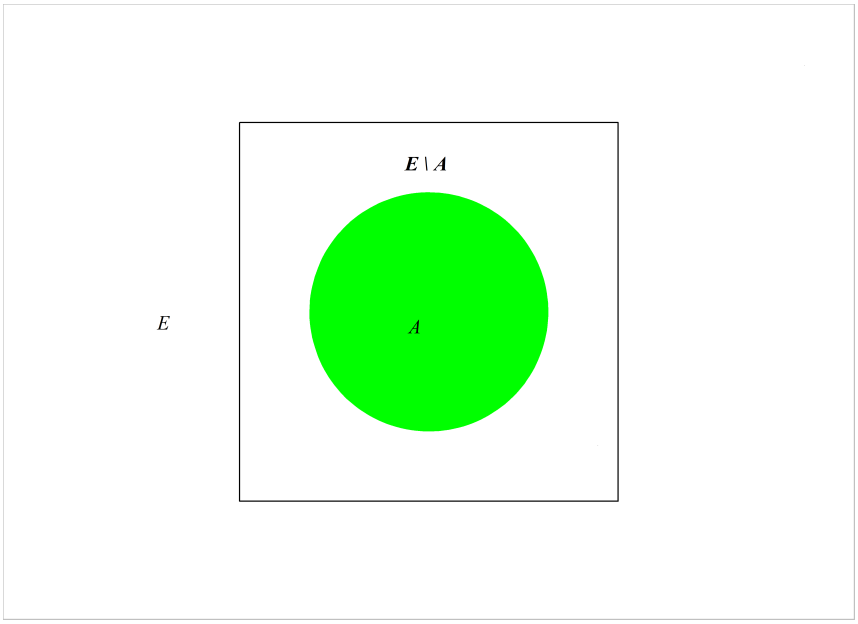
Exemple **17** (Différence symétrique)**.**

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

Remarque **11.**

- *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* $A \setminus B = \emptyset$.

Exemple **18** (Complémentaire d'un ensemble)**.**



Exemple 19 (Complémentaire d'un ensemble)**.**

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 12.
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* $C_E \emptyset = E$.

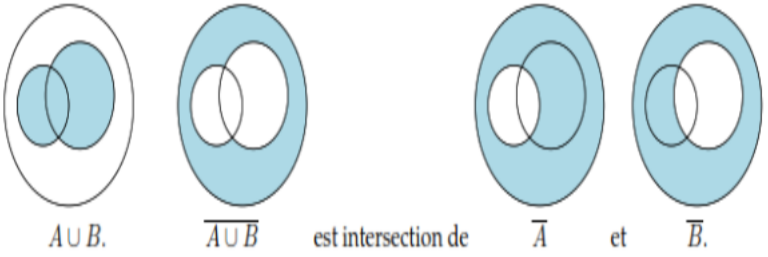
1.5.3 Propriétés des opérations élémentaires

Soit E, F et G trois ensembles et A et B deux parties de E.

Commutativité	$E \cup F = F \cup E$ $E \cap F = F \cap E$ $E \triangle F = F \triangle E$
Associativité	$E \cup (F \cup G) = (E \cup F) \cup G$ $E \cap (F \cap G) = (E \cap F) \cap G$ $E \triangle (F \triangle G) = (E \triangle F) \triangle G$
Distributivité	$E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$ $E \cup (F \cap G) = (E \cup F) \cap (E \cup G),$
Elément neutre	$E \cup \emptyset = \emptyset \cup E = E$ $E \triangle \emptyset = \emptyset \triangle E = E$
Lois de De Morgan	$C_E(A \cap B) = (C_E A) \cup (C_E B)$ $C_E(A \cup B) = (C_E A) \cap (C_E B)$
Dichotomie	$A \cup C_E A = E \; A \cap C_E A = \emptyset$ $C_E(C_E A) = A$
	$A \triangle B = (A \cup B) - (A \cap B)$

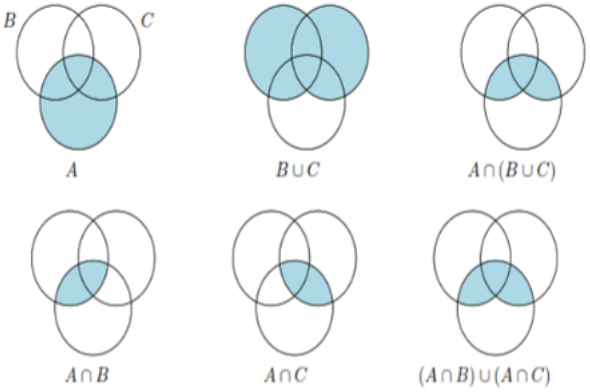
Ces règles sont faciles à comprendre si on les visualise à l'aide de diagrammes

Exemple **20.** *Illustration de* $\overline{A \cup B} = \overline{A} \cap \overline{B}$



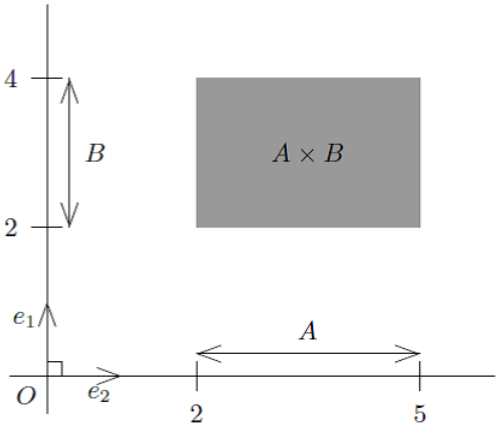
Exemple **21.**

Illustration de $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



Exemple **22** (Produit cartésien)**.**

• 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.



Exemple 23 (Produit cartésien)**.**

– *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* $A = \{daurade, poulet\}$ *et* $B = \{pomme, orange\}$*, alors*

$$\begin{aligned} A \times B &= \{(daurade, pomme), (daurade, orange), \\ &\quad (poulet, pomme), (poulet, orange)\}. \end{aligned}$$

Remarque 13.

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*

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

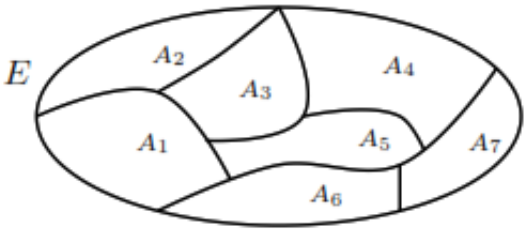
Définition 7 (Partition d'un ensemble)**.**

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 **24.**



Exemple **25.** *Si* $A \subset E$, *la paire* $\{A, C_E A\}$ *est une partition de* E.

Chapitre 2

Logique

2.1 Définitions

Définition 8.

- *Dans le cadre d'une théorie mathématique donnée, une **assertion/proposition / affirmation** est une phrase mathématique à laquelle on peut attribuer une, et une seule, valeur de vérité, à savoir V (vraie) ou F (faux).*
- *Certaines assertions sont déclarées vraies a priori : ce sont les **axiomes** ; sinon, la véracité d'une assertion doit résulter d'une démonstration.*
- *Les assertions démontrées sont appelées **théorèmes** ou **propositions** suivant leur importance.*
- *Un lemme est un résultat préalable utile à une démonstration plus conséquente. C' est une proposition intermédiaire utile à la démonstration d'une autre proposition*
- *Un **corollaire** est une assertion vraie qui découle d'un résultat précédent. C'est la conséquence d'une proposition ou d'un théorème.*
- *La **démonstration** d'une assertion est un processus respectant strictement les règles de la logique, partant des hypothèses, supposées vraies, et en aboutissant à la conclusion attendue. La démonstration permet d'établir qu'une assertion est vraie.*
- *Une conjecture est une assertion dont on pense qu'elle est vraie, mais qui n'a pas été démontrée.*

Exemple 26.

♢ *« 3 = 7 » est une assertion fausse,*

♢ *« $3 = -(-3)$ » est une assertion vraie,*

♢ *« 2 est un nombre pair » est une assertion vraie.*

♢ *Les énoncés suivants sont des propositions mathématiques.*

(a) $1 + 1 = 2$. *Cette proposition est vraie.*

(b) $1+1=3$. *Cette proposition est fausse.*

(c) $\ln(1)=1$. *Cette proposition est fausse.*

♢ *Par contre,* $1+1-2$ *et* $(\sqrt{18})^3$ *ne sont pas des propositions puisqu'on ne peut leur attribuer de valeur de vérité. Ce sont des expressions arithmétiques dont le résultat est un réel.*

2.2 Des symboles à connaître

2.2.1 Implication, réciproque et équivalence

Définition 9. *Le symbole* $\Rightarrow$ *signifie « implique ». On peut également traduire une propriété contenant ce sym- bole sous la forme « Si* $\cdots$ *Alors ».*
L'implication est le principe même du raisonnement mathématique : dans une propriété, une hypothèse entraîne une conclusion.
On dit que l'hypothèse est une de condition suffisante pour conclure, et que la conclusion est une condition nécessaire pour avoir l'hypothèse.

Exemple 27. *Considérons les propositions vraies suivantes :*

1. *Si je m'appelle Ana, alors je suis une fille. S'appeler Ana est une condition suffisante pour conclure que je suis une fille.*
2. *Si un quadrilatère est un rectangle, alors c'est un parallélogramme. Qu'un quadrilatère soit un rectangle est une condition suffisante pour conclure qu'il s'agit d'un parallélogramme.*
3. $x \geq 10 \Rightarrow 3x \geq 15$.

Définition 10. *La réciproque d'une propriété consiste à retourner la phrase en échangeant l'hypothèse et la conclu- sion, ou encore à changer le sens de la flèche.*
Une propriété et sa réciproque sont indépendantes et se démontrent séparément. En effet le fait qu'une propriété soit vraie n'implique pas que sa réciproque le soit !

Exemple 28. *Considérons les réciproques des propositions de l'exemple précédent.*

1. *Si je suis une fille, alors je m'appelle Ana : FAUX*
   Pour m'appeler Ana, il n'est pas suffisant d'être une fille.
2. *Si un quadrilatère est un parallélogramme, alors c'est un rectangle : FAUX*
   Pour qu'un quadrilatère soit un rectangle, il n'est pas suffisant qu'il soit un parallélogramme.
3. $x \geq 10 \Leftarrow 3x \geq 15$ *: FAUX*

Définition 11. *Lorsqu'une propriété et sa réciproque sont vraies, on utilise le symbole $\Leftrightarrow$, qui signifie « équivaut à ». On peut également traduire ce symbole par « Si et seulement si ». On parle d'équivalence entre l'hypothèse et la conclusion.*

Exemple 29. *1.* ABC *est un triangle rectangle en* A *si et seulement si* $BC^2 = AB^2 + AC^2$.

2. $x \geq 5 \Leftrightarrow 3x \geq 15$.

2.2.2 Les quantificateurs pour tout $\forall$ et il existe $\exists$

Définition 12 (Les quantificateurs)**.** *Ils précisent le domaine de validité d'une propriété. Au lycée, vous devez connaître les symboles $\forall$ et $\exists$, qui signifient respectivement « Pour tout » et « Il existe un », sous entendu « (au moins) ». La virgule qui suivra le symbole $\exists$ sera alors traduite par « tel que ». Il est donc essentiel de bien les comprendre pour savoir dans quels cas une propriété peut s'appliquer.*

Exemple 30. *1.* $\forall x \in \mathbb{R}, x^2 \geq 0$.

2. $\exists x \in \mathbb{R}, x^2 \geq 100$.

Remarque 14. *Lorsqu'on énonce des propositions toujours vraies en français, on sous-entend souvent les quantificateurs.*

Exemple 31.
- *Noël est en décembre (sous entendu « Tous les ans »)*
- *Un parallélogramme dont les diagonales sont de même longueur est un rectangle (sous-entendu « Tous les parallélogrammes »)*
- *Un parallélogramme peut avoir des diagonales de même longueur (sous-entendu « il existe (au moins) un tel parallélogramme »)*

Remarque 15. *Les deux quantificateurs « tout » et « il existe » sont liés lorsqu'il s'agit d'énoncer le contraire d'une proposition. En effet, le contraire de « tout » n'est pas « aucun », mais « il existe (au moins) un ».*

Exemple 32.
- *Le contraire de « Tous les ans, Noël est en décembre » est la proposition « Il existe une année (au moins) ou Noël n'est pas en décembre ».*
- *Le contraire de « Tous les rectangle sont des parallélogrammes »est la proposition « Il existe un rectangle (au moins) qui n'est pas un parallélogramme ».*

Remarque 16. *Evidemment une proposition et son contraire ne peuvent pas être toutes les deux vraies. Pour énoncer le contraire de ces propositions, on a dit qu'il existait au moins un cas où l'hypothèse émise était vérifiée, mais pas la conclusion.*

2.3 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 étudiants de l'IUA,

- P : avoir le Bac C ;
- Q : avoir moins de 20 ans ;
- R : avoir obtenu la mention bien ;
- S : avoir le Bac D.

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

2.3.1 Opérations logiques élémentaires

1) $nonP$ **(negation 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.

2.3.2 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 $x \in A$ possédant 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 propriétés P et Q.**
On dit que la propriété P est équivalente à la propriété Q et on écrit $P \Leftrightarrow Q$, si les éléments $x \in A$ possédant 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

2.4 Logique mathématique classique

Définition 13 (Assertion)**.** *Une assertion est un énoncé dont on peut affirmer sans ambiguïté s'il est vrai ou s'il est faux.*

Exemple 33. *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 34. *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 14 (Proposition)**.** *Une proposition est un énoncé qui contient des variables, qui est vrai pour certaines valeurs attribuées à ces variables.*

Exemples 1.
1. $x > 10$ *est une proposition, elle est vraie pour les nombres strictement supérieurs à 10, fausse dans tous les autres cas.*
2. *La 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 **17.** *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

Chapitre 3

Raisonnements Mathématiques

3.1 Raisonnement direct

3.1.1 Principe

Le raisonnement mathématique le plus courant est l'implication directe, aussi appelé raisonnement déductif. On veut montrer que l'assertion $\ll\ P \Rightarrow Q\ \gg$ est vraie. On suppose que P est vraie et on montre qu'alors Q est vraie.
Autrement dit, à partir d'une hypothèse (assertion que l'on suppose vraie) ou d'une proposition, on montre, par une suite de déductions (raisonnement logique), une autre proposition. Dans la suite de déductions, on peut se servir d'autres propositions vraies, que l'on a démontrées auparavant. C'est la méthode à laquelle vous êtes le plus habitué.

3.1.2 Exemples

Exemple 35. *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 rationnels sont des 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 $q' \in \mathbb{N}^*$. On a :

$$a + b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}.$$

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 36. *Montrer que* $\forall n \in \mathbb{N}$, $8\frac{n(n+1)}{2} + 1$ *est un carré.*

Démonstration. Soit $n \in \mathbb{N}$, on a $8\dfrac{n(n+1)}{2} + 1 = 4n^2 + 4n + 1 = (2n+1)^2$. □

Exemple 37. *Montrer que si $x < 1$ alors $|x - 4| > 3$.*

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

Exemple 38. *Soit A et B deux ensembles non vides. Montrons que $A \cap B \subset A$.*

Démonstration. Soit $x \in A \cap B$, montrons que $x \in A$. Par définition de l'intersection, on a $x \in A$ et $x \in B$, et en particulier, $x \in A$. □

Exemple 39. *Soient x et y deux réels non nuls. Montrer que si $\dfrac{1}{x} + \dfrac{1}{y} = 1$ alors $xy = x + y$.*

Démonstration. On suppose que $\dfrac{1}{x} + \dfrac{1}{y} = 1$. On a $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{x+y}{xy}$ d'après notre hypothèse, $\dfrac{x+y}{xy} = 1$. On en déduit que $xy = x + y$. Finalement, on a bien démontré l'implication « $\dfrac{1}{x} + \dfrac{1}{y} = 1 \Longrightarrow xy = x + y$ ». □

3.2 Raisonnement par double implication

3.2.1 Principe

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

3.2.2 Exemples

Exemple 40. *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 41. *Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction définie sur $\mathbb{R}$. Montrer que :*
" f est une fonction à la fois paire et impaire" $\Longleftrightarrow$ " f est la fonction nulle".

Démonstration. Considérons les deux propositions : P : " f est une fonction à la fois paire et impaire" et Q : "f est la fonction nulle".
• Supposons que P est vraie et montrons qu'il en est de même de Q. Comme f est paire et impaire, on a :

$$\forall x \in \mathbb{R}, \quad \begin{cases} f(-x) = f(x) \\ f(-x) = -f(x) \end{cases}$$

On obtient donc : $\forall x \in \mathbb{R}$, $f(x) = -f(x)$, soit : $\forall x \in \mathbb{R}$, $2f(x) = 0$ qui s'ecrit aussi $\forall x \in \mathbb{R}$, $f(x) = 0$. Ce qui prouve bien que f est la fonction nulle.
• La reciproque est triviale. Supposons que Q est vraie. Alors : $\forall x \in \mathbb{R}$, $f(x) = 0$ et clairement :

$$\forall x \in \mathbb{R},\ -x \in \mathbb{R},\ et\ f(x) = f(-x) = -f(x).$$

Ce qui prouve que f est a la fois paire et impaire et donc Q est vraie. □

Exemple 42. *Prouver que « $\forall n \in \mathbb{N}$; n^2 impair $\Longleftrightarrow$ n impair ».*

Démonstration. Soit $n \in \mathbb{N}$.
Supposons que n^2 est impair.

$$\begin{aligned} n^2\ impair &\Longrightarrow \exists k \in \mathbb{N} \text{ tel que } n^2 = 2k + 1 \\ &\Longrightarrow n^2 - 1 = 2k \\ &\Longrightarrow (n-1)(n+1) = 2k \\ &\Longrightarrow n+1 \text{ est pair ou } n-1 \text{ est pair} \\ &\Longrightarrow n \text{ est impair.} \end{aligned}$$

Supposons que n est impair.

$$\begin{aligned} n\ impair &\Longrightarrow \exists k \in \mathbb{N} \text{ tel que } n = 2k + 1 \\ &\Longrightarrow n^2 = (2k+1)^2 \\ &\Longrightarrow n^2 = 4k^2 + 4k + 1 \\ &\Longrightarrow n^2 = 2(2k^2 + 2k) + 1 \\ &\Longrightarrow n^2 \text{ est impair.} \end{aligned}$$

□

3.3 Raisonnement par disjonction de cas ou Raisonnement cas par cas

3.3.1 Principe

Si l'on souhaite vérifier une assertion $P(x)$ pour tous les x dans un ensemble E, on montre l'assertion pour les x dans une partie A de E, puis pour les x n'appartenant pas à A. C'est la méthode de disjonction ou du cas par cas.

3.3.2 Exemples

Exemple 43. *Deux nombres entiers naturels distincts de 0 et de 1 ont pour somme 11. Prouver que lorsqu'on multiplie chacun d'eux par 9, on obtient alors deux nombres formés des mêmes chiffres.*

Preuve. Nous avons les cas suivants :

Cas 1	2+9=11	$2 \times 9 = 18$	$9 \times 9 = 81$
Cas 2	3+8=11	$3 \times 9 = 27$	$9 \times 8 = 72$
Cas 3	4+7=11	$4 \times 9 = 36$	$9 \times 7 = 63$
Cas 4	5+6=11	$5 \times 9 = 45$	$9 \times 6 = 54$

□

Exemple 44. *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 : $x \geq 1$. 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 45. *montrer que, pour tout $n \in \mathbb{N}$, $\dfrac{n(n+1)}{2}$ est un entier naturel.*

Démonstration. Soit $n \in \mathbb{N}$. On va démontrer que $\dfrac{n(n+1)}{2}$ est un entier naturel en distinguant les cas n pair ou impair.

• Si n est pair, on peut écrire $n = 2k$, où $k \in \mathbb{N}$. Alors

$$\frac{n(n+1)}{2} = \frac{2k(2k+1)}{2} = k(2k+1) \in \mathbb{N}.$$

• Si n est impair, on peut écrire $n = 2p+1$, où $p \in \mathbb{N}$. Alors

$$\frac{n(n+1)}{2} = \frac{(2p+1)(2p+2)}{2} = (2p+1)(p+1) \in \mathbb{N}.$$

Finalement, pour tout entier naturel n, $\dfrac{n(n+1)}{2}$ est un entier naturel. □

Exemple 46. *Démontrer que* $n(2n+1)(7n+1)$ *est divisible par* 2 *et* 3.

Démonstration.

$J = n(2n+1)(7n+1)$ divisible par 2.

Pour $n = 2k$	$J = 2k(4k+1)(14k+1) = 2(k(4k+1)(14k+1))$
Pour $n = 2k+1$	$J = (2k+1)(4k+3)(14k+8) = 2(2k+1)(4k+3)(7k+4)$

$J = n(2n+1)(7n+1)$ divisible de 3.

Pour $n = 3k$	$J = 3k(6k+1)(21k+1) = 3(k(6k+1)(21k+1))$
Pour $n = 3k+1$	$J = (3k+1)(6k+3)(21k+8) = 3(3k+1)(2k+1)(21k+8)$
Pour $n = 3k+2$	$J = (3k+2)(6k+5)(21k+15) = 3(3k+2)(6k+5)(7k+5)$

□

3.4 Raisonnement par élimination des cas

3.4.1 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 ≫.

3.4.2 Exemples

Exemple 47. *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 $(x;y) = (1;1)$. □

3.5 Raisonnement par contraposée

3.5.1 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.

3.5.2 Exemples

Exemple 48. *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 49. *Soient x et y deux reels. Montrer que*

$$xy \neq 0 \Longrightarrow x \neq 0 \; et \; y \neq 0.$$

Démonstration. La contraposee de $xy \neq 0 \Longrightarrow x \neq 0 \; et \; y \neq 0$ est

$$si \; x = 0 \; ou \; y = 0, \; alors \; xy = 0.$$

Montrons donc cette assertion. Si nous choisissons $x = 0$ ou $y = 0$, alors le produit xy est nécessairement nul. Nous en déduisons donc le résultat cherché. □

Exemple 50. *Montrer que si x et y sont des réels distincts de 1, et si $x \neq y$, alors $\dfrac{1}{x-1} \neq \dfrac{1}{y-1}$.*

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

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

□

Exemple **51.** *Montrer l'implication à* "$x \notin \mathbb{Q}$" $\Longrightarrow$ "$1+x \notin \mathbb{Q}$".

Démonstration. Nous allons de nouveau utiliser la contraposée en démontrant l'implication "$1 + x \in \mathbb{Q}$" $\Longrightarrow$ "$x \in \mathbb{Q}$". Soit x un réel tel que $1 + x \in \mathbb{Q}$. On peut écrire $x = (1+x) - 1$. Or $1+x$ est un nombre rationnel (hypothèse), et 1 aussi. Par conséquent, $(1 + x) - 1$ est un nombre rationnel, ce qui montre que $x \in \mathbb{Q}$. Par contraposition, on a démontré l'implication "$x \notin \mathbb{Q}$" $\Longrightarrow$ "$1 + x \notin \mathbb{Q}$". □

Remarque **18.** *"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* $\ll A \Rightarrow B \gg$ *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".*

3.6 Raisonnement par l'absurde

3.6.1 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.

3.6.2 Exemples

Exemple **52.** *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 **53.** *Soient* $a, b \geq 0$. *Montrer que si* $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ *alors* $a = b$.

Démonstration. Nous raisonnons par l'absurde en supposant que $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ et $a \neq b$.
Comme $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ 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 **54.** *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 **55.** *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 élevant au carré : On a $a + b = a + b + 2\sqrt{a} \times \sqrt{b}$ soit $\sqrt{a} \times \sqrt{b} = 0$ 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'énoncé, d'où $\sqrt{a+b} \neq \sqrt{a} + \sqrt{b}$. □

Exemple **56.** *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 **19.** *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.*

3.7 Raisonnement par contre-exemple

3.7.1 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 $P(x)$.

3.7.2 Exemples

Exemple 57. *Montrons que l'assertion* $(\forall x \in \mathbb{R},\ x \geq 0)$ *est fausse.*

Démonstration. $-10 \in \mathbb{R}$ et $-10 < 0$, donc l'assertion $(\forall x \in \mathbb{R},\ x \geq 0)$ est fausse. □

Exemple 58. *Montrer que l'assertion suivante est fausse « Tout entier positif est somme de trois carrés ». (Les carrés sont les* $0^2, 1^2, 2^2, 3^2, \ldots$ *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 obtenir 7. □

Exemple 59. *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 60. *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 61. *Soit* $f(x) = x^3 + x^2$*. Montrer que* f *n'est ni paire ni impaire.*

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

3.8 Raisonnement par récurrence

3.8.1 Principe de la récurrence classique

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, le principe de récurrence permet de montrer qu'une assertion $P(n)$,

dépendant de n, est vraie pour tout entier $n \geq n_0$ avec $n_0 \in \mathbb{N}$. La démonstration par récurrence se déroule en trois étapes :

• **Etape d'initialisation.** Nous verifions que $P(n_0)$ est vraie.

• **Etape d'hérédité.** Fixons un entier naturel $n \geq n_0$, puis montrons que si $P(n)$ est vraie alors $P(n+1)$ est vraie.

• **Etape de conclusion.** Nous concluons que l'assertion $P(n)$ est vraie $\forall n \geq n_0$.

3.8.2 Exemples

Exemple 62. *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 63. *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 $n \geq 0$, c'est-à-dire pour tout entier naturel n, l'entier $n^3 - n$ est divisible par 3. □

Exemple 64. *Montrer par récurrence que, pour tout $n \geq 1$, $n(2n+1)(7n+1)$ est divisible par 6.*

Exemple 65. *Les fonctions de couts sous-additives On note C(x) le coat de production d'une quantile x d'un certain bien par une firme. La fonction C, definie de $\mathbb{R}$, dans $\mathbb{R}_+$, est appelée fonction de coût. Supposons qu'il soit toujours moins coilteux de produire une*

quantité totale de bien avec une seule firme qu'avec deux.
Dans ce cas, on a $C(x_1 + x_2) \leq C(x_1) + C(x_2)$ *pourtout* $x_1, x_2 \geq 0$. *On dit que la fonction de coût est sous-additive. Montrons par recurrence que :*

$$\forall n \geq 2, \quad C(x_1 + \cdots + x_n) \leq C(x_1) + \cdots + C(x_n) \quad \textit{pour tout } x_1, x_2, \cdots, x_n \geq 0.$$

Aurremenr dit, montrons que quel qne soit le nomhre n *de firmes, i1 est moins coûteux de produire avec une seule firme qu' avec* n *firmes.*
C'est vrai pour $n = 2$ *puisque la fonction* C *est supposee sous-additive. Supposons que la propriété est vraie pour* n *firmes, et montronsqu'elle est vraie pour* $n + 1$ *firmes.*
Pour tout $x_1, \cdots, x_n, x_{n+1} \geq 0$,*on a :*

$$C(x_1 + \cdots + x_n + x_{n+1}) = C((x_1 + \cdots + x_n) + x_{n+1}) \leq C(x_1 + \cdots + x_n) + C(x_{n+1}).$$

d'après la sous-additivite et

$$C(x_1 + \cdots + x_n) \leq C(x_1) + \cdots + C(x_n)$$

d'après I'hypothèse de récurrence au rang n.
Donc :

$$C(x_1 + \cdots + x_n + x_{n+1}) \leq C(x_1) + \cdots + C(x_n) + C(x_{n+1}).$$

Ce qui signifie que la propriété est vraie pour $n + 1$ *firmes.*
La propriété est vraie pour 2 firmes, et on a montré que si elle est vraie pour n *firmes, alors elle sera vraie aussi pour* $n + 1$ *firmes, donc on peut dire qu'elle est vraie pour n'importe quel nombre* n *de firmes, avec* $n \geq 2$.
On a donc démontré que si la fonction de coût est sous-additive, il est moins coûteux de produire avec une seule firme qu'avec n *firmes (quel que soit* n*).*

Remarque 20.
Pour démontrer un résultat par un raisonnement par récurrence, il faut tout d'abord énoncer proprement l'hypothèse de récurrence $P(n)$*, démontrer l'initialisation, c'est-à-dire que* $P(n_0)$ *est vraie, et ensuite prouver l'hérédité* $(P(n) \Longrightarrow P(n+1))$ *pour* $n \geq n_0$. *On conclut alors en appliquant le principe de récurrence.*

3.8.3 Principe de la récurrence forte

Soit $P(n)$ une propriete dependant d'un entier n. Si
• **Etape d'initialisation.** $P(n)$ est vrai pour un certain entier n_0,
• **Etape d'hérédité.** $P(n_0)$, $P(n_0 + 1), \cdots, P(n) \Rightarrow P(n + 1)$ est vrai pour tout entier $n \geq n_0$,
alors $P(n)$ est vraie pour tout entier $n \geq n_0$.

3.8.4 Exemples

Exemple 66. *Soit (u_n) la suite definie par $u_0 = u_1 = 4$ et pour tout $n \in \mathbb{N}$: $u_{n+2} = \frac{5}{2}u_{n+1} - \frac{3}{2}u_n$. Demontrer par recurrence que pour tout entier naturel n, $u_n = 4$.*

Démonstration. 1. Par hypothese $u_0 = 4$.

2. Supposons que pour un entier quelconque fixe $n \geq 1$, $u_k = 4$ pour tout entier k tel que $O \leq k \leq n$. Alors : $u_{n+1} = \frac{5}{2}u_n - \frac{3}{2}u_{n-1} = \frac{5}{2} \times 4 - \frac{3}{2} \times 4 = 4$.
Donc pour tout $n \in \mathbb{N}$, $u_n = 4$.

□

3.9 Raisonnement par analyse-synthèse

3.9.1 Principe

Le raisonnement par analyse-synthèse est presque toujours utilisé lorsqu'on doit résoudre un problème qui se ramène à :

"Trouver tous les objets x de l'ensemble E vérifiant une propriété P donnée".

Il se déroule en deux temps :

- **Analyse :** On "prend" un objet x de l'ensemble E vérifiant la propriété P, et on essaie par déductions de réduire au maximum le domaine des objets x possibles. On obtient finalement un certain ensemble (qui doit être le plus petit possible) de "candidats" x solutions du problème.
- **Synthèse :** On "teste", parmi les candidats x restant après la phase d'analyse a), lesquels (il peut y en avoir aucun, un, plusieurs ou une infinité) vérifient effectivement la propriété P. Ceux qui restent constituent l'ensemble des solutions du problème posé.

3.9.2 Exemples

Exemple 67. *Déterminer les réels tels que $\sqrt{1-x} = x$.*

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

du second degré donne $x_1 = \dfrac{-1-\sqrt{5}}{2}$ et $x_2 = \dfrac{-1+\sqrt{5}}{2}$. Seul x_2 est dans l'intervalle souhaité. Donc la seule solution possible est $\dfrac{-1+\sqrt{5}}{2}$.

Synthèse : Prouvons que $\dfrac{-1+\sqrt{5}}{2}$ est solution de l'équation. On sait que $1-x=x^2$. Prenons la racine carrée de cette inégalité. Alors :

$$x = \sqrt{x^2} = \sqrt{1-x}.$$

(tout est légitime ici car $x \in [0;1]$). Conclusion : la seule solution de l'équation est $\dfrac{-1+\sqrt{5}}{2}$. □

Exemple **68.** *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 :

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

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

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 4

Relations binaires dans un ensemble

4.1 Définitions et exemples

Définition **15.** *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 **21.** *La relation binaire « vide » correspond au sous-ensemble $\emptyset$ de $E \times F$.*

Exemples **2.**

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 definit 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 définit par*

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

4. *Ordre strict sur les entiers : $(0, 1)$ est noté $0 < 1$.*

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 **69.** *On a par rapport aux relations* 1 *et* 2 *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* $* \not\mathcal{R}\diamondsuit$.

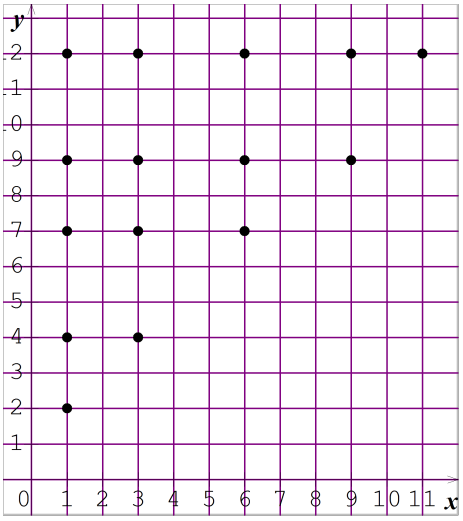
Remarque **22.** *Une relation binaire* $\mathcal{R}$ *sur un ensemble* E *est définie lorsqu'on sait quand un point x de cet ensemble et en relation avec un point y de l'ensemble.*

4.2 Mode de représentation

4.2.1 Diagramme cartésien

Définition **16.** *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 **70.** *Soit* $A = \{1, 3, 6, 9, 11\}$, $B = \{2, 4, 7, 9, 12\}$ *et la relation "est plus petit que", le graphique cartésien est :*



4.2.2 Matrice binaire

Définition **17.** *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 **71.** *Soit $E = \{e_1, e_2, e_3\}$, $B = \{f_1, f_2, f_3, f_4\}$ et la relation*

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

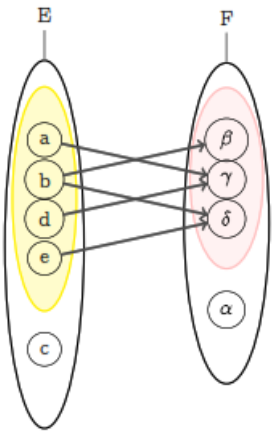
La représentation matricielle de $\mathcal{R}$ est :

	f_1	f_2	f_3	f_4
e_1	0	1	0	0
e_2	0	1	1	1
e_3	1	0	0	1

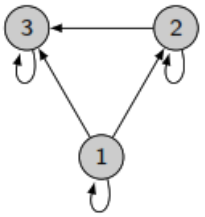
4.2.3 Diagramme sagittal

Définition **18.** *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 **72.** *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 **73.** *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*



4.3 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-symetrique 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.** *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 :*

$$x\mathcal{R}_1 y \; si \; x \geq y; \quad x\mathcal{R}_2 y \; si \; x = y; \quad x\mathcal{R}_3 y \; si \; x = 2y + 5;$$

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

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.*

4.4 Relation d'ordre

4.4.1 Dénitions et exemples

Définition **19.** *Une relation binaire $\mathcal{R}$ sur un ensemble non vide E est dite relation d'ordre si $\mathcal{R}$ est à la fois* ***réflexive***, ***anti-symétrique*** *et* ***transitive***.

Exemples **4.** *1)* $(\mathbb{R}, \leq)$ *usuel*

2) L'ensemble des mots ecrits avec l'alphabet français muni de l'ordre lexicographique.

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

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

c'est l'ordre cartésien.

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

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

Définition **20** (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 **74.** *Les exemples 1) et 2) sont des relations d'ordre total.*

4.4.2 Eléments singuliers dans un ensemble ordonné

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

Définition **21** (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 **23.** *Les majorants et minorants n'existent pas toujours, s'ils existent ils ne sont pas uniques.*

Définition 22 (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 24. *Les éléments maximums et minimums n'existent pas toujours, s'ils existent ils sont uniques.*

Exemples 5. *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 23 (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 24 (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 25. *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 **6.** *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 minimaux.*
   Dans $\mathcal{P}(E)\backslash\{\emptyset; E\}$ (ensembles des parties propres de E) il y a des éléments minimaux $\{x\}$ et des éléments maximaux $E - \{x\}$.

4.5 Relation d'équivalence

4.5.1 Dénitions et exemples

Définition **25.** *Une relation binaire $\mathcal{R}$ est une relation d'equivalence si elle est à la fois **réflexive**, **symétrique** et **transitive**.*

Exemple **75.** *Voici des exemples basiques.*

1. *La relation $\mathcal{R}$ « être parallèle » est une relation d'équivalence pour l'ensemble E des droites affines du plan :*
   - *réflexivité : une droite est parallèle à elle-même,*
   - *symétrie : si D est parallèle à D' alors D' est parallèle à D,*
   - *transitivité : si D parallèle à D' et D' parallèle à D'' alors D est parallèle à D''.*
2. *La relation « être du même âge » est une relation d'équivalence.*
3. *La relation « être perpendiculaire » n'est pas une relation d'équivalence (ni la réflexivité, ni la transitivité ne sont vérifiées).*
4. *La relation $\leq$ (sur $E = \mathbb{R}$ par exemple) n'est pas une relation d'équivalence (la symétrie n'est pas vérifiée).*

Exemples **7.**

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.*

4.5.2 Classes d'équivalence

Définition **26.** *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 **76.** *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 **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.*

Chapitre 5

Applications d'un ensemble vers un autre

5.1 Relations d'un ensemble vers un autre

5.1.1 Définitions

Définition 27. *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.

5.1.2 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 $E \xrightarrow{f} F$.

5.1.3 Exemple

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.

5.2 Applications

5.2.1 Définitions

Définition 28. *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 29. *Soit $f : A \to B$ une application.*

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

Remarque 26.

1. *Si $A' \subset A$, alors f induit une application naturelle $f' : A' \to B$ déflnie 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 déflnit pas nécessaire une application de A dans B'.*

5.2.2 Exemples et contre-exemples

1. Les applications constantes
2. L'application identité de A notée 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 $A = \{1, 2, 3, 4, 5, 7\}$ 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.

5.2.3 Egalité de deux applications

Définition 30. *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 **77.** *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 égales.*

Définition **31** (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 écrit une suite d'éléments d'un ensemble* E *sous la forme* $(u_n)_{n\in D}$*.*

5.2.4 Fonctions caractéristiques

Définition **32.** *Soient* E *un ensemble non vide et* A *une partie de* E*. On appelle fonction caractéristique (ou indicatrice) de* A *l'application notée* χ_A *définie comme suit :*

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

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

Propriété 1 (propriétés remarquables des fonctions caractéristiques)**.**

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. $\chi_{\overline{A}} = 1 - \chi_A$.

5.2.5 Image directe, Image réciproque

Définition **33.** *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 appelé* ***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 départ E *est appelée image de* f*, on la note* $\operatorname{Im} f$*.*

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

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

Remarque **27.** 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 **78.** *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 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* $(F_i)_{i\in I}$ *est une famille de parties de* F, *alors* $f^{-1}(\bigcup_{i\in I} F_i) = \bigcup_{i\in I} f^{-1}(F_i)$.
9. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. *Plus généralement, si* $(F_i)_{i\in I}$ *est une famille de parties de* F, *alors* $f^{-1}(\bigcap_{i\in I} F_i) = \bigcap_{i\in I} f^{-1}(F_i)$.

5.2.6 Composition des applications

Définition **34.** *Soient* $f : E \to F$ *et* $g : N \to M$ *deux applications. Si* $F \subset N$, *alors on peut définir une nouvelle application* $h : E \to M$ *par :* $x \mapsto g(f(x))$. h *est appelé la composée de* g *par* f *et est noté* $g \circ f$.
Notons que par définition on a pour tout $x \in E$, $(g \circ f)(x) = g(f(x))$.

Propriété 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 **8.** $s : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ *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 **28.** *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* $(f \circ g)(a) = a$.

5.2.7 Applications injectives, surjectives, bijectives

a) Définitions et remarques

Définition **35.** *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 signifie qu'il existe dans F un élément qui a moins deux antécédents.

Remarque **29.** *Si les ensembles E et F sont finis 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 fini non vide est non injective.

Définition **36.** *f est dite **surjective**, si tout élément de F a au moins un antécédent dans E par f.*

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

Remarque **30.** *Si les ensembles E et F sont finis et $f : E \to F$ est surjective, alors nécessairement $card(E) \geq card(F)$.*

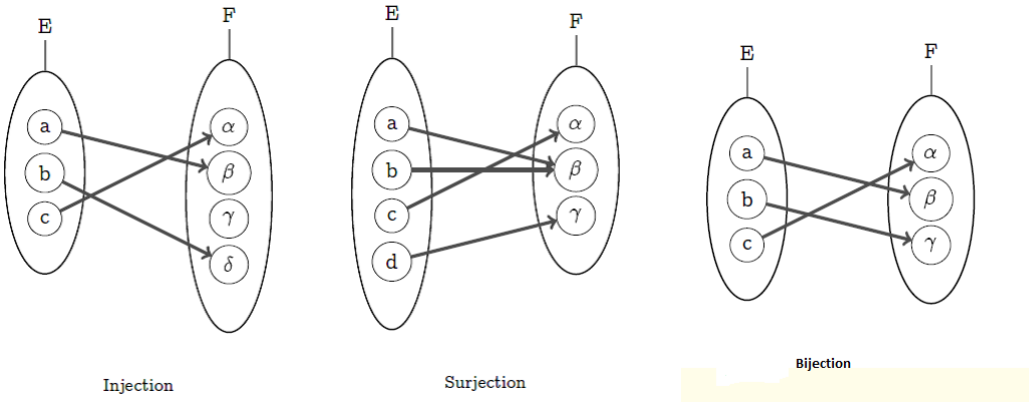
Définition **37.** *f est dite **bijective**, si f est à la fois injective et surjective , ou encore si tout élément de F a un antécédent et un seul dans E par f.*

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

Exemple **79.**

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 80.



b) Bijection réciproque d'une application bijective

Définition 38. *Soit $f : E \to F$ une application bijective. Alors on peut définir 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 réciproque de f et on la note f^{-1}.

Proposition 2. *Si $f : E \to F$ est une bijection, alors $f^{-1} \circ f = id_E$ et $f \circ f^{-1} = id_F$.*

Proposition 3. *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 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 9.

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

Exemples 10.

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 égale a sa propre bijection réciproque.*
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. $\sin : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ *est une bijection et* $\sin^{-1} = \arcsin$.

5.2.8 Ensembles dénombrables

Définition **39.** *Deux ensembles non vides E et F sont dits équipotents s'il existe une application $f : E \to F$ bijective.*
Un ensemble non vide E est dit dénombrable, si E est équipotent à $\mathbb{N}$ ou à une partie de $\mathbb{N}$.

Exemples **11.** 1. *Tout ensemble fini est dénombrable.*
2. $\mathbb{N}$ *et* $\mathbb{Z}$ *sont dénombrables.*

Propriété 4.

1. *Toute partie non vide d'un ensemble dénombrable est encore dénombrable.*
2. *La réunion finie d'ensembles dénombrables est dénombrable.*
3. *Le produit cartésien de deux ensembles dénombrables est dénombrable. En particulier $\mathbb{Q}$ est dénombrable.*

Chapitre 6

Lois de composition internes et externes

6.1 Lois de composition internes (LCI)

6.1.1 Définitions et exemples

Définition **40.** *Soit E un ensemble 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 **2.** *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 **31.** *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 **12.**

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.*

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

Définition **41.** *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 **13.** *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 **42.** *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 **81.** *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 $\mathbb{R}$.*

6.1.3 Loi associative

Définition **43.** *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 **14.** *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 $\mathcal{P}(E)$.

6.1.4 Lois commutatives

Définition **44.** *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 **45.** *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 **15.** – *$+$, $\times$ 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 **82.** *La composition des applications " $\circ$ " n'est pas commutative.*

Remarque **32.** *Tout élément $x \in E$ permute avec lui même. Si " $*$ " est associative, tout x permute avec x^n, $(n \in \mathbb{N}^*)$.*

Définition **46.** *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.*

6.1.5 Elément neutre à gauche, élément neutre à droite, élément neutre

Définition **47.** *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 **33.** *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 **83.** *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 **84.** *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 **85.** *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 **4.** *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 $e_1 = e_2$.

Remarque **34.** *Un magma associatif ou semi-groupe admettant un élément neutre s'appelle **monoïde**.*

6.1.6 Elément symétrique à gauche, à droite, élément symétrique

Définition 48. *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. *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 16.
- *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 3. *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 6. *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 2. *Si x admet un symétrique, alors pour tout $n \in \mathbb{N}^*$, x^n admet $(x^{-1})^n$ pour symétrique :*

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

6.1.7 Distributivité

Définition 49. *Soient E un ensemble, $*$ et $\top$ deux lois de composition internes sur E.*

1. *On dit que la loi T est **distributive à gauche** par rapport à la loi $*$ si et seulement si :*
$$\forall (x,y,z) \in E^3, \quad x\top(y*z) = (x\top y)*(x\top z),$$
2. *On dit que la loi T est **distributive à droite** par rapport à la loi $*$ si et seulement si :*
$$\forall (x,y,z) \in E^3, \quad (x*y)\top z = (x\top z)*(y\top z),$$
3. *On dit que la loi $\top$ est **distributive** par rapport à la loi $*$ si et seulement si $\top$ est **distributive à gauche et à droite** par rapport à la loi $*$. C'est-à-dire*
$$\forall (x,y,z) \in E^3, \quad x\top(y*z) = (x\top y)*(x\top z) \quad et \quad (y*z)\top x = (y\top x)*(z\top x).$$

Remarque 35. *Notons que les distributivités à gauche et à droite de $\top$ par rapport à $*$ sont équivalentes dans le cas où $\top$ est commutative.*

Exemple 86. *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

6.2 Lois de composition externes (LCE)

6.2.1 Définitions et exemples

Définition 50. *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 87. *Une application $g : \mathbb{N}^* \times E \to E\,;\ (n,e) \mapsto ne$ est le model de lois externes le plus connu.*

Exemple 88. *Soit E un ensemble muni d'une loi de composition interne $\top$. En posant $n\bot x = \overset{n}{\top} x$, 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 $\mathbb{Z}$.*

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

Définition 51. *Soit E un ensemble muni d'une loi de composition externe $\bot$ à opérateurs dans X. Soit F une partie de E. On dit que F est stable par $\bot$ si :*
$$\forall a \in X, \qquad \forall x \in F, \qquad a\bot x \in F.$$

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

6.2.3 Distributivité

Définition **52.** *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 **89.** *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

Chapitre 7

Structures algébriques

7.1 Groupes

7.1.1 Définitions et exemples

Définition **53.** *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 **17.**

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 $S(E) = \{f \to \mathbb{A}(E) / \quad f \text{ bijective}\}$. $S(E)$ 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* +.

7.1.2 Sous-groupes d'un groupe

a) Définitions et Exemples

Définition 54. *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 7. *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) $\forall x, y \in H, \quad x.y^{-1} \in H$.

Exemples 18.
- 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 **36.** *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 **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 $H = a\mathbb{Z}$.

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

Lemme **2.** *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 $\bigcap_{i\in I} H_i$, $I \subset \mathbb{N}$, est un sous groupe de $(G, *)$.

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

c) 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 $\mathbb{Z}$.

7.2 Anneaux

7.2.1 Définition et exemples

Définition **55.** *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 A 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 ;*

(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 4.
- *L'élément neutre de + dans 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 19.
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 $\mathbb{Z}^2$, $\mathbb{Z}^3$, $\mathbb{Z}^4$, $\mathbb{C}^2$, ... sont des anneaux.

7.2.2 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 "$\cdot$ ") 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 3. *Soit $a \in A$. Calculer $(1_A + a)^5$*

Définition **56.** *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 **90.** *Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément $\overline{3}$ est un diviseur de $\overline{0}$.*

Exercice 4. *Déterminer tous les diviseurs de $\overline{0}$ de l'anneau $\mathbb{Z}/24\mathbb{Z}$.*

Définition **57.** *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 **91.** *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.

7.2.3 Sous-anneaux, Idéaux

a) Sous-anneaux

Définition **58.** *Soient A un anneau et B une partie non vide de A. On dit que B est un sous-anneau de A si :*

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

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

Exemple **92.**
- $\mathbb{Z}$ *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 **37.** *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

$$\mathbb{Z}.1_A = \{n.1_A;\ n \in \mathbb{Z}\}.$$

Définition **59.** *Soient A un anneau commutatif unitaire et B une partie non vide 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* $\forall b, b' \in B$, $bb' \in B$.

Théorème **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 $(Aut(A), \circ)$.*

7.3 Corps

7.3.1 Définitions-exemples

Définition **60.** *On dit qu'un ensemble $\mathbb{K}$ muni de deux lois "+" et " $\times$ " 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 **38.** *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 **39.**
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 **20.** *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 **93.** *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.*

7.3.2 Sous-corps

Définition **61.** *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 **94.** *(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 **8.** *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) $\forall x \in K\backslash\{0\}$, $x^{-1} \in K\backslash\{0\}$.

Remarque **40.** *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] **A. Soyeur, F. Capaces, E. Vieillard-Baron** : *Cours de Mathématiques Sup MPSI PCSI PTSI TSI* . sesamath.net (2011).

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

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

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

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

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