**Université Ibn Tofail**
**Faculté des Sciences**
**Département de Mathématiques**
**Kénitra**

**Filière SMA S1**

# Polycopié du cours d'Algèbre de Base

Auteur : Pr. Rachid ECHARGHAOUI

# Table des matières

# Chapitre 1

# Raisonnement et vocabulaire ensembliste

**Définition 1.1.**
*Une proposition (ou une assertion) est un énoncé mathématique qui a une et une seule valeur :* ***vrai*** *ou* ***faux****.*

**Exemple 1.1.**

- *"4 est un nombre impair" est une proposition* ***fausse****.*
- *"$3 \times 2 = 6$" est une proposition* ***vraie****.*
- *"Pour tout $x \in \mathbb{R}$ on a $x^2 \geq 0$" est une proposition* ***vraie****.*
- *Par contre*
$$1 + 1 - 2 \text{ et } (\sqrt{18})^3$$
*ne sont pas des proposition puisqu'on ne peut pas confirmer s'ils sont vraies ou fausses, se sont des expressions mathématiques dont le resultat est un réel.*
*Le mot proposition est clair : On propose quelque chose, mais cela reste à justifier et à demontrer.*

## 1.1 Connecteurs logiques

Les connecteurs logiques suivant permettent de combiner deux propositions pour former une nouvelle proposition.

**La conjonction**

Soit P et Q deux propositions mathématiques. La nouvelle proposition "P et Q" est vraie quand P et Q sont simultanément vraies et fausse sinon. Autrement dit :
la proposition "P et Q" est fausse si au moins l'une des deux est fausse.
On le note aussi
$$<< P \wedge Q >>$$

**Exemple 1.2.**

- *"$x + 2 \geq 4$" pour tout "$x \geq 2$" et "$1 + 1 = 3$", or la proposition "1+1=3" est fausse donc cette proposition est* ***fausse****.*
- *"$x + 2 \geq 4$" pour tout "$x \geq 2$" et "$1 + 1 = 2$". Cette proposition est* ***vraie****.*

- *"$x+2 \geq 4$" pour tout "$x \geq 1$" et "$1+1=3$". Les deux proposition sont fausses donc cette proposition est* ***fausse****.*

**La disjonction**

Soit P et Q deux propositions mathématiques, la proposition "P ou Q" est fausse si les deux propositions P et Q sont simultanément fausses et vraie sinon. Autrement dit :
la proposition "P ou Q" est vraie si au moins l'une des deux propositions P ou Q est vraie.

**Exemple 1.3.**

- *($x+2 \geq 4$ pour tout $x \geq 2$) ou ($1+1=3$). Cette proposition est* ***vraie****.*
- *($x+2 \leq 2$ pour tout $x \geq 2$) ou ($1+1=3$). Cette proposition est* ***vraie****.*
- *($x+2 \leq 2$ pour tout $x \geq 2$) ou ($1+1=3$). Cette proposition est bien* ***fausse****.*

**La négation**

Soit P une proposition mathématique. La nouvelle proposition "non P" (ou parfois $\neg P$) est vraie lorsque P et fausse, et fausse lorsque P est vraie.

**Exemple 1.4.**

- *($\overline{x \text{ est pair}}$) est (x est impair).*
- *La négation de $<< \exists x \in \mathbb{E}; P(x) >>$ est $<< \exists x \in \mathbb{E}$ non $P(x) >>$.*
- *non ($\mid x \mid < 1$) est :*

$$(x \leq -1 \text{ ou } x \geq 1)$$

*Les valeurs de verité de ces nouvelles propositions verifiant le tableau suivant :*

| $P$ | $Q$ | $P$ et $Q$ | $P$ ou $Q$ | Non $Q$ |
|---|---|---|---|---|
| $V$ | $V$ | $V$ | $V$ | $F$ |
| $F$ | $F$ | $F$ | $F$ | $V$ |
| $F$ | $V$ | $F$ | $V$ | $V$ |
| $V$ | $F$ | $F$ | $V$ | $F$ |

**L'implication**

Soit $P$ et $Q$ deux propositions mathématiques. On note $P \Rightarrow Q$ la proposition $P \Rightarrow Q$ est vraie si $Q$ est vrai a chaque fois que $P$ est vraie.
L'implication $P \Rightarrow Q$ se lit en francais $P$ implique $Q$, l'implication $Q \Rightarrow Q$ s'appelle la reciproque de l'implication $P \Rightarrow Q$. Non $(P \Rightarrow Q)$ est "$P$ et non $Q$"

**Exemple 1.5.**

- *$x \in \mathbb{R}$ , $x^2 = 4 \Rightarrow x = 2$ est* ***fausse****.*
- *$x = \pi \Rightarrow e^{ix} = -1$ est* ***vraie****.*

**L'équivalence :**

Soit $P$ et $Q$ deux propositions mathématique, on note $P \Leftrightarrow Q$ la proposition qui est vraie si $P \Rightarrow Q$ et $Q \Rightarrow P$ on dit que $P$ est équivalent a $Q$.

**Exemple 1.6.**

- $x \in \mathbb{R}$ ; $x^2 = 4 \Leftrightarrow x = 2$ *ou* $x = -2$ *est* ***vraie***.
- $x = \pi \Leftrightarrow e^{ix} = -1$ *est* ***fausse***.

## 1.2 Quantificateurs universels

### 1.2.1 Le quantificateur "$\forall$"

**Définition 1.2.**
*Le quautifacteur universel "$\forall$" se lit «parout» ou «quelque soit».*
*L'assertion $\forall x \in \mathbb{E}$ ; P(x) est vraie lorsque les assertions P(x) est vraie pour tout les éléments de l'ensemble E.*

**Exemple 1.7.**

- $\forall x \in [1; +\infty[$ , $(x^2 \geq 1)$ *est* ***vraie***.
- $\forall x \in \mathbb{R}$ $(x^2 \geq 1)$ *est* ***fausse***. *Mais si* $x \in ]-1; 1[$ *alors* $x^2 < 1$.
- $\forall n \in \mathbb{N}$ ; $n(n+1)$ *est divisible par 2.*
  *Si n est* ***pair*** *alors :*

$$\exists k \in \mathbb{N}/n = 2k \; n(n+1) = 2k(2k+1) = 2k'$$

*Si n est* ***impair*** *alors ;* $\exists k \in \mathbb{N}/n = 2k+1$, *il s'en suit que :*

$$n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1) = 2k'$$

### 1.2.2 Le quantificateur "$\exists$"

**Définition 1.3.**
*Il se lit "il existe au moins un élément".*
*La notation $\exists!$ signifie "il existe un et un seul élément".*
*L'assertion $\exists x \in \mathbb{E}$, P(x) est une assertion vraie lorsque l'on peut trouver au moins un élément de E pour lequel P(x) est vraie.*

**Exemple 1.8.**

- $\exists x \in \mathbb{R}$ *;* $(x(x-1)) < 0$ *est vraie, il suffit de prendre* $x \in ]0; 1[$.
- $\exists n \in \mathbb{N}$ *;* $n^2 - n > n$ *est vraie, on prend* $n \in \mathbb{N}$.
- $\exists x \in \mathbb{R}$ $(x^2 = -1)$ *est fausse.*

**Exemple 1.9.**

- $\exists z \in \mathbb{C}$ $(z^2 + z + 1 = 0)$ *sa négation est :*

$$\forall z \in \mathbb{C} \;\; (z^2 + z + 1 \neq 0)$$

- $\forall x \in \mathbb{R}$ , $x + 1 \in \mathbb{Z}$ *sa négation est :*

$$\exists x \in \mathbb{R} \; ; \; x + 1 \notin \mathbb{Z}$$

- $\forall x \in \mathbb{R} \;\; \exists y > 0 \;\; (x + y > 10)$ *sa négation est :*

$$\exists x \in \mathbb{R} \;\; \forall y > 0 \;\; x + y \leq 10$$

**Remarque 1.1.**
*L'ordre des quantificateurs est très important!!*

$$\forall x \in \mathbb{R} \; ; \;\; \exists y \in \mathbb{R} \;\; (x + y > 0)$$

*est vraie.*

$$\exists y \in \mathbb{R} \; ; \;\; \forall x \in \mathbb{R} \;\; (x + y > 0)$$

*est fausse.*

$$\exists x \in \mathbb{R} \; ; \; f(x) = 0$$

*il existe au moins un réel pour lequel $f$ s'annule.*
*L'assertion :*

$$\exists! x \in \mathbb{R} \; ; \; f(x) = 0$$

*Il existe un unique réel pour lequel f(x) s'annule.*
*La négation de l'inégalité stricte « $<$ » est l'inégalité au sens large « $\geq$ ».*
*Les quantificateurs ne sont pas des abréviations*

$$<< \textit{pour tout rel } x, \textit{ si } f(x) = 1 \textit{ alors } x \geq 0 >>$$

$$\Rightarrow \forall x \in \mathbb{R} \; ; \; f(x) = 1$$

$$\Rightarrow x \geq 0$$

## 1.3 Modes de Raisonnement

**Raisonnement direct**

Pour montrer que $<< P \Rightarrow Q >>$ est vrai.
On suppose que $P$ est vraie et on montre que $Q$ est vraie.

**Exemple 1.10.**
*Montrons que :*

$$\textit{si } a, b \in \mathbb{Q} \;\; \textit{alors} \;\; a + b \in \mathbb{Q}$$

*Soit $a \in \mathbb{Q}$ et $b \in \mathbb{Q}$ donc :*

$$a = \frac{p}{q} \textit{ avec } (p \in \mathbb{Z} \;\; \textit{et} \;\; q \in \mathbb{N}^*)$$

$$b = \frac{p'}{q'} \textit{ avec } (p' \in \mathbb{Z} \;\; \textit{et} \;\; q' \in \mathbb{N}^*)$$

*Donc :*

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

*Or :*

$$(pq' + p'q) \in \mathbb{Z} \textit{ et } qq' \in \mathbb{N}^*$$

*donc :*

$$a + b \in \mathbb{Q}$$

**Demonstration cas par cas**

Pour verifier une assertion P(x) pour tous les x dans E, on montre que l'assertion pour les x dans une partie A dans E, puis pour les x n'appartenant pas a A.

**Exemple 1.11.**
*montrons que :*

$$\forall x \in \mathbb{R} \ ; \ |x-1| \leq x^2 - x + 1$$

*Soit $x \in \mathbb{R}$, distinguant deux cas :*

- *$x \geq 1$ alors :*

  $$|x-1| = x-1$$

  *on obtient :*

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

- *$x \leq 1$ alors :*

  $$|x-1| = 1 - x$$

  *On obtient :*

  $$x^2 - x + 1 - 1 + x = x^2 \geq 0$$

  *Conclusion :*
  *Dans touts les cas on a :*

  $$x^2 - x + 1 - |x-1| \geq 0$$

**Démonstartion par contraposition**

Basée sur l'équivalence contre les assertions.

$$P \Rightarrow Q \text{ équivaut non } Q \Rightarrow \text{ non } P$$

Pour montrer l'assertion $P \Rightarrow Q$ :
On suppose que non $Q$ est vrai et on montre que non $P$ est vraie.

**Exemple 1.12.**
*Soit $n \in \mathbb{N}$, montrons que :*

$$n^2 \text{ est paire } \Rightarrow \text{ } n \text{ est pair}$$

*Supposons que n n'est pas pair càd n est impair.*

$$\exists k \in \mathbb{N} \ / \ n = 2k + 1$$

*Ainsi*

$$\begin{aligned} n^2 = (2k+1)^2 &= 4k^2 + 4k + 1 \\ &= 2\underbrace{(2k^2 + 2k)}_{k'} + 1 \text{ est impair} \end{aligned}$$

*Conclusion : $n^2$ n'est pas pair.*
*Et par contraposition ceci est équivalent a : si $n^2$ pair alors n est pair.*

**Démonstartion par absurde**

Pour montrer qu'une proposition est vraie par l'absurde, on suppose que sa négation est vrai et on déduit d'elle une contradiction.
Autrement dit, pour monter que $P \Rightarrow Q$, on suppose a la fois que P est vrai et Q est fausse et puis on cherche une contradiction.

**Exemple 1.13.**
*Soit* $(a, b) \in \mathbb{R}^*$, *montrons que :*

$$si \quad \frac{a}{b+1} = \frac{b}{a+1}$$

*alors :*

$$a = b$$

*Résolvons par absurde*
*On suppose que :*

$$\frac{a}{b+1} = \frac{b}{a+1} \; et \; a \neq b$$

*Alors :*

$$a(a+1) = b(b+1)$$
$$\Rightarrow a^2 + a = b^2 + b$$
$$\Rightarrow (a-b)(a+b) = b - a$$

*Or :*

$$a \neq b \Rightarrow a + b = -1$$

*Contradiction car :*

$$a; b \geq 0$$

*Conclusion :*

$$si \; \frac{a}{b+1} = \frac{b}{a+1} \; alors \; a = b$$

**Raisonnement par contre exemple**

Montrons que :

$$<< \forall x \in \mathbb{E} \; ; \; P(x) >> est \; fausse.$$

$$<< Tout \; entier \; positif \; est \; somme \; de \; carrés >>$$

Les carrés sont :

$$0^2, 1^2, 2^2 \ldots$$

un contre exemple est 7.
Les carrés qui sont inférieurs a 7 sont $0^2, 1^2, 2^2$

$$7 = a + b + c, \; a, b, c \in \{0, 1, 4\}$$

impossible.

**Raisonnement par Reccurence**

Soit $P$ une proprieté definie sur $(n_0, n_0+1, \ldots)$ $\{exp \ : \ P(x) = \frac{1}{n(n-1)(n-2)} \ \ n_0 = 3\}$

- $P(x_0)$ est vraie.
- Pour tous $n \geq 0$ $P(x)$ est vraie entraine que $P(n+1)$ est vraie.
- Alors $P(x)$ est vraie pour tout $n \geq n_0$.

**Exemple 1.14.**
*Montrons que :*

$$Pour \ \ tout \ \ n \in \mathbb{N} \ ; \ 2^n > n$$

***Initialisation** :*

$$on \ a \ pour \ n = 0 \quad 2^0 = 1 \geq 0$$

***Hérédité** :*
*fixons $n \geq 0$ supposons que P(x) est vraie*

$$2^{n+1} = 2^n \times 2 = 2^n + 2^n \geq n + 2^n \geq n + 1 \ \ (car \ 2^n \geq n)$$

*Donc :*

$$P(n+1) \ est \ vraie$$

*Conclusion :*
*d'après le principe de Reccurence $P(n)$ est vrai pour tout $n \geq 0$*

# Chapitre 2

# Structures fondamentales

## 2.1 les Ensemble

**Définition 2.1.** *Un ensemble est une Collection d'éléments.*

**Exemple 2.1.**

- $\{1, 2, 3\}$ ; $\{Rouge, vert, Jaune\}$ ; $\{0, 1, 2, 3, 4 \ldots\}$
- $x \in \mathbb{E}$ *; si* $x$ *est un élément de* $E$*, la négation est* $x \notin E$
  *Autre façon : une collection d'élément qui verifie une certaine propriété.*
- $\{x \in \mathbb{R} / |x - 2| \leq 1\} = ]1 \ ; \ 3[$
- $\{z \in \mathbb{C} / z^5 = 1\}$ *(racine cinquième de l'unité).*
- $\{x \in \mathbb{R} \ ; \ 0 \leq x \leq 2\}$.

On appelle ensemble vide l'ensemble qui ne contient aucun élément on le note $\emptyset$

### 2.1.1 L'appartenance

**Définition 2.2.**
*Soit* $E$ *un ensemble, on dit que* $x$ *est un élément de* $E$ *lorsque* $x$ *appartient a* $E$ *et on note alors :*

$$x \in \mathbb{E} \ , \ lorsque \ x \ n'appartient \ pas \ a \ E \ on \ note \ x \notin \mathbb{E}$$

*On appelle le singleton un ensemble ne contenant qu'un élément.*

$A = \{x\}$ est le singleton $x$.

### 2.1.2 L'inclusion

**Définition 2.3.**
*Soit $A$ et $B$ deux ensembles, on dit que $A$ est inclue dans $B$ lorsque tout élément de $A$ est un élément de $B$, et on la note $A \subset B$. Autrement dit :*

$$x \in \mathbb{A} \Rightarrow x \in \mathbb{B}$$

*On dit aussi que $A$ est une partie ou sous ensemble de $B$.*
*Soit $E$ un ensemble. On note $P(E)$ ensemble des parties de $E$*

**Exemple 2.2.**
$E = \{1, 2, 3\}$ *alors* $P(E) = P(\{1, 2, 3\}) = \{\emptyset, \{1, 2, 3\}, \{1\}, \{2\}, \{3\}, \{1, 2\}\{1, 3\}\{2, 3\} \ldots\}$

**Remarque 2.1.**
*Soient A,B et D trois sous ensembles d'un ensemble E.*
*Si $A \subset B$ et $B \subset D$ alors : $A \subset D$*

#### Egalité de deux ensembles

**Définition 2.4.**
*Deux ensembles $A$ et $B$ sont égaux si :*

$$A \subset B \text{ et } B \subset A$$

*Autrement dit :*

$$x \in \mathbb{A} \Leftrightarrow x \in \mathbb{B}$$

#### réunion de deux ensembles

**Définition 2.5.**
*Soit $E$ un ensemble, $A$ et $B$ deux ensembles de $E$, on appelle la réunion de $A$ et $B$ l'ensemble noté :*

$$A \cup B := \{x \in \mathbb{E} / x \in \mathbb{A} \text{ ou } x \in \mathbb{B}\}$$

#### Intersection de deux ensembles

**Définition 2.6.**
*Soient $E$ un ensemble, $A$ et $B$ deux ensembles de $E$.*
*On appelle l'intersection de $A$ et $B$ :*

$$A \cap B := \{x \in \mathbb{E} / x \in \mathbb{A} \text{ et } x \in \mathbb{B}\}$$

.

### Complémentaire d'un ensemble

**Définition 2.7.**
*Soit $E$ un ensemble et $A$ un sous ensemble de $E$ ($A \in \mathcal{P}(E)$) On appelle complémentaire de $A$ dans $E$ qu'on le note :* $A^c$ , $C^A$ , $\overline{A}$ , $E \setminus A$

**Proposition 2.1.**
*Soit $E$ un ensemble : $A$,$B$ et $C$ des sous ensembles de $E$ ($A, B, C \in \mathcal{P}(E)$)*

1. $A \cap (B \cap C) = (A \cap B) \cap C$
2. $A \cup (B \cup C) = (A \cup B) \cup A$
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. $(A^c)^c = A$
5. $A \subset B = C^B \subset C^A$
6. $C^{A \cap B} = C^A \cap C^B$
7. $C^{A \cup B} = C^A \cup C^B$

**Démonstration 1.**

- *Soit* $x \in A \cap (A \cap B)$
  *donc :*

$$\begin{aligned} & x \in A \text{ et } x \in (B \cap C) \\ \Leftrightarrow\ & x \in A \text{ et } x \in B \text{ et } x \in C \\ \Leftrightarrow\ & x \in (A \cap B) \text{ et } x \in C \\ \Leftrightarrow\ & x \in ((A \cap B) \cap C) \end{aligned}$$

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

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

- $C^{A \cap B} = C^A \cup C^B$

$$\begin{aligned} & \text{soit } x \in E \ , \ x \in C^{A \cap B} \\ \Leftrightarrow\ & x \notin A \cap B \\ \Leftrightarrow\ & x \in A \text{ ou } x \notin B \\ \Leftrightarrow\ & x \in C^A \text{ ou } x \in C^B \\ & x \in C^A \cup C^B \end{aligned}$$

### 2.1.3 Produit cartésien de n ensembles$(n \in \mathbb{N}^*)$

**Définition 2.8.**
*Soit* $E_1$ ; $E_2$ ; ... ; $E_n$ *des ensembles. Le produit cartésien de* $E_1 \times E_2 \times ..... \times E_n$
*c'est l'ensemble des n-uplets* $(x_1\ ,\ x_2\ ,\ \dots\ ,\ x_n)$ *où* $x_i \in E_i\ ,\ \forall i \in [1\ ;\ n] = \{1\ ;\ 2\ ;\ 3\ ;\dots\ ;\ n\}$
$E_1 \times E_2 \times ..... \times E_n := \{(x_1\ ,\ x_2\ ,\ \dots\ ,\ x_n)\ /\ \forall x_i \in E_i\ /\ \forall i \in [1\ ;\ n]\}$
*1-uplet s'appelle élément*
*2-uplet s'appelle couple*
*3-uplet s'appelle tripled*
*NB :* $E^n = \underbrace{E \times E \times ..... \times E}_{n\ fois}$

**Exemple 2.3.**

$$R^2 = R \times R = \{(x, y)/x, y \in R\}$$

$$[0; 2] \times R = \{(x; y)/0 \leq x \leq 2\ et\ y \in \mathbb{R}\}$$

$$[0; 1] \times [0; 1] \times [0; 1] = \{(x; y; z)\ /\ x; y; z \in [0; 1]\} = [0; 1]^3$$

## 2.2 Les applications

**Définition 2.9.**
*Soient* $E$ *et* $F$ *deux ensembles, une application ou une fonction* $f\ :\ E \to F$, *c'est associé à chaque* $x \in E$, *un unique élément de* $F$ *noté* $f(x)$

**Deuxième définition d'une application :**

Une application $f$ est triplet $(E, F, G)$ $E$ et $F$ sont des ensembles non vides, et $G$ un sous ensemble de $E \times F$ tel que :

$$\forall x \in E \ \ \exists! y \in F \ tel \ que \ (x; y) \in G$$

(L'élément $y$ est noté $f(x)$. On dit alors que $f$ est une application sur $E$ à valeurs dans F)

- L'ensemble des applications de $E$ dans $F$ est noté $F^E$ ou bien $\mathcal{F}(E, F)$
  - L'ensemble $E$ s'appelle l'ensemble de départ de $f$.
  - L'ensemble $F$ s'appelle l'ensemble d'arrivée de $f$.

  si $x \in E$, on appelle $f(x)$ l'image de $x$ par $f$, et si $y = f(x)$ on appelle $x$ un antécédant de $y$ par $f$.
- Deux applications $\ et\ g$ sont égaux si elles ont même ensemble de départ E et même ensemble d'arrivé F et partout $x \in E$, on a :

$$f(x) = g(x) \ \ (\forall x \in E \ , \ f(x) = g(x))$$

- Pour deux applications $f, g \ : \ E \to F$
  La négation de $f = g$ notée $f \neq g$ est :

$$(\forall x \in E \ ; \ \ f(x) = g(x))$$

  est fausse.
  Ceci équivalent à :

$$(\exists x \in E \ ; \ \ f(x) \neq g(x))$$

  Bref, pour montrer que $f \neq g$, il suffit de donner un contre exemple, c-à-d de donner un $x \in E$ tel que $f(x) \neq g(x)$.

### 2.2.1 Composée de deux applications

**Définition 2.10.**
*Soient E,F et G trois sous ensembles non vides*

$$f \ : \ \ E \to F \ \ et \ \ g \ : \ \ F \to G$$

*On définie une application de E vers G par*

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

*En posant :*

$$\forall x \in E \ \ g \circ f(x) := g(f(x))$$

**Exemple 2.4.**
*Soit $f$ et $g$ deux applications suivante :*

$$f \ : \ ]0;+\infty[\longrightarrow]0;+\infty[$$
$$x \longmapsto \frac{1}{x}$$
$$g \ : \ ]0;+\infty[\longrightarrow \mathbb{R}$$
$$x \longmapsto \frac{x-1}{x+1}$$
$$g \circ f \ : \ ]0;+\infty[\longrightarrow \mathbb{R}$$
$$g \circ f(x) = g(f(x)) = g(\frac{1}{x}) = \frac{1-x}{1+x} = -g(x)$$

### 2.2.2 L'image directe et l'image reciproque par une application

**L'image directe par une application**

**Définition 2.11.**
*Soient $E$ et $F$ deux ensembles, et $f$ est une application de $E$ dans $F$*
*$A$ une partie de $E$ et $B$ une partie de $F$.*
*L'image directe de $A$ par $f$ est notée $f(A)$ elle est définie par :*

$$f(A) = \{y \in F/ \ \exists x \in A \ ; \ y = f(x)\}$$

*C'est le sous ensemble de $F$ formé des éléments $x$ de $E$ tels $x$ a au moins un antécédant par $f$ appartenant à $A$.*
*On dit pour simplifier que :*

$$f(A) = \{f(x) \ / \ x \in A\}$$

*C'est l'ensemble des valeurs prises par $f$ lorsque $x$ parcourt $A$, càd :*

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

**Exemple 2.5.**

$$f \ : \ \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longrightarrow x^2$$

$A = [-1;1]$

$$\begin{aligned} f(A) &= \{f(x) \ / \ -1 \leq x \leq 1\} \\ &= \{x^2 \ / \ -1 \leq x \leq 1\} \\ &= [0;1] \end{aligned}$$

**L'image réciproque par une application**

**Définition 2.12.**
*L'image réciproque de $B$ par $f$ est notée $f^{-1}(B)$, elle est définie par :*

$$f^{-1}(B) = \{x \in E \ / \ f(x) \in B\} \in \mathcal{P}(E)$$

*C'est l'ensemble des éléments $x$ de $E$ dont l'image appartient à $B$.*

**Exemple 2.6.**

$$\begin{aligned} f \ : \ & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \to x^2 \end{aligned}$$

$B = [-4; 4]$

$$\begin{aligned} f^{-1}(B) &= \{x \in \mathbb{R} \ / \ f(x) \in [-4; 4]\} \\ &= \{x \in \mathbb{R} \ / \ -4 \leq x \leq 4\} \\ &= [-2; 2] \end{aligned}$$

**Remarque 2.2.**
*Pour determiner $f^{-1}(B)$, on ne suppose pas que $f$ est bijective. $f^{-1}$ n'est pas une application réciproque.*
*C'est l'application qui a un ensemble $B \subset F$, fait correspondre un ensemble.*

$$(f^{-1}(B) \leq E)$$

$$\begin{aligned} f^{-1} \ : \ & \mathbb{P}(F) \longrightarrow \mathbb{P}(E) \\ B \longrightarrow & f^{-1}(B) = \{x \in E \ / \ f(x) \in B\} \end{aligned}$$

**Proposition 2.2.**
*Soient E,F deux ensembles $f \ : \ E \longrightarrow F$ une application $A \subset E$ et $B \subset F$*

1. $f(\emptyset) = \emptyset$
2. $A \subset B \Rightarrow f(A) \subset f(B)$
3. $f(A \cup B) = f(A) \cup f(B)$
4. $f(A \cap B) \subset f(A) \cap f(B)$
5. $f^{-1}(\emptyset) = \emptyset$
6. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
7. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
8. $f^{-1}(C^A) = C^{f^{-1}(A)}$

**Démonstration 2.**

- $f^{-1}(A \cup B) = f^{-1} \cup f^{-1}(B)$
  *Soit $x \in f^{-1}(A \cup B)$ :*

$$\begin{aligned} & \Leftrightarrow f(x) \in A \cup B \\ \Leftrightarrow & f(x) \in A \ ou \ f(x) \in B \\ \Leftrightarrow & x \in f^{-1} \ ou \ x \in f^{-1}(B) \\ \Leftrightarrow & x \in f^{-1}(A) \cup f^{-1}(B) \end{aligned}$$

- $f(A \cap B) \subset f(A) \cap f(B)$
  *soit* $y \in f(A \cap B)$

  $$\Rightarrow \exists x \in A \cap B \ / \ y = f(x)$$

  $x \in A \cap B$

  $$\Rightarrow x \in A \text{ et } x \in B$$
  $$\Rightarrow f(x) \in f(A) \text{ et } f(x) \in f(B)$$
  $$\Rightarrow f(x) \in f(A) \cap f(B)$$
  $$\Rightarrow y \in f(A) \cap f(B)$$

  *En genéral :*

  $$f(A \cap B) \subseteq f(A) \cap f(B)$$

  *On prend :*

  $$f(x) = x^2 \quad A = \{1\} \ ; \ B = \{-1\} \ A \cap B = \emptyset \ f(A) = \{1\} \ f(B) = \{1\}$$

  $f(A) \cap f(B) = 1$ *($\emptyset$ est inclus strictement dans $\{1\}$)*

- $f^{-1}(C^A) = C^{f^{-1}(A)}$
  *soit* $x \in f^{-1}(C^A)$

  $$\Leftrightarrow f(x) \in C^A$$
  $$\Leftrightarrow f(x) \notin A$$
  $$\Leftrightarrow x \notin f^{-1}(A)$$
  $$\Leftrightarrow x \in C^{f^{-1}(A)}$$

**Exemple 2.7.**
*Determinons* $\cos([\frac{\pi}{4}; \frac{5\pi}{6}])$ *et* $\cos^{-1}(\{-1; 1\})$

$$\cos([\frac{\pi}{4}; \frac{5\pi}{6}]) = \{\cos x \ ; \ x \in [\frac{\pi}{4}; \frac{5\pi}{6}]\} = [-\frac{\sqrt{3}}{2}; \frac{\sqrt{2}}{2}].$$
$$\cos^{-1}(\{-1; 1\}) = \cos^{-1}(\{-1\} \cup \{1\})$$
$$= \cos^{-1}(\{-1\}) \cup \cos^{-1}(\{1\})$$
$$\Leftrightarrow \cos^{-1}(\{1\}) = \{x \in \mathbb{R} \ / \ \cos(x) = 1\}$$
$$\Leftrightarrow \cos(x) = 1$$
$$\Leftrightarrow \ \{x = 2k\pi \ ; \ k \in \mathbb{Z}\}$$
$$\cos^{-1}(\{1\}) = \{2k\pi \ ; \ k \in \mathbb{Z}\}$$
$$\cos(\{-1\}) = \{x \in \mathbb{R} \ / \ \cos(x) = -1\}$$
$$\Leftrightarrow \cos(x) = -1$$
$$\Leftrightarrow x = \pi + 2k\pi$$
$$= \pi(2k + 1) \ / \ k \in \mathbb{Z}$$
$$\cos^{-1}(\{-1\}) = \{(2k + 1)\pi \ / \ k \in \mathbb{Z}\}$$

*Finalement :*

$$\cos^{-1}(\{-1; 1\})) = \cos^{-1}(\{1\}) \cup \cos^{-1}(\{-1\})$$
$$= \{k\pi \ ; \ k \in \mathbb{Z}\}$$
$$= \mathbb{Z}\pi$$

**Application injective : (injection)**

**Définition 2.13.**
*Soient $E$ et $F$ deux ensembles, et $f : E \longrightarrow F$ une application.*
*$f$ est injective signifie :*

$$\forall (x,y) \in E^2 \ ; \ f(x) = f(y) \Rightarrow x = y$$

*Ceci équivaut à :*

$$\forall (x,y) \in E^2 \ ; \ x \neq y \Rightarrow f(x) \neq f(y)$$

*Intuitivement : une application est injective si deux éléments differents de son ensemble de départ ne peuvent pas avoir la même image.*
*$f$ n'est pas injective :*

$$\exists x; y \in E \ / \ x \neq y \ et \ f(x) \neq f(y)$$

*Autrement, $f$ est injective si et seulement si :*
*$\forall y \in F$, l'équation $f(x) = y$ admet au plus une solution dans l'ensemble de départ $E$ (éventuellement aucune solution), c-à-d tout élément $y \in F$ a au plus un antécédant (éventuellement aucun antécédant).*

**Exemple 2.8.**

- *Montrer que $f$ est injective.*

$$\begin{aligned} f \ : \ \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\to x^2 \end{aligned}$$

*$f$ est injective :*
*en effet, soit $(x,y) \in \mathbb{R}_+^2$*

$$\begin{aligned} f(x) = f(y) &\Rightarrow x^2 = y^2 \\ x^2 - y^2 = 0 \ &\Rightarrow \ (x-y)(x+y) = 0 \\ &\Rightarrow \ x = y \ ou \ x = -y \\ &\Rightarrow x = y \ ou \ x = -y = 0 \\ &\Rightarrow x = y \end{aligned}$$

*Donc l'application est injective.*

- *Montrer $f$ n'est pas injective.*

$$\begin{aligned} f \ : \ \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\to x^2 \end{aligned}$$

*on donne un contre exemple :*

$$x = 1 \ et \ x' = -1 \ , \ f(x) = f(x') = 1$$

**Remarque 2.3.**
*En général, pour montrer qu'une application est injective ou pas consiste à essayer de montrer qu'elle est injective, en cours de route, si on rencontrer une difficulté alors on utilise cette difficulté pour avoir une idée pour trouver $x$ et $x'$ qui contre dise l'injection, c-à-d :*

$$(x \neq x' \ et \ f(x) = f(y))$$

**Exemple 2.9.**
*on donne l'application :*

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \to \frac{x}{1+x^2}$$

*Soient* $x; y \in \mathbb{R}$ / $f(x) = f(y)$

$$\Rightarrow \frac{x}{1+x^2} = \frac{y}{1+y^2}$$
$$\Rightarrow x(1+y^2) = y(1+x^2)$$
$$\Rightarrow x - x^2y + xy - y = 0$$
$$\Rightarrow x - y + xy(y-x) = 0$$
$$\Rightarrow (x-y)(1-xy) = 0$$

*donc*

$$x = y \ ou \ xy = 1$$

*on prend :*

$$x = 2 \ et \ y = \frac{1}{2}x \neq y$$

*donc :*

$$f(2) = \frac{2}{1+4} = \frac{2}{5} \ et \ f(\frac{1}{2}) = \frac{2}{5}$$

*donc :*

$$\exists x, y \in \mathbb{R} \ / \ x \neq y \ et \ f(x) = f(y)$$
$$\Rightarrow f \ n'est \ pas \ injective$$

**Application surjective**

**Définition 2.14.**
*Soient E,F deux ensembles et f une application de E dans F, dire que f est surjective (ou f est une surjection) signifie :*

$$\forall y \in \mathbb{F} \ , \ \exists x \in \mathbb{E} \ / \ y = f(x)$$

*c-à-d partout* $y \in F$*, l'équation* $y = f(x)$ *admet au moins une solution. Autrement : tout élément* $y \in F$ *admet au moins un antécédant dans* $\mathbb{E}$*.*
*f n'est pas surjective :*

$$\exists y \in F \ ; \ \forall x \in E \ ; \ y \neq f(x)$$

**Exemple 2.10.**

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \to 2x + 1$$

*On montre que f est surjective.*
*Soit* $y \in \mathbb{R}$

$$y = f(x) \Leftrightarrow y = 2x + 1$$
$$\Leftrightarrow x = \frac{1}{2}(y-1) \in \mathbb{R}$$

*On a montrer que :*
$\forall y \in \mathbb{R}$ ; *l'équation* $y = 2x + 1$ *admet au moins une solution.*

$$\forall y \in \mathbb{R} \ ; \ \exists x \ (x = \frac{y-1}{2}) \in \mathbb{R} \ / \ y = f(x)$$

*donc l'application* $f$ *est surjective.*

$$\begin{aligned} f \ : \ \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\to x^2 \end{aligned}$$

*On prend* $y = -1$ *on a :*

$$f(x) = x^2 \geq 0 \quad \forall x \in \mathbb{R}$$

*donc :*

$$f(x) \neq -1 \quad \forall x \in \mathbb{R}$$

$\Rightarrow$ *l'application* $f$ *n'est pas surjective.*

$$\begin{aligned} f \ : \ \mathbb{R} \setminus \{1\} &\longrightarrow \mathbb{R} \\ x &\longrightarrow \tfrac{x+2}{x-1} \end{aligned}$$

*On va tenter de montrer la surjectivité et repérer les difficultés qui l'on peut rencontrer pour resoudre l'equation* $y = f(x)$
*Supposons que* $f$ *est surjective. Soit* $y \in F$ *:*

$$\begin{aligned} y = f(x) \Rightarrow y &= \frac{x+2}{x-1} \\ &\Rightarrow y(x-1) = x + 2 \\ &\Rightarrow x(y-1) = y + 2 \\ &\Rightarrow x = \frac{y+2}{y-1} \end{aligned}$$

*(probleme quand* $y = 1$*), on donne un "contre exemple".*

$$\begin{aligned} y = f(x) \Leftrightarrow 1 &= \frac{x+2}{x-1} \\ &\Leftrightarrow x - 1 = x + 2 \\ &\Leftrightarrow -1 = 2 \ (Absurde!!) \end{aligned}$$

*D'où* $f$ *n'est pas surjective.*

### Application bijective

**Définition 2.15.**
*Soient* $E$ *et* $F$ *deux ensembles et* $f \ : \ E \to F$ *une application.*
*Dire que* $f$ *est bijective signifie qu'elle est à la fois injective et surjective.*
*Autrement, si elle verifie l'une des 3 proprietés suivants :*

- $\forall y \in F \ ; \ \exists! x \in E \ ; \ y = f(x)$
- *Tout élément* $y$ *de l'espace d'arrivée a un seul antécédant.*
- *Pour tout élément* $y$ *de l'espace d'arrivée l'équation* $y = f(x)$ *admet une et une seule solution dans l'espace de départ.*

**Exemple 2.11.**

$$\begin{aligned} f \ : \ \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\to f(x,y) = (x-2y, 2x+3y) \ . \end{aligned}$$

*Soit* $(a,b) \in \mathbb{R}$ :

$$f(x,y) = (a,b) \Leftrightarrow (a,b) = (x-2y \ ; \ 2x+3y)$$

$$\Leftrightarrow \begin{cases} x-2y = a & (1) \\ 2x+3y = b & (2) \end{cases}$$

$$(1) \times 2 - (2) \Rightarrow -7y = 2a - b$$

$$\Rightarrow y = -\frac{2a-b}{7}$$

$$x = a + 2y = a - \frac{4a-2b}{7} = \frac{3a+2b}{7}$$

*L'équation* $(a,b) = f(x,y)$ *admet une seule solution*

$$(x;y) = (\frac{3a+2b}{7}; \frac{-2a-b}{7})$$

*Conclusion :* $f$ *est bijective de* $\mathbb{R}^2$ *vers* $\mathbb{R}^2$.

**Proposition 2.3.**
*Soient E,F et G trois ensembles,* $f$ *une application de E dans F et* $g$ *une application de F dans G.*

$$\left.\begin{array}{c} g \text{ est injective} \\ f \text{ est injective} \end{array}\right\} \Rightarrow g \circ f \text{ injective}$$

$$\left.\begin{array}{c} g \text{ est surjective} \\ f \text{ est surjective} \end{array}\right\} \Rightarrow g \circ f \text{ surjective}$$

**Démonstration 3.**

- $$\begin{aligned} g \circ f \ : \ E &\longrightarrow G \\ x &\to g \circ f(x) = g(f(x)) \end{aligned}$$

  *Soient* $x, y \in E$ *tel que* $g \circ f(x) = g \circ f(y)$

  $$\Rightarrow g(f(x)) = g(f(y))$$

  *Comme* $g$ *est injective, alors :*

  $$f(x) = f(y)$$

  *on a* $f$ *est injective, donc :*

  $$x = y$$

  *Conclusion :*

  $$g \circ f \text{ est injective}$$

- *Soit $z \in G$, on a $g$ est surjective alors :*

$$\exists y \in F \text{ tel que } g(y) = z$$

*Comme $f$ est surjective alors :*

$$\exists x \in E \text{ tel que } f(x) = y$$

*alors :*

$$g \circ f(x) = g(f(x)) = g(y) = z$$

*puisque on a :*

$$\forall z \in G \ \ \exists \in E \text{ tel que } g \circ f(x) = z$$

*donc $g \circ f$ est surjective.*

**Application identité**

**Définition 2.16.**
*Soit $E$ un ensemble non vide, on appelle application identité ou (identité de $E$) et l'on note $Id_E$. L'application de $E$ vers $E$ definie par :*

$$Id_E(x) = x \ ; \ \forall x \in E$$

$$Id_E : E \longrightarrow F$$

$$x \to Id_E(x) = x$$

**Remarque 2.4.**
*Si $f \ : \ E \longrightarrow F$ est une application.*

$$Id_E \circ f = f \text{ et } f \circ Id_E = f$$

### 2.2.3 Application reciproque

**Définition 2.17.**
*Si $f$ est une application bijective de $E$ vers $F$.*
*L'application qui à tout $y$ de $F$ fait correspondre son unique antécédent $x$ est appelée application ou bijection reciproque de $f$ et notée $f^{-1}$*

$$f^{-1} \ : \ F \longrightarrow E$$

$$f^{-1}(y) = \ l'unique \ antécédant \ de \ y$$

**Exemple 2.12.**
*Soit $f$ l'application dans* ***exemple 1.25***

$$f \ : \ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$(x, y) \to (x - 2y; 2x + 3y)$$

*On a verifié qu'elle est bijective.*

$$f^{-1} \ : \ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$f^{-1}(a, b) = (\frac{3a + 2b}{7}, \frac{b - 2a}{7})$$

***comment determiner $f^{-1}$***

*Pour determiner $f^{-1}$, on résout l'équation $y = f(x)$ et on utilise la caracterisation suivante de $f^{-1}$ :*

$$\forall x \in E \ ; \ \forall y \in F \quad y = f(x) \Leftrightarrow f^{-1}(y) = x$$

**Remarque 2.5.**

1. $f^{-1} \circ f(x) = x \ ; \ \forall x \in E$
2. $f \circ f^{-1}(y) = y \ ; \ \forall y \in F$
3. $f(f^{-1}(y)) = y \ ; \ \forall y \in F$

**Autre méthode pour montrer qu'une application est bijective**

**Proposition 2.4.**
*Si $f \ : \ E \longrightarrow F$ et $g \ : \ F \longrightarrow E$ sont deux applications verifiant :*

$$f \circ g = Id_E \text{ et } g \circ f = Id_E$$

*alors elles sont touts les deux bijectives et reciproque l'une de l'autre.*

**Démonstration 4.**
*Soit $y \in F$ si :*

$$y = f(x) \Rightarrow g(y) = g(f(x)) = g \circ f(x) = x$$
$$\Rightarrow x = g(y) \ (l'unicité)$$
$$f(g(y)) = f \circ g(y) = y \ (existance)$$
$$\Rightarrow \ l'équation \ y = f(x) \ admet \ une \ unique \ solution.$$
$$x = g(y) = f^{-1}(y) = g(y) \ \Rightarrow f^{-1} = g$$

***Conséquence***

$$(f^{-1})^{-1} = f \quad f \ : \ E \longrightarrow F \text{ et } g \ : \ F \longrightarrow G \ \text{ est bijective.}$$
$$g \circ f \text{ est bijective, avec } (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

**Remarque 2.6.**
*L'utilisation de la notation $f^{-1}(B)$ ne suppose pas que $f$ est bijective, lorsque $f$ est bijective. $f^{-1}(B)$ represente aussi bien l'image directe de $B$ par l'application $f^{-1}$.*
*Une application $f \ : \ E \longrightarrow F$ est :*

$$f \text{ injective } \Leftrightarrow \ \forall y \in F \ ; \ f^{-1}(\{y\}) \text{ contient au plus un élément}$$
$$f \text{ est surjective } \Leftrightarrow \ \forall y \in F \ ; \ f^{-1}(\{y\}) \text{ contient au moins un élément}$$
$$f \text{ est bijective } \Leftrightarrow \ \forall y \in F \ ; \ f^{-1}(\{y\}) \text{ contient un seul élément}$$

## 2.3 Les structures algebriques

**Définition d'une loi de composition interne : (LCI)**

Soit E un ensemble non vide, on appelle (LCI) ou opération sur E, toute application de l'ensemble produit $E \times E$ dans l'ensemble E lui même.

$$E \times E = \{(x, y)/x \in E \ ; \ y \in E\}$$

Une loi de composition interne sur E consiste donc, intuitivement à faire correspondre à tout couple $(x, y)$ d'éléments, un troisième élément de E qui depend de $x$ et $y$ suivant une loi donnée d'avance.

**Exemple 2.13.** $\{1, 2\}$ $E \times E = \{(1, 1); (2, 2); (1, 2); (2, 1)\}$

**Notations**

Dans la pratique on emploie pour designer les lois de composition(LCI) des notations tel que :
$+$(se lit plus)
$\times$ (se lit fois)
$\top$ (se lit truc)
$\perp$ (se lit antitruc)
$\circ$ (se lit rang)
$*$ (se lit etoile)

- Une LCI sur un ensemble E, notée $+$ s'appelle une addition sur E.
- Une loi LCI sur un ensemble E, notée $\times$ s'appelle une multiplication sue E.
- Soit une LCI sur E :
  $$\begin{array}{c} E \times E \longrightarrow E \\ (x, y) \to x * y \end{array}$$
  L'image d'un couple $(x, y) \in E \times E$ par $*$ est notée :
  $$x * y \ au \ lieu \ de \ *(x, y)$$

**Exemple 2.14.**
*L'addition usuelle sur* $\mathbb{N}, \mathbb{N}^*, \mathbb{Q}$ *(mais pas sur* $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$ *et* $\mathbb{C}^*$*)*

- *Soit E un ensemble, l'opération de composition des applications* $\circ$ *constitue une LCI sur l'ensemble* $\mathbb{F}(E, F)$ *des applications de E vers lui même.*
  $$\begin{array}{rcl} \circ \ : & \mathbb{F}(E, E) \times \mathbb{F}(E, E) \longrightarrow \mathbb{F}(E, E) \\ & (f, g) \longmapsto f \circ g = f(g(x)) \end{array}$$
- *Sur l'ensemble* $\mathbb{P}(E)$ *des parties de E, les opérations* $\cup$ *et* $\cap$ *sont des LCI :*
  $$\begin{array}{rcl} \cup \ : & \mathbb{P}(E) \times \mathbb{P}(E) \longrightarrow \mathbb{P}(E) \\ & (A, B) \longmapsto A \cup B \end{array} \qquad \begin{array}{rcl} \cap \ : & \mathbb{P}(E) \times \mathbb{P}(E) \longrightarrow \mathbb{P}(E) \\ & (A, B) \longmapsto A \cap B \end{array}$$
- *L'addition entre fonctions de* $\mathbb{R}$ *dans* $\mathbb{R}$ *constitue une LCI sur* $\mathbb{F}(\mathbb{R}, \mathbb{R})$
  $$\begin{array}{rcl} + \ : & \mathbb{F}(\mathbb{R}, \mathbb{R}) \times \mathbb{F}(\mathbb{R}, \mathbb{R}) \longrightarrow \mathbb{F}(\mathbb{R}, \mathbb{R}) \\ & (f, g) \longmapsto f + g \end{array}$$

- *L'addition entre deux vecteurs dans* $\mathbb{R}^2$ *consitue aussi une LCI :*

$$+ \ : \ \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$((x,y);(x',y')) \longmapsto (x+x', y+y')$$

**Remarque 2.7.**
*Dans toute la suite* $*$ *designe un LCI sur un ensemble* $E$ *(ou* $E$ *un ensemble muni d'une LCI).*

**Définition de l'associativité :**

On dit que $*$ est associativie lorsque pour tous :

$$x, y, z \in E \quad : \quad x * (y * z) = (x * y) * z$$

cette valeur commune peut être alors notée sans ambiguité $x * y * z$, cela veut dire lorsqu'on va composer $y$ et $z$ et puis $x$ et le resultat obtenu, or $x$ et $y$ et puis le resultat obtenu et $z$. On obtient le même resultat.

**Notations**
$x * y$ s'appelle $x$ composé $y$.

**Exemple 2.15.**

- *La loi "*$\circ$*" est associative sur* $\mathbb{F}(E,E)$ *:*

$$(f \circ g) \circ h = f \circ (g \circ h) \quad \forall f; g; h \in \mathbb{F}(E,E)$$

- *la loi usuelle "*$-$*" n'est pas associative sur* $\mathbb{R}$ *:*

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(a,b) \longmapsto a - b$$

***Contre exemple***
$a = 0, b = 1, c = 1$

$$(a-b) - c = (-1) - 1 = -2$$

$$a - (b - c) = 0 - (0) = 0 \neq -2$$

**Défintion de la commutativité**

On dit que $*$ est commutativité :

$$\forall x, y \in E \ , \ x * y = y * x$$

**Exemple 2.16.**
*En général, la loi* $\circ$ *n'est pas commutative.*
*La loi* $\circ$ *n'est pas commutative sur* $\mathbb{F}(\mathbb{N},\mathbb{N})$*, on donne un contre exemple :*
*Soit* $g$ *et* $h$ *deux applications de* $\mathbb{N}$ *vers* $\mathbb{N}$ $\quad h \ : \ x \longmapsto x+1$

$$g \ : \ x \longmapsto \begin{cases} x & si\ x = 0 \\ x-1 & si\ x \geq 1 \end{cases}$$

$$g \circ h(x) = g(h(x)) = g(x+1) = x+1-1 = x \qquad g \circ h = Id_{\mathbb{N}}$$

$$h \circ g(x) = h(g(x)) = \begin{cases} x+1 & si\ x = 0 \\ x & si\ \ x \geq 1 \end{cases} \quad ; \quad \forall x \in \mathbb{N}$$

$$g \circ h(0) = 0 \neq h \circ g(0) = 1$$

$$\Longrightarrow g \circ h \neq h \circ g$$

*Conclusion : la loi $\circ$ n'est pas commutative sur $\mathbb{F}(\mathbb{N}, \mathbb{N})$*

**Définition de l'élément neutre**

Soit $e \in E$. On dit que e est l'élément neutre si :

$$\forall x \in E \quad x * e = e * x = x$$

(les deux égalités doivent être vérifiées lorsque $*$ n'est pas commutative).

**Exemple 2.17.**

1. *Adittion usuelle sur $\mathbb{R}$ : $e = 0$*
2. *La multiplication usuelle sur $\mathbb{R}$ : $e = 1$*
3. *La loi $\cup$ sur $\mathbb{P}(E)$ : $e = \emptyset$* $\qquad A \cup \emptyset = \emptyset \cup A = A;\ \forall A \in \mathbb{P}(E)$
4. *La loi $\cap$ sur $\mathbb{P}(E)$ : $e = E$* $\qquad A \cap E = E \cap A = A;\ \forall A \in \mathbb{P}(E)$
5. *La loi $\circ$ sur $\mathbb{F}(E, E)$ : $e = Id_E$* $\qquad f \circ Id_E = Id_E \circ f = f;\ \forall f \in \mathbb{F}(F, F)$
6. *La loi "$-$" usuelle sur $\mathbb{R}$, n'admet aucun élément neutre.*

*Supposons par Absurde qu'elle admet un élément neutre e, donc :*

$$e - a = a - e = a\ ;\ \forall a \in \mathbb{R}$$

$$\Rightarrow 2E = 2a \Rightarrow\ e = 0$$

$$\Rightarrow\ a = 0\ ;\ \forall a \in \mathbb{R}$$

*Quand on compose "e" a n'importe quel élément x, on va trouver l'élément x.*

**Proposition 2.5.**
*S'il y a dans E un élément neutre pour $*$, alors il'y en a qu'un seul.*

**Démonstration 5.**
*Si e et $e'$ sont deux éléments neutres pour $*$.*
*Le fait que e est neutre, alors : $e * e' = e' * e = e'$*
*Le fait que $e'$ est neutre, alors :*

$$e' * e = e * e' = e$$

*On déduit que :*

$$e = e'$$

**Définition d'un monoïde**

Si $*$ est LCI associative sur E et s'il y a dans E un élément neutre.
Pour $*$, on dit que $(E, *)$ est un monoïde. Si deplus $*$ est commutative, on dit que ce monoïde est commutatif.

**Exemple 2.18.**
*$(\mathbb{R}, \times)$ est un monoïde commutative, $\times$ est commutative, 1 est l'élément neutre :*

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

*$\mathbb{F}(\mathbb{N} \times \mathbb{N}, \circ)$ est un monoïde, $\circ$ est associative, $Id_{\mathbb{N}}$ est l'élément neutre, mais elle n'est pas commutative.*

$$(\mathbb{P}(E), \cup) \text{ est un monoïde commutatif}$$

$$(\mathbb{P}(E), \cap) \text{ est un monoïde commutatif}$$

**Définition d'un élément symétrique**

On suppose ici que E admet un élément neutre $e$ pour $*$
Soient $x, x'$ deux éléments de E. On dit $x$ est symétrique de $x'$ par la loi $*$ lorsque :

$$x * x' = x' * x = e$$

Lorsqu'on va composer deux éléments symétrique le résultat obtenu est l'élément neutre.
$x'$ s'appelle le symétrique de $x$. On dit que $x$ est symétrisable.

**Remarque 2.8.**
*Si $x$ est symétrique, il en est de même de son symétrie.*
*$x'$ et celui ci admet $x$ pour symétrique.*

**Exemple 2.19.**
*Les éléments symétrisables de $(\mathbb{R}; \times)$ sont $\mathbb{R}^*$*
*$Id_E$ est un élément symétrisables de $(\mathbb{F}(E, E); \circ)$*
*L'élément neutre s'il existe est toujours symétrisable et son symétrique est lui-même.*

**Proposition 2.6.**
*Si $*$ est associative et si $x$ un élément de $E$ admet un symétrique pour $*$. Alors il est unique.*

**Démonstration 6.**
*Si $x'$ et $x''$ sont deux symétrique de $x$.*

$$\begin{aligned} x' = e * x' &= (x" * x) * x' \\ &= x" * (x * x') \\ &= x" * e = x" \end{aligned}$$

*donc :*

$$x' = x" \text{ d'où l'unicité}$$

**Définition de la distributivité d'une LCI par rapport à une autre loi de composition interne**

On suppose que E est muni d'une deuxième LCI noté $\top$. On dit que $*$ est distributive sur $\top$ lorsque :

$$\forall x, y, z \in E\ x * (y \top z) = (x * y) \top (x * y) \text{ et } (y \top z) * x = (y * x) \top (z * x)$$

**Exemple 2.20.**

- $E = \mathbb{R}$ $* = \times$ *et* $\top = +$

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

*Dans* $\mathbb{R}$ *la multiplication est distributive sur l'addition.*

- *Soit* $X$ *un ensemble et* $E = P(X)$
  $\cup$ *est distributive sur l'intersection :*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \ ; \ \forall A, B, C \in E$$

  $\cap$ *est distributive sur la réunion :*

$$A \cap (B \cup C) = (A \cup B) \cap (A \cup C) \ ; \ \forall A; B; C \in E$$

- $E = F(\mathbb{R}) \circ$ *est distrubitive sur la loi* $+$*, on rappelle que :*

$$(f + g)(x) = f(x) + g(x) f \circ (h + g) = f \circ h + f \circ g$$

*et*

$$(g + h) \circ f = g \circ h + h \circ f \quad \forall f; g; h \in E$$

**Vocabulaire :**

Dans le cas d'une LCI notée $\times$
On emploie le mot inverse au lieu du mot symétrique,et le mot inversible au lieu de mot symétrisable. L'inverse de $x$ est souvent noté $x^{-1}$.
Dans le cas d'une LCI notée $+$ l'élément neutre est appelé zéro, $O_{\mathbb{R}^2} = (0, 0)$ est noté $O$.

$$O_{F \in \mathbb{N}} = la \ fonction \ nul \ f(x) = 0 \ (l'axe \ des \ abscisces)$$

L'élément symétrique de $x$ est appelé l'opposé de $x$ et notée $-x$.
On écrit :

$$x - y \ au \ lieu \ de \ x + (-y)$$

**Définition de stabilité pour une LCI**

Soit F une partie de E,F est dite stable par loi $*$, si pourtout couple $(x, y)$ d'éléments de F. Le composé de $x$ et $y$, $x * y$ appartient à F, ce qui s'écrit avec les quantificateurs.

$$\forall x \in F \ , \ \forall y \in F \ , \ x * y \in F$$

**Exemple 2.21.**

- $F = E$ *est stable pour* $*$*. Si* $*$ *admet un élément neutre.*
  $E = \mathbb{R}^2$ ; $* = +$ *et* $F = \{(x, y) \in \mathbb{R} / x \geq 0\}$*,* $F$ *est stable pour la loi* $+$
  *Soit en effet :*

$$(x, y) \ et \ (x', y') \in F$$

$$(x, y) + (x', y') = (x + x', y + y')$$

  *on a :*

$$x + x' \geq 0 \Rightarrow (x, y) + (x', y') \in F$$

- $E = \mathbb{Z}$ , $* = +$ $n \in \mathbb{N}^*$ *et* $F = n\mathbb{Z} = \{nk \ ; \ k \in \mathbb{Z}\}$
  *Soient* $x, y \in F$ *:*

$$\exists k \in \mathbb{Z}/x = nk$$
$$\exists k' \in \mathbb{Z}/y = nk'$$
$$x + y = nk + nk'$$
$$= n(k + k') \in F$$

**Définition de la loi induite**

Si F est stable par $*$ alors la restriction de $*$ à F. $f \ : \ E \longrightarrow F \ \ (A \subset E)$
la restriction de $f$ à $A$.

$$f_{/A} \ : \ A \longrightarrow F$$
$$x \longmapsto f_A(x) = f(x)$$

est une loi LCI sur F dite la loi induite par $*$.
En pratique on conserva le même symbole de la loi sur E on la note $*$ au lieu de $T$.

$$T \ : \ F \times F \longrightarrow F$$
$$(x, y) \longmapsto x * y$$

### 2.3.1 Structure de groupe

**Définition 2.18.**
*Un ensemble non vide G muni d'une loi de composition interne notée* $*$ *est un groupe, ssi :*

1. $*$ *est associative* $x * (y + z) = (x * y) * z \ , \ \forall x, y, z \in G$.
2. $*$ *admet un élément neutre c-à-d :* $\exists e \in G/x * e = e * x = x \ , \ \forall x \in G$
3. *Toute élément de G est symétrisable de x.*

*Lorsque la loi* $*$ *est commutative, on dit que G est un groupe commutatif ou abélien.*

**Exemple 2.22.**
$(\mathbb{Z}, +); (\mathbb{R}, +); (\mathbb{Q}, +); (\mathbb{R}^*, \times); (\mathbb{C}, +); (\mathbb{Q}^*, \times); (\mathbb{C}^*, \times)$ *sont des groupes abeliens.*
$(\mathbb{R}^2, +)$ *est un groupe abelien.*
*On définit d'abord l'addition dans* $\mathbb{R}^2$ *:*

$$\forall (x, y) \ ; \ (x', y') \in \mathbb{R}^2 \ \ (x, y) + (x', y') = (x + x', y + y')$$

$\rightarrow$ *soient* $(x, y); (x', y'); (x", y") \in \mathbb{R}^2$

$$(x, y) + [(x', y') + (x", y")] = (x, y) + (x' + x", y' + y")$$
$$= (x + (x' + x"); y + (y' + y"))$$
$$= ((x + x') + x"; (y + y') + y")$$

$$= (x + x'; y + y') + (x", y")$$
$$= [(x, y) + (x', y')] + (x", y")$$

*Donc la loi + sur* $\mathbb{R}^2$ *est associative.* $(O_{\mathbb{R}^2} = (0, 0))$ *est l'élément neutre. On a :*

$$-(x, y) = (-x, -y) \ ; \ \forall (x, y) \in \mathbb{R}^2$$

$$\begin{aligned}(x, y) + (x', y') &= (x + x', y + y') \\ &= (x' + x, y' + y) \\ &= (x', y') + (x, y) \quad \forall (x, y); (x', y') \in \mathbb{R}^2\end{aligned}$$

*La loi + est commutative dans* $\mathbb{R}^2$, *c-à-d* $(\mathbb{R}^2, +)$ *est un groupe abélien.*
$(\mathbb{N}, +)$ *n'est pas un groupe, car les éléments de* $\mathbb{N}^*$ *ne sont pas symétrisables.*

**structure de sous groupe**

**Définition 2.19.**
*Soit* $(G, *)$ *un groupe non vide, une partie* $H \subset G$ *est un sous groupe de G si :*

- $H$ *est stable par* $*$
- $H$ *muni de la loi induite par* $*$ *est un groupe.*

**Proposition 2.7.**
*Soit* $(G, *)$ *un groupe. Une partie* $H \subset G$ *est un sous groupe de G si :*

$$(I) \Leftrightarrow \begin{cases} 1)\ e \in H \ (l'élément\ neutre \in H) \\ 2)\ Pour\ tout\ x, y \in H \ ; \ x * y \in H \ (H\ est\ stable\ pour\ *) \\ 3)\ Pour\ tout\ x \in H\ son\ symétrique\ x' \in H \end{cases} \tag{2.1}$$

$$(II) \Leftrightarrow \begin{cases} 1)\ e \in H \ (l'élément\ neutre \in H) \\ 2)\ \forall (x, y) \in H^2 \ ; \ x * y' \in H \quad (où\ y'\ désigne\ le\ symétrique\ de\ y\ dans\ G) \end{cases} \tag{2.2}$$

**Démonstration 7.**
*montrons que H est un sous groupe de* $(G, *) \Rightarrow (I)$
*H est un sous groupe de* $(G, *)$. *Si H est un sous groupe de* $(G, *)$, *alors la proprieté 2 de* $(I)$ *est bien verifiée.*
*Notons* $e_H$ *l'élément neutre de H pour loi induite par* $*$ *dans H. On a :*

$$e_H * e = e_H = e_H * e_H$$

*D'autre part, dans un groupe tout élément a est simplifiable, c-a-d si :*

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

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

*alors :*

$$x = y$$

*Cela se déduit du fait que a est symétrisable et associative.*

$$a * x = a * y \Leftrightarrow a' * (a * x) = a' * (a * y)$$

$$\Leftrightarrow \underbrace{(a' * a)}_{=e} * x = \underbrace{(a' * a)}_{=e} * y$$

$$\Leftrightarrow e * x = e * y$$

$$\Leftrightarrow x = y$$

$\longrightarrow$ *On en déduit que* $e = e_H \in H$. *Ce qui montre* 1) *de* $(I)$
*Soit* $x \in H$, *notons* $x'_H$ *le symétrie de* $x$ *par la loi induite par* $*$ *dans* $H$. *On a :*

$$x'_H * x * x' = e * x' = x'$$

*d'autre part :*

$$x'_H * x * x' = x'_H * e = x'_H$$

*Donc :*

$$x' = x'_H \in H$$

*d'où* 3) *de* $(I)$.
$\mapsto$ *Montrons maintenant que* $(I) \Rightarrow$ $H$ *est un sous groupe de (G,*)*
*D'après* 1) *de* $(I)$ $H$ *est une partie non vide de* $G$. $H$ *est stable pour* $*$ *d'après* 2) *de* $(I)$.
*La loi induite par* $*$ *dans* $H$ *est associative, car elle est déja associative dans* $G$. *On a :*

$$e \in H \text{ et } x * e = e * x = x \quad \forall x \in H$$

*donc est l'élément neutre de* $H$.
*Soit* $x \in H$, *d'après* 3) *de* $(I)$ *on a :*

$$x' \in H \text{ et } x * x' = x' * x = e$$

*Donc* $x'$ *est le symétrique de* $x$ *dans* $H$.

**Exemple 2.23.**
$(\mathbb{R}_+^*, \times)$ *est un sous groupe de* $(\mathbb{R}^*, \times)$.

- $1 \in \mathbb{R}_+^*$
- $x, y \in \mathbb{R}_+^*$, *alors* $x \times \frac{1}{y} = \frac{x}{y} > 0 \Rightarrow x \times \frac{1}{y} \in \mathbb{R}_+^*$.
- $(U, \times)$ *est un sous groupe de* $(\mathbb{C}^*, \times)$
  $U = \{z \in \mathbb{C};\ |z| = 1\}$ *cercle de centre 0 et de rayon 1.*
- $|1| = 1 \Rightarrow 1 \in U$.
- $z, z' \in U$, *cád :*

$$|z| = 1 \text{ et } |z'| = 1 \quad |zz'| = |z||z'| = 1 \times 1 = 1$$

$$\Rightarrow \ zz' \in U \ z \in U; |\frac{1}{z}| = \frac{1}{|z|} = \frac{1}{1} = 1 \Rightarrow \frac{1}{z} \in U$$

- *Soit :*

$$f_{a,b} \ : \ \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto ax + b$$

*et* $F = \{f_{a,b};\ a \in \mathbb{R}^*\ ,\ b \in \mathbb{R}\}$ *est un groupe muni de la loi* $\circ$ .
*On verifie que* $F$ *est un sous groupe de* $(B_{ij}(\mathbb{R}); \circ)$, $B_{ij} = \{f \ : \ \mathbb{R} \longrightarrow \mathbb{R}\ ;\ f \text{ est bijective}\}$
*On a :*

$$Id(x) = 1 \times x + 0 \Rightarrow Id \in F$$

*Soient* $f, g \in F$ *alors :*

$$f(x) = ax + b$$

*et*

$$g(x) = cx + d$$
$$(avec\ a; c \in \mathbb{R}^*)\ et\ b, d \in \mathbb{R}$$
$$g \circ f(x) = g(f(x)) = g(ax + b)$$
$$= c(ax + b) + d$$
$$= cax + cb + d$$

*or on a :* $ca \in \mathbb{R}^*\ ;\ cb + d \in \mathbb{R}$

$$\Rightarrow g \circ f \in F$$

*Soit :*

$$f \in F\ ,\ \exists a \in \mathbb{R}^*\ ,\ \exists b \in \mathbb{R}/f(x) = ax + b\ \forall x \in \mathbb{R}$$
$$y \in f(x) \Leftrightarrow y = ax + b$$
$$\Leftrightarrow x = \frac{y - b}{a}$$
$$\Leftrightarrow \frac{1}{a}y - \frac{b}{a} = f(y) \quad \forall y \in \mathbb{R}$$
$$\Rightarrow f^{-1} \in F$$

**Proposition 2.8.**
*L'intersection de 2 sous groupe* $H$ *et* $K$ *d'un groupe* $G$ *est un sous groupe.*

**Démonstration 8.**
*On a :*

$$e \in H \text{ et } e \in K \Rightarrow e \in H \cap K$$

*Si* $x, y \in H \cap K$

$$\Rightarrow x, y \in H \text{ et } x, y \in K$$
$$\Rightarrow x * y \in H \text{ et } x * y \in K$$
$$\Rightarrow x * y \in H \cap K$$

*Si* $x \in H \cap K$

$$\Rightarrow x \in H \text{ et } x \in K$$
$$\Rightarrow x' \in H \text{ et } x' \in K$$
$$\Rightarrow x' \in H \cap K$$

*Conclusion :*

$$H \cap K \text{ est un sous groupe de } (G, *)$$

**Un sous groupe engendré**

**Définition 2.20.**
*Soit $A$ une partie d'un groupe $(G,*)$, il existe des sous groupes de $G$ qui contient $A$ (exp : $G$ lui même)*
*L'intersection de ces groupes est encore un sous groupe de $G$ et contient $A$.*
*Le sous groupe intersection est donc le plus petit de touts les sous groupes de $G$ contenant $A$.*
*On dit que c'est les sous groupe engendré par $A$.*
*On le note $< A >= \cap H$. $H$ sous groupe $A \subset H$.*

$$< A > \text{ est le plus petit sous groupe contenant } A$$

*càd :*
*si $H$ est un sous groupe de $(G,*)$ et $A \subset H$ alors $< A > \subset H$. $< A >$ est un sous groupe.*
*$A \subset < A >$, si $H$ est un sous groupe de $G$ et $A \subset H \Rightarrow < A > \subset H$*

**Remarque 2.9.**
$A = \emptyset$ ; $< A >= \{e\}$ *En effet :*
$\emptyset \subset \{e\}$,

$$\text{qui est un sous groupe } \Rightarrow < \emptyset > \subset \{e\}$$

*d'autre part*

$$< \emptyset > \text{ est un sous groupe } < A >$$

*Si $H =< A >$,alors $A$ s'appelle une partie génératrice de $H$.*

**Proposition 2.9.**
*Soit $A$ une partie non vide d'un groupe $(G,*)$*

$$< A >= \{a_1 * a_2 * \ldots * a_p \ ; \ p \in \mathbb{N} \ ; \ a_i \in A \cup A'\}$$

*où $A'$ désigne l'ensemble formé par les symetriques de $A$.*

**Démonstration 9.**
*On pose*

$$H = \{a_1 * a_2 * \ldots \times a_p \ ; \ p \in \mathbb{N} \ ; \ a_i \in A \cup A'\}$$

*vérifiant que $H$ est un sous groupe :*
*$H$ est non vide donc $H$ contient au moins un élément $x \in G$.*

$$p = 2 \ ; \ a_1 = x \ ; \ a_2 = x' \Rightarrow a_1 * a_2 = e \in H$$

*Soient $x, y \in H$ :*

$$\exists (a_i)_{i=1}^{p} \subset A \cup A' / x = a_1 * a_2 * \ldots * a_p \ ; \ \exists (b_i)_{i=1}^{q} \subset A \cup A' / x = b_1 * b_2 * \ldots * b_p$$

*On pose :*

$$C_i = a_i \ ; \ si \ \ 1 \leq i \leq p \ et \ C_{p+i} = b_i \ si \ \ 1 \leq i \leq q$$

*On a :*

$$(C_i)_{i=1}^{p+q} \subset A \cup A' / \ x * y = a_1 * a_2 * \ldots * a_p$$
$$= C_1 * C_2 * \ldots * C_p * C_p + 1 * \ldots * C_{p+q} \in H$$

*Ce qui implique que $H$ est stable par loi $*$*

$$x = a_1 * a_2 * \ldots * a_p \Rightarrow x' = a'_p * a'_{p-1} * \ldots * a'_1$$

*On a :*

$$a_i \in A \cup A' \Rightarrow a'_i \in A \cup A'. \text{ Donc } x' \in H$$

*Donc $H$ est stable par passage à l'élément symétrique.*
*Conclusion : $H$ est un sous groupe de $G$.*
*Si $a \in A$, On prend*

$$a_1 = a \ ; \ a_2 = e \Rightarrow a = a_1 * a_2 \in H$$

*Donc $A \subset H$, et par suite $< A > \subset H$.*
*D'autre part :*

$$\begin{aligned} A \subset < A > &\Rightarrow A' \subset < A > \\ &\Rightarrow A \cup A' \subset < A > \\ &\Rightarrow H \subset < A > \end{aligned}$$

*d'où :*

$$H = < A >$$

**Exemple 2.24.**
*Soit $G = \mathbb{Z}$ muni de l'addition usuelle.*
*$A = \{2\}$. $< A >= 2\mathbb{Z}$. En effet $2\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$*

$$\begin{aligned} 2 = 2 \times 1 \in 2\mathbb{Z} &\Rightarrow < A > \subset 2\mathbb{Z} \\ 2 \in A &\Rightarrow 2 \in < A > \\ &\Rightarrow 2k = \underbrace{2 + 2 + \ldots + 2}_{k \text{ fois}} \in < A > \end{aligned}$$

*donc : $2\mathbb{Z} \subset < A >$, conclusion :*

$$< A >= 2\mathbb{Z}$$

*Le sous groupe engendré par :*

$$A = \{4; 16\} \text{ est } < A >= 4\mathbb{Z}$$

*Le sous groupe engendré par :*

$$A = < a; b > \in \mathbb{Z}$$

*est :*

$$< A >= pgcd(a; b)$$

**Morphisme de groupes**

**Définition 2.21.**
*Soient $(E, *)$ et $(F, \perp)$ deux ensembles menu des lois de composition interne $*$ et $\perp$*
*On appelle morphisme de $(E, *)$ dans $(F, \perp)$ une application $\varphi$ : $E \longrightarrow F$ telle que :*

$$\varphi(x * y) = \varphi(x) \perp \varphi(y)$$

**Exemple 2.25.**

- *l'application* $x \mapsto ln(x)$ *est un morphsime de* $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$.
- *l'application* $z \mapsto \overline{z}$ *est un morphisme de* $(\mathbb{C}, \times) \to (\mathbb{C}, \times)$.
- *Un morphisme d'un ensemble vers lui même muni de la même loi de composition interne est appelé endomorphisme.*
- *Un morphisme bijective est appelé isomorphisme.*
- *Un endomorphisme bijective est appelé automorphisme.*

**Proposition 2.10.**
*L'ensemble des metamorphisme de* $(E, *)$ *est un sous groupe de* $(B_{ij}(E), \circ)$ *notée* $Aut(E)$

*Démonstration.*

- Soit :
$$Id_E \ : \ E \longrightarrow E$$
$$x \longmapsto x$$
$$Id_E(x * y) = x * y = Id_E(x) * Id_E(y) \ \ \forall x; y \in E$$
donc $Id_E \in Aut(E)$.

- Soient :
$$\begin{aligned} \varphi, \psi \in Aut(E) \ . \ \ \psi \circ \varphi(x * y) &= \psi(\varphi(x * y)) \\ &= \psi(\varphi(x) * \varphi(y)) \\ &= \psi(\varphi(x)) * \psi(\varphi(y)) \\ &= \psi \circ \varphi(x) * \psi \circ \varphi(y) \ \ \forall x, y \in E \end{aligned}$$

- Soit :
$$\psi \in Aut(E) \ \ \psi^{-1}(x * y) = \psi^{-1}(x) * \psi^{-1}(y)$$
On a :
$$\begin{aligned} \psi(\psi^{-1}(x) * \psi^{-1}(y)) &= \psi(\psi^{-1}(x)) * \psi(\psi^{-1}(y)) \\ &= \psi \circ \psi^{-1}(x) * \psi \circ \psi^{-1}(y) \\ &= x * y \end{aligned}$$
Donc :
$$\begin{aligned} \psi^{-1}(x * y) &= \psi^{-1}(x) * \psi^{-1}(y) \\ &\Rightarrow \psi \in Aut(E) \end{aligned}$$
Conclusion : $Aut(E)$ est un sous groupe de $(B_{ij}(E), \circ)$

□

**Proposition 2.11.**
*Soient* $(E, *)$ *et* $(F, \perp)$ *deux groupes d'éléments neutres respectifs* $e_1$ *et* $e_2$ *et* $\varphi$ *un morphisme de* $G_1$ *dans* $G_2$ *alors :*

$$\varphi(e_1) = e_2 \ et \ \varphi(x') = (\varphi(x))'$$

**Démonstration 10.**

$$e_2 \perp \varphi(e_1) = \varphi(e_1) * \varphi(e_1) = \varphi(e_1 * e_1) = \varphi(e_1) \perp \varphi(e_1)$$

*On simplifie et on obtient* $\varphi(e_1) = e_2$.
*Soit :*

$$x \in G_2 \quad \varphi(x') \perp \varphi(x) = \varphi(x' * x) = \varphi(e_1) = e_2$$

*Donc :*

$$\varphi(x') = (\varphi(x))'$$

**Noyau d'un morphisme de groupes**

**Définition 2.22.**
*Noyau d'un morphisme de groupes :*
*Soient* $(G_1, *)$ *et* $(G_2, \perp)$ *deux groupes d'éléments neutres respectifs* $e_1$ *et* $e_2$ *et* $\varphi$ *un morphisme de* $G_1$ *dans* $G_2$. *On appelle noyau de* $\varphi$ *l'ensemble de* $G_1$ *qui ont pour image* $e_2$, *on le note :*

$$Ker\varphi = \{x \in G_1 \ ; \ \varphi(x) = e_2\} = \varphi^{-1}(\{e_2\})$$

**Théorème 2.1.**
*Pour tout morphisme* $\varphi$ *du groupe* $G_1$ *dans le groupe* $G_2$, *on a :*

1. $ker\varphi$ *est un sous groupe de* $G_1$.
2. $ker\varphi = \{e_1\} \Leftrightarrow \varphi$ *est injective.*

**Démonstration 11.**

- *On a* $\varphi(e_1) = e_2$, *ce qui implique que* $e_1 \in ker\varphi$.
  *Soient* $x, y \in ker\varphi$ *on a :*

$$\begin{cases} \varphi(x) = e_2 \\ \varphi(y) = e_2 \end{cases} \tag{2.3}$$

  *Donc :*

$$\varphi(x * y) = \varphi(x) \perp \varphi(y) = e_2 \perp e_2 = e_2$$

  *Ceci implique que* $x * y \in ker\varphi$.
  *Et soit* $x \in ker\varphi$ *on a* $\varphi(x) = e_1$. *D'autre part, on sait que :*

$$\varphi(x') = (\varphi(x))' \Rightarrow \varphi(x') = (\varphi(x))' = e_2' = e_2$$

  *Conclusion : ceci implique que* $x' \in ker\varphi$
  $ker\varphi$ *est un sous groupe de* $G_1$.

- $(\Rightarrow)$ *Soient* $x, y \in G_1$ *tel que :* $\varphi(x) = \varphi(y)$
  *Ceci implique que :*

$$\varphi(x) \perp (\varphi(y))' = \varphi(x) \perp \varphi(y') = \varphi(x * y') = e_2$$

  *On obtient :*

$$x * y' \in ker\varphi = \{e_1\}$$
$$\Rightarrow x * y' = e_1$$

$$\Rightarrow x = y$$

*Conclusion : $\varphi$ est injective.*
*($\Leftarrow$) D'abord on a :*

$$\{e_1\} \subseteq ker\varphi$$

*Soit $x \in ker\varphi$. On a :*

$$\varphi(x) = e_2 = \varphi(e_1)$$

*Comme $\varphi$ est injective donc $x = e_1$, d'où*

$$ker\varphi = \{e_1\}$$

**Exemple 2.26.**
*L'application $\varphi$ : $x \to e^{ix}$ est un morphisme de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.*

$$\varphi(x+y) = e^{i(x+y)} = e^{ix} \times e^{iy} = \varphi(x) \times \varphi(y) \ ; \ \forall x, y \in \mathbb{R}$$
$$ker\varphi = \{x \in \mathbb{R} / \varphi(x) = 1\}$$
$$= \{x \in \mathbb{R} / e^{ix} = 1\}$$
$$= \{2k\pi \ ; \ k \in \mathbb{Z}\}$$
$$= 2k\mathbb{Z}$$

*qui est un sous groupe de $(\mathbb{R}, +)$*

### L'image d'un morphisme de groupes

**Définition 2.23.**
*L'image d'un morphisme de groupes :*
*Soient $(G_1, *)$ et $G_2$, $\perp$ deux groupes et $\varphi$ un morphisme de $G_1$ dans $G_2$.*
*On appelle image de $\varphi$ l'ensemble des éléments de $G_2$ qui ont un antécédant dans $G_1$, on le note :*

$$Im\varphi = \{y \in G_2 \ ; \ \exists x \in G_1 \ ; \ y = \varphi(x)\} = \{\varphi(x) \ ; \ x \in G_1\} = \varphi(G_2)$$

**Théorème 2.2.**
*Pour tout morphisme $\varphi$ du groupe $(G_1, *)$ dans le groupe $(G_2, \perp)$, on a :*

1. *$Im\varphi$ est un sous groupe de $G_2$.*
2. *$Im\varphi = G_2 \Leftrightarrow \varphi$ est surjective.*

**Démonstration 12.**
1) *On a :*

$$e_2 = \varphi(e_1) \Rightarrow e_2 \in Im\varphi$$

*Soient :*

$$y_1, y_2 \in Im\varphi$$

*$\exists x_1, x_2 \in G_1$ tel que*

$$\varphi(x_1) = y_1 \text{ et } \varphi(x_2) = y_2$$

*Par suite :*

$$y_1 \perp y_2 = \varphi(x_1) \perp \varphi(x_2) = \varphi(x_1 * x_2) \Rightarrow y_1 \perp y_2 \in Im\varphi$$

2) *Soit* $y \in Im\varphi$, *donc :*

$$\exists x \in G_1/\varphi(x) = y$$

*On a :*

$$y' = (\varphi(x))' = \varphi(x')$$

*Donc :*

$$y' \in Im\varphi$$

*conclusion* $Im\varphi$ *est un sous groupe de* $G_2$.

**Exemple 2.27.**
*L'application* $\varphi : x \to e^{ix}$ *est un morphisme de groupe de* $(\mathbb{R}, +)$ *dans* $(\mathbb{C}^*, \times)$

$$\begin{aligned} Im\varphi &= \{z \in \mathbb{C}^*/\exists x \in \mathbb{R}; \varphi(x) = z\} \\ &= \{z \in \mathbb{C}^*/\exists x \in \mathbb{R}; e^{ix} = z\} \\ &= \{z \in \mathbb{C}/|z| = 1\} \text{ est le cercle unité} \end{aligned}$$

*donc,* $\varphi$ *n'est pas surjective.*

### 2.3.2 Structure d'anneaux

**Définition 2.24.**
*On appelle anneau un ensemble* $A$ *muni de deux lois de composition internes notées respectivement* $+$ *et* $\times$ *telle que :*

- $(A, +)$ *est un groupe abélien,l'élément neutre est noté* $O_A$.
- *la loi* $\times$ *est associative.*
- $A$ *possède un élément neutre (ou élément unité) pour la loi* $\times$ *noté* $1_A$.
- *La loi* $\times$ *est distributive par rapport à loi* $+$, *c'est à dire :*

$$a(b+c) = ab + ac \text{ et } (b+c)a = ba + ca \quad \forall a, b, c \in A$$

**Exemple 2.28.**
$(\mathbb{Z}, +, \times)$ ; $(\mathbb{Q}, +, \times)$ ; $(\mathbb{R}, +, \times)$ *et* $(\mathbb{C}, +, \times)$ *sont des anneaux.*
▪ *Si* $a, b$ *sont deux éléments qui commuttent* $(a \times b = b \times a)$ *alors :*
$\forall n \in \mathbb{N}$ *On a :*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k \; a^{n-k} \; b^k \; ; \; C_n^k = \frac{n!}{k!(n-k)!}$$

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1} \; b^k \; ; \; \forall n \in \mathbb{N}^*$$

*En particulier :*

$$1 - x^n = (1-x) \sum_{k=0}^{n-1} x^k = \sum_{k=0}^{n-1} x^k \; (1-x)$$

**Structure de sous anneau**

**Définition 2.25.**
*Une partie $B$ d'un anneau $A$ est un sous anneau.*

- $1_A \in B$
- $\forall (x,y) \in B^2 \ ; \ x-y \in B$
- $\forall (x,y) \in B^2 \ ; \ x \times y \in B$

**Morphisme d'anneau**

**Définition 2.26.**
*On appelle morphisme d'anneau une application. $\varphi \ : \ (A,+,\times) \to (A',+,\times)$ telle que :*

- $\varphi(1_A) = 1'_A$
- $\forall (x,y) \in A^2 \ ; \ \varphi(x+y) = \varphi(x) + \varphi(y)$
- $\forall (x,y) \in A^2 \ ; \ \varphi(x \times y) = \varphi(x) \times \varphi(y)$

**Exemple 2.29.** *L'application $z \to \bar{z}$ est un automorphisme de l'anneau $(\mathbb{C},+,\times)$*

### 2.3.3 Structure de corps

**Définition 2.27.**
*On appelle un corps un anneau (toujours supposé commutatif) non réduit à $\{0\}$ dont tout élément non nul est inversible.*

**Structure de sous corps**

**Définition 2.28.**
*Une partie $L$ d'un corps $K$ est un sous coprs de $K$ :*

1. $L \diagdown \{0\} \neq \emptyset$
2. $\forall x,y \in L^2 \ ; \ x-y \in L$
3. $\forall (x,y) \in L \times L^* \ ; \ xy^{-1} \in L$

### Morphisme de corps

**Définition 2.29.**
*On appelle morphisme de corps une application* $\varphi : K \to K$ *qui est un morphisme pour la loi* $+$ *et* $\times$*. Autrement dit :*

1. $\varphi(1_K) \neq 0$
2. $\forall (x, y) \in K^2 \ : \ \varphi(x + y) = \varphi(x) + \varphi(y)$
3. $\forall (x, y) \in K^2 \ : \ \varphi(x \times y) = \varphi(x) \times \varphi(y)$
   *On a forcément* $\varphi(1_K) = 1_{K'}$ *car* $\varphi$ *est un morphisme de groupe de* $(K, \times)$ *dans* $(K', \times)$

# Chapitre 3

# Arithmétique

## 3.1 Division euclidienne

**Définition 3.1.**
*Soient $a$ et $b \in \mathbb{Z}$, s'il existe $n \in \mathbb{Z}$ tel que $a = nb$.*
*On dit $a$ est multiple de $b$. On dit que $b$ est un diviseur de $a$.*

**Exemple 3.1.**
*$a = 9$ $b = 3$ $a = 3b$ / 9 est un multiple de 3 et 3 est un diviseur de 9.*

**Notation :**
L'ensemble des multiples de $a$ est noté :

$$a\mathbb{Z} = \{ak / k \in \mathbb{Z}\}$$

L'ensemble des diviseurs de $a$ est noté :

$$D(a) = \{b \ ; \ \exists k \in \mathbb{Z} \ ; \ a = kb\}$$

### 3.1.1 Division euclidienne dans $\mathbb{Z}$

**Théorème 3.1.**
*Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

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

**Démonstration 13.**
*l'unicité du couple $(q, r)$*
*Si*

$$a = bq + r = q'b + r' \text{ avec } q, q' \in \mathbb{Z} \quad r, r' \in \mathbb{N}$$

*on écrit donc :*

$$(q - q')b = r' - r \text{ et } 0 \leq r < b \text{ et } 0 \leq r' < b$$

*D'autre part :*

$$-b < -r' \leq r - r' \leq r < b$$

*Par suite :*

$$-b < (q' - q)b < b$$

*comme :*

$$b > 0 \quad -1 < q' - q < 1$$

*donc*

$$q - q' \in \mathbb{Z}$$

*Ceci implique que*

$$q - q' = 0$$

*donc*

$$q = q'$$

*et par suite*

$$r = r'$$

*Existance : Soit* $q = E(\frac{a}{b})$.
*On a :*

$$q \leq \frac{a}{b} < q + 1$$

*Ceci implique que :*

$$0 \leq \frac{a}{b} - a < 1$$

*donc* $0 \leq a - bq < b$. *On pose* $r = a - bq$. *On a bien :*

$$a = bq + r \ avec \ 0 \leq r < b$$

*Ce qui conclut la demonstration.*

**Exemple 3.2.**
$a = 6789 \quad b = 34 \qquad a = 34 \times 199 + 23$

## 3.2 L'algorithme d'euclide

**Théorème 3.2.**
*L'ensemble des diviseurs communs de 2 entiers relatifs.*
*a et b est l'ensemble d'un unique entier positif appelé PGCD de a et b est noté :*

$$a \wedge b \ ; \ ou \ pgcd(a, b) \ ; \ D(a) \wedge D(b) = D(a \wedge b)$$

**Remarque 3.1.**
*Soient* $a, b \in \mathbb{Z}$, *alors :*

$$D(a) = \{\mathbb{Z}\} \Leftrightarrow a = 0$$

$$D(a) = D(b) \Leftrightarrow a = b \ ou \ a = -b$$

$$D(-a) = D(a)$$

**Démonstration 14.**
*Dabord, on suppose que* $0 \leq b \leq a$
*Si*

$$a = 0 \Rightarrow b = 0$$

*D'après la remarque précédente on a :*

$$D(a) \wedge D(b) = D(0) \wedge D(0) = \mathbb{Z} \wedge \mathbb{Z} = \mathbb{Z} = D(0)$$

*donc :*

$$0 \wedge 0 = pgcd(0;0) = 0$$

*$\underline{a > 0}$ alors on pose :*

$$r_0 = a \text{ et } r_1 = b$$

$\longrightarrow$ *si $r_1 = 0$, on a donc :*

$$D(a) \cap D(b) = D(r_0) \cap D(r_1) = D(r_0) \cap \mathbb{Z} = D(r_0) \Rightarrow \ a \wedge b = r_0$$

*$\underline{Si\ r_1 \neq 0}$ :*
*Par division euclidienne, $\exists!(q_2; r_2) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$r_0 = q_2 r_1 + r_2 \ ; \ 0 \leq r_2 < r_1 \leq r_0$$

*Il est clair que :*

$$D(r_0) \cap D(r_1) = D(r_1) \cap D(r_2)$$

*$\underline{Si\ r_2 = 0}$, on a donc :*

$$D(a) \wedge D(b) = D(r_0) \cap D(r_1) = D(r_1) \cap \mathbb{Z} = D(r_1)$$

*Donc :*

$$a \wedge b = r_1$$

*$\underline{r_2 \neq 0}$ :*
*Par la division euclidienne, $\exists!(q_3; r_3) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$r_1 = q_3 r_2 + r_3. \quad 0 \leq r_3 < r_2 < r_1 \leq r_0$$

*$\underline{Si\ r_3 = 0}$ :*
*donc on a :*

$$D(r_1) \cap D(r_2) = D(r_2) \cap D(r_3) = D(r_2) \cap \mathbb{Z} = D(r_2)$$

$$\Longrightarrow a \wedge b = r_1 \wedge r_2 = r_1 \wedge r_3 = r_2$$

*On continue cette procédure tant que le reste est non nulle, on obtient une suite de reste strictement decroissante. Comme il n'existe pas une suite d'entiers strictement décroissante minorée alors elle est necessairement au bout d'un nombre fini d'étapes on oboutit à un reste nul $r_{n+1} = 0$ et $r_n \neq 0$ de plus :*

$$D(a) \cap D(b) = D(r_0) \cap D(r_1) = D(r_1) \cap D(r_2) = \ldots = D(r_n) \cap D(r_n + 1) = D(r_n) \ ; \ r_n < \ldots < r_2 < r_1 < r_0$$

*$r_n$ est l'unique entier posistif tel que :*

$$D(a) \cap D(b) = D(r_n)$$

*$r_n$ s'appelle le plus grand commun diviseur de $a$ et $b$ et noté :*

$$pgcd(a, b) = a \wedge b = r_n$$

*Si $a, b \in \mathbb{Z}$ quelconques :*

$$D(a) \cap D(b) = D(|a|) \cap D(|b|) = D(|a| \wedge |b|) \quad a \wedge b = |a| \wedge |b| = pgcd(a, b)$$

### 3.2.1 Caractérisation intuitive du pgcd

$a \wedge b$ est un diviseur commun de $a$ et $b$, et tout diviseur commun de $a$ et $b$ est un diviseur de $a \wedge b$

$$(si\ n/a\ et\ n/b \Rightarrow\ n \in D(a) \cap D(b) = D(a \wedge b) = n/a \wedge b)$$

**Exemple 3.3.**
$a = -240\ ;\ b = 50$

$$a \wedge b = pgcd(-240, 50) = pgcd(240, 50)$$

*On pose :*

$$r_0 = 240\ et\ r_1 = 50\ \ r_0 = 4 \times 50 + 40.\ \ r_2 = 40$$

$$50 = 40 \times 1 + 10.\ \ r_3 = 10.\ \ 40 = 4 \times 10 + 0.\ \ r_4 = 0$$

$$pgcd(240, 50) = 10$$

Conclusion : Le pgcd de deux entiers non nuls est unique et qui est le dernier reste non nul de l'algorithme d'Euclide.

**Théorème 3.3.**
*soient $(a, b) \in \mathbb{Z}^2$ un entier est la somme d'un multiple de a et d'un multiple de b est un multiple de leur pgcd. Autrement dit :*

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}\ \ avec\ \ \mathbb{Z} + b\mathbb{Z} = \{au + bv\ ;\ u, v \in \mathbb{Z}^2\}$$

**Démonstration 15.**
*On a $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$ D'après (exo 1 , série n4)*

$$\exists n \in \mathbb{N}\ ;\ a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$$

*On verifie que $n = a \wedge b$, càd :*

$$D(a) \wedge D(b) = D(n)\ a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$$

*donc :*

$$\exists k \in \mathbb{Z}/a = nk \Rightarrow n/a$$

*de même :*

$$b = a \times 0 + b \times 1 \in a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}.\ \exists k' \in \mathbb{Z}/b = nk' \Rightarrow n/b$$

*Donc :*

$$n \in D(a) \cap D(b) = D(a \wedge b) \Rightarrow D(n) \subset D(a) \wedge D(b)$$

$$\Rightarrow d/n\ ,\ \exists m \in \mathbb{Z}/n = md$$

*et on a :*

$$n/a \Rightarrow\ /\ \exists k \in \mathbb{Z}\ /\ a = kn$$

*d'où :*

$$a = k(md) = kmd = k'd = k'd\ ,\ k' \in \mathbb{Z}$$

*d'où $d/a$. D'autre part, on a :*

$$n = n \times 1 \in n\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

*donc*

$$\exists u, v \in \mathbb{Z} \ / \ n = au + bv$$

*Si* $d/a$ *et* $d/b$, *alors*

$$\exists k, k' \in \mathbb{Z} \ , \ a = kd \ ; \ b = k'd$$

*Par suite :*

$$n = (ku + k'v)d = d/n$$

*Ce qui implique que*

$$D(a) \cap D(b) \subset D(n) \ d'où \ D(a) \wedge D(b) = D(n)$$

*Comme* $n \geq 0$, *donc :*

$$n = pgcd(a, b) = a \wedge b$$

*Conclusion :*

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

**Remarque 3.2.**
*Si*

$$d = a \wedge b \ alors : \exists u, v \in \mathbb{Z}/d = au + bv$$

*deux entiers* $a$ *et* $b$ *sont dits premiers entre eux si*

$$a \wedge b = 1$$

**Théorème 3.4.**
*Deux entiers* $a$ *et* $b$ *sont premiers entre eux si et seulement si il existe* $u, v \in \mathbb{Z}$ *tels que :*

$$au + bv = 1 \ (\textbf{\textit{Bézout}})$$

**Démonstration 16.**
*(⇒) Supposons que* $a \wedge b = 1$. *On a :*

$$(a \wedge b) \times 1 \in (a \wedge b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \ (Theoréme \ precedent)$$

*Ceci qui implique que :*

$$\exists u, v \in \mathbb{Z}/au + bv = 1$$

*(⇐) Supposons qu'il existe* $u, v \in \mathbb{Z}$ *tel que :*

$$au + bv = 1$$

*Vérifions que :*

$$a \wedge b = 1$$

*Soit* $d \in \mathbb{Z}$ *tel que :*

$$d/a \ et \ d/b$$

*Donc :*

$$\exists k, k' \in \mathbb{Z} \ tel \ que \ a = kd \ et \ b = k'd$$

*Par suite :*

$$\begin{aligned} au + bv = 1 &= kdu + k'dv \\ &= d(ku + k'v) = 1 \Rightarrow d/1 \end{aligned}$$

*et donc*

$$D(a) \cap D(b) \subset D(1)$$

*On a toujours*

$$D(1) \subset D(a) \cap D(b)$$

*d'où :*

$$D(a) \subset D(b) = D(1)$$

*Ce qui montre que :*

$$a \wedge b = 1$$

**Remarque 3.3.**

$$au + bv = d \Rightarrow d$$

*est un multiple de* $a \wedge b$.
*Par contre*

$$au + bv = 1 \text{ entraine que } : \ a \wedge b = 1$$

*càd :*

$$a \text{ et } b \text{ sont premiers entre eux}$$

**Théorème 3.5.**
*Soient a,b et c trois entiers, si :* $a/bc$ *et* $a \wedge b = 1 \Longrightarrow a/c$ *(Gauss)*

**Démonstration 17.**
*On a* $a \wedge b = 1$ *donc :*

$$\exists u, v \in \mathbb{Z}, au + bv = 1$$

*multiplications par c, on obtient :*

$$cau + cbv = c$$

*D'autre part on a* $a/bc$ *donc :*

$$\exists k \in \mathbb{Z} \text{ tel que } bc = ak$$

*Par suite :*

$$cau + kav = c \ \ a(cu + bv) = c$$

*donc :*

$$a/c$$

**Théorème 3.6.** *(Caractérisation du pgcd)*
*Soient* $a, b \in \mathbb{Z}$ *et soit* $d \in \mathbb{N}$. *d est un pgcd de a et b si, et seulement si :*
$\exists (a', b') \in \mathbb{Z}^2$ *tel que :*

$$\begin{cases} a = a'd \\ b = b'd \end{cases} \quad et \quad a' \wedge b' = 1 \tag{3.1}$$

**Démonstration 18.**
*Supposons que* $d = a \wedge b$
*si* $d = 0$ *donc :*

$$D(d) = D(a) \cap D(b) = \mathbb{Z} \Rightarrow D(a) = \mathbb{Z}$$

*et :*

$$D(b) = \mathbb{Z} \Rightarrow a = 0$$

*et*

$$b = 0$$

*donc si* $d = 0$ *alors*

$$a = 0 = b$$

*On suppose que* $d \neq 0$. *On a*

$$d/a \text{ et } d/b$$

*donc :*

$$\exists a', b' \in \mathbb{Z} \ / \ a = a'd \quad b = b'd$$

*D'autre part :*

$$\exists u, v \in \mathbb{Z} \quad au + bv = d$$
$$\Leftrightarrow \quad a'du + b'dv = d$$
$$\Leftrightarrow \quad a'u + b'v = 1$$

*Ce qui montre d'après* ***Bézout***

$$a' \wedge b' = 1$$

*(⇐) On a clairement :*

$$D(d) \subset D(a) \cap D(b)$$

*D'autre part :*

$$\exists u, v \in \mathbb{Z} \text{ tel que } a'u + b'v = 1$$

*On a donc :*

$$ua'd + vb'd = d$$

*On Obtient :*

$$au + bv = d \quad d \in (a \wedge b)\mathbb{Z}$$

*Ceci implique que*

$$a \wedge b/d$$

*et donc*

$$D(a \wedge b) \subseteq D(d)$$

*D'autre part, on a :*

$$d/a \text{ et } d/b \Rightarrow d/a \wedge b$$
$$\Rightarrow D(d) \subseteq D(a \wedge b)$$

*D'où :*

$$D(d) = D(a \wedge b)$$
$$\Rightarrow \quad d = a \wedge b$$

**Définition 3.2.**
*Soient $a, b \in \mathbb{Z}$ :*
*Le plus petit commun multiple de $a$ et $b$ noté $a \vee b$ est l'unique entier positif verifiant :*

$$a\mathbb{Z} \cup b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

**Définition intuitive**

$$a \vee b \in \mathbb{N}, a \vee b \in a\mathbb{Z} \cap b\mathbb{Z} \; si \; m \in a\mathbb{Z} \cap b\mathbb{Z}$$

alors :

$$a \vee b \geq m$$

**Proposition 3.1.**
*Soient $a, b \in \mathbb{Z}^*$, alors :*

$$(a \wedge b) \times (a \vee b) = |ab|$$

**Démonstration 19.**
*D'après la caractèrisation précédente :*

$$\exists a', b' \in \mathbb{Z} \; / \; a = (a \wedge b)a' \; ; \; b = (a \wedge b)b' \quad avec \; a' \wedge b' = 1$$

*On pose :*

$$m = a'b' \; et \; d = a \wedge b$$

*donc :*

$$a = a'd \; et \; b = bd' \; avec \; a' \wedge b' = 1$$

*On pose*

$$m = |a'b'|d \in \mathbb{N}$$

*On Verifie que :*

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

*On a clairement que :*

$$m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$$

*Soit*

$$n \in a\mathbb{Z} \cap b\mathbb{Z} \; ; \; \exists k, k' \in \mathbb{Z}$$

*tel que :*

$$n = ak \; , \; n = bk' \Leftrightarrow n = a'dk = b'dk'$$

*On simplifie par $d$ alors :*

$$a'k = b'k' \Rightarrow a'/b'k'$$

$$\Rightarrow a'/k'a \Leftrightarrow k' = k"a' \quad (d'après \; Gauss)$$

*Par suite :*

$$n = b'a'dk" \Rightarrow m/n$$

$$\Rightarrow n = mk \in m\mathbb{Z}$$

$$\Rightarrow n \in \mathbb{Z}$$

*donc :*

$$a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$$

*Donc*

$$m = a \vee b$$

**Définition 3.3.**
*Un entier $p > 1$ est dit premier si ses seuls diviseurs positifs sont 1 et lui même.*

### 3.2.2 Décomposition en facteurs simples

**Théorème 3.7.**
*Tout entier $n > 1$ est un produit de facteurs premiers, la décomposition est unique à l'ordre près càd : $\forall n \in \mathbb{N}^* \ \exists p_1; \ldots; p_n \in \mathbb{N}^*$ $p_i$ est premier $\forall i = 1; \ldots; n \ \exists \alpha_1; \ldots; \alpha_n \in \mathbb{N}^*$ tel que :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times; \ldots; p_n^{\alpha_n}$$

**Démonstration 20.**
*On la démontre en utilisant la réccurence pour $n \geq 2$ que tous les entiers de 1 à n admettent une décomposition en facteurs premiers.*
*Le resultat est vrai pour $n = 2$ car 2 est un nombre premier.*
*Supposons que tous les entiers de 1 à n admettent une decomposition en facteurs premier et montrons qu'il en est de même pour $n + 1$*
*si*

$$n + 1 \text{ est un nombre premier}$$

*alors c'est fini.*
*Sinon, on peut écrire :*

$$n + 1 = pq$$

*où p et q sont des entiers naturels strictement inférieurs à $n + 1$.*
*Or par hypothèse de reccurence ces deux entiers admettent une décomposition en facteurs premiers.*
*Et par suite il en est de même pour $n + 1$ ce qui termine le raisonnement par reccurence.*

**Propriété 3.1.**

1. *Dans la pratique, pour savoir si un entier $n \geq 2$ est premier, on cherche à le diviser par tous les entiers premiers qui sont inferieurs $\sqrt{n}$.*
2. *Si p est un nombre premier et n un entier, alors $p/n$ où p est premier avec n.*
3. *Deux nombres premiers distinctes sont premiers entre eux.*
4. *Si un nombre premier divise le produit deux entiers, alors il divise au moins l'un de ces entiers.*
   *Attention : Ce resultat n'est pas valable pour un entier quelconque.*
5. *Si un nombre premier p divise un produit de facteurs premiers alors p et l'un de ces facteurs premiers.*
6. *Un nombre p premier est premiers avec toutes les puissances d'un nombre premier.*

**Démonstration 21.**

1. *On resonne par contraposé*
   *Suppossons que n n'est pas premier et montrons qu'il est divisible par un nombre premier* $p \leq \sqrt{n}$.
   *n n'est pas premier donc :*

$$\{1 < q < n \ , \ q \ premier \ q/n\} \neq \emptyset$$

   *qui admet un élément minimal p.*
   *D'où il existe* $q \in \{2; \ldots; n-1\}$ *tel que* $n = qp$ *necessairement on a :*

$$p \leq q \Rightarrow p^2 \leq qp = n \Rightarrow p \leq \sqrt{n}$$

2. *Si p ne divise pas n.*
   *Alors :*

$$D(p) \cap D(n) = D(1) = \{-1; 1\} \quad a \in D(p) \cap D(n) \Rightarrow d/p$$

   *et*

$$d/n \quad |d| = p \ et \ |d| = p \ (p \ ne \ divise \ pas \ n) \ |d| = 1$$

   *alors :*

$$D(p) \cap D(n) = D(1)$$

3. $p \neq q$ *p et q sont premiers*

$$D(q) \cap D(p) = D(1) \quad d/q \Rightarrow d = \pm p \ ou \ d = \pm q$$

   *et*

$$d/q \Rightarrow d = \pm 1 \ ou \ d = \pm p$$

   *or*

$$p \neq q \ alors \ pgcd = 1$$

   *donc ils sont premiers entre eux.*

4. *Supposons que* $p/n_1 \times n_2 \times \ldots \times n_p$. *Si* $p \nmid n_1$ *d'après la proprieté* $p \wedge n_1 = 1$ *Ceci implique d'après Gauss* $p/n_2 \times \ldots \times n_p$. *On verifie que si*

$$p \nmid n_i; \quad 1 \leq i \leq p-1 \Rightarrow p/n_p$$

5. $n/p_1 \times p_2 \times \ldots \times p_n$ *donc* $p_i$ *sont premiers d'après la propriété (4) :*

$$\exists i \in \{1; \ldots; n\} \quad n/p_i \Rightarrow n = p_i$$

6. *p et q* $p \neq q$ *sont deux nombres premiers alors*

$$p \nmid q \ et \ p \nmid q^\alpha \ d'après \ la \ propriété \ (5) \ et \ d'après \ p \wedge q^\alpha = 1$$

   *donc :*

$$p^n \wedge q^\alpha = 1 \quad \forall \alpha, \beta \geq 1$$

**Corollaire 3.1.**
*Soit $n \geq 2$ et $n \in \mathbb{N}$, si :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n} \text{ avec } p_{i/i=1;\ldots;n} \text{ premiers distincts}$$

*Alors l'ensemble des diviseurs de n est :*

$$\{\pm p_1^{k_1} \times p_2^{k_2} \times \ldots \times p_n^{k_n} \ ; \ 0 \leq k_1 < \alpha_1, \ldots, 0 \leq k_n < \alpha_n\}$$

**Démonstration 22.**
*Si*

$$d = \pm p_1^{k_1} \times p_2^{k_2} \times \ldots \times p_n^{k_n} \ ; \ 0 \leq k_i \leq \alpha_i$$

*alors*

$$d/n$$

*Réciproquement :*
*si $d \in \mathbb{N}/d \geq 2$ $d \nmid n$, d'après le théorème fondamental de l'arithmétique :*

$$d = q_1^{k_1} \times \ldots \times q_r^{k_r}, \ q_i \geq 2 \ / \ i = 1; \ldots; r$$

*sont premiers distincts.*
*Soit $i \in \{1; \ldots; r\}$ on a :*

$$q_i / p_1^{k_1} \times p_2^{k_2} \times \ldots \times p_n^{k_n}$$

*et on a d'après (5)*

$$\exists i \in \{1; \ldots; n\} \ / \ q_i = p_j$$

*On a :*

$$k_i \leq \alpha_j \quad d = q_1^{k_1} \times \ldots \times q_i^{k_i} \times q_{i+1}^{k_i+1} \times \ldots \times q_r^{k_r}$$
$$= q_1^{k_1} \times \ldots \times q_{i-1}^{k_{i-1}} \times q_j^{k_j} \times \ldots \times q_{i+1}^{i+1} \times \ldots \times q_r^{k_r}$$

*Car sinon on aura :*

$$q_i / p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_{j-1}^{\alpha_{j-1}} \times p_{j+1}^{\alpha_{j+1}} \times \ldots \times p_n^{\alpha_n}$$

**Exemple 3.4.**
*determiner les diviseurs de 60 :*
$60 = 2^2 \times 3 \times 5$ *les diviseurs sont 2,$2^2$,3 et 5. Les diviseurs sont :*

$$\{2^{k_1} \times 3^{k_2} \times 5^{k_3} \ ; \ 0 \leq k_1 \leq 2 \ , \ 0 \leq k_2 \leq 1 \ , \ 0 \leq k_3 \leq 1\}$$

## 3.3 Congruence et classes d'équivalence

**Définition 3.4.**
*Soit $n \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z}^2$*
*On dit que a est congrue à b modulo n, et on écrit $a \equiv b[n]$ si n divise $b - a$*
*La relation «modulo n» est une relation d'équivalence :*

- *$a \equiv a[n]$ (la relation «modulo n» est reflexive)*
- *Si $a \equiv b[n]$ alors $b \equiv a[n]$ (la relation «modulo n» est symétrique)*
- *Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (la relation «modulo n» est transitive)*

**Notations et Définition :**

L'ensemble $\bar{a} = \{b \in \mathbb{Z}; a \equiv b[n]\}$ est appelé la classe d'équivalence par la relation «module n». L'ensemble de toute les classes d'équivalences noté :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a}; a \in \mathbb{Z}\}$$

**Proposition 3.2.** *Compatibilité du modulo avec les lois classiques*
*Soit $n \in \mathbb{N}^*$ et $(a, b, c, d) \in (\mathbb{Z}^*)^4$. Alors on a :*

$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d\ [n] \\ ac \equiv bd\ [n] \end{cases}$$

**Démonstration 23.**

- $a \equiv b\ [n] \Leftrightarrow n/b - a, \exists k \in \mathbb{Z}$ *tel que*

  $$b - a = nkc \equiv d\ [n] \Leftrightarrow n/d - c, \exists k' \in \mathbb{Z}$$

  *tel que :*

  $$d - c = nk',\ et\ b - a + d - c = b + d - (a + c) = n(k + k')$$

  *donc*

  $$n/b + d - (a + c)$$

  *Ceci implique :*

  $$a + c \equiv b + d\ [n]$$

- $ac - bd = a(c - d) + ad - bd$

  $$= a(c - d) + d(a - b) = -nk' - nk\ donc\ :\ n/ac - bd$$

  *Ceci implique que :*

  $$ac \equiv bd\ [n]$$

**Remarque 3.4.**

$$a \equiv b\ [n] \Leftrightarrow \bar{a} = \bar{b}$$

*En effet :*
*($\Rightarrow$) Soit $c \in \bar{a}$ On a :*

$$a \equiv b\ [n]\ donc\ c \equiv b\ [n]$$

*Ceci implique :*

$$c \in \bar{b}\ et\ donc\ \bar{a} \subset \bar{b}$$

*de même on a :*

$$\bar{b} \subset \bar{a}$$

*d'où :*

$$\bar{a} = \bar{b}$$

*($\Leftarrow$) On a*

$$a \in \bar{a} \equiv \bar{b}\ donc\ a \in \bar{b}$$

*D'où :*

$$a \equiv b\ [n]$$

Pour tous $a; b \in \mathbb{Z}$. On pose :

$$\bar{a} + \bar{b} = a \bar{+} b \text{ et } \bar{a} \times \bar{b} = a \bar{\times} b$$

"+" et "×" sont bien definies càd si :

$$\begin{cases} \bar{a} = \bar{a'} \\ \bar{b} = \bar{b'} \end{cases} \Rightarrow \begin{cases} \overline{a+b} = \overline{a+b} \\ \overline{ab} = \overline{a'b'} \end{cases}$$

D'après la remarque précédente " + " et "× sont deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

**Propriété 3.2.**

- $(\mathbb{Z}/n\mathbb{Z})$ *est un groupe commutatif.*
- *Si de plus n est premier, alors* $(\mathbb{Z}/n\mathbb{Z})$ *est un corps commutatif.*

**Démonstration 24.**

1. $\bar{0}$ *est l'élément neutre*

$$(\bar{0} + \bar{a} = \overline{0+a} = \bar{a})$$

$(\bar{-a})$ *est l'élément symétrique de* $\bar{a}$

$$(\bar{a} + \bar{-a} = \bar{0})$$

2. $\bar{1}$ *est l'élément neutre de la loi "*$\times$*. Si*

$$\bar{a} \neq \bar{0} \ n \text{ ne divise pas } a$$

*d'après (5)* $n \wedge a = 1$.
*D'après Bezout*

$$\exists u, v \in \mathbb{Z} \text{ tel que } au + nv = 1$$

*Par suite :*

$$\overline{au+nv} = \bar{1} \Leftrightarrow \overline{au} + \overline{nv} = \bar{a}\bar{u} + \bar{n}\bar{v} = \bar{a}\bar{u} + \bar{0}\bar{v} = \bar{a}\bar{u} = \bar{1}$$

*Donc* $\bar{u}$ *est le symétrique de* $\bar{a}$ *par la multiplication.*

**Proposition 3.3.**
$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \ldots; \overline{n-1}\}$

**Démonstration 25.**
*Soit* $a \in \mathbb{Z}$ *par la division euclidienne.*

$$a = qn + r; q \in \mathbb{Z} \ ; \ 0 \leq r \leq n-1$$

*donc :*

$$\bar{a} = \overline{qn} + \bar{r} = \bar{q}\bar{n} + \bar{r} = \bar{q} \times \bar{0} + \bar{r} = \bar{0} + \bar{r} = \bar{r}$$

### 3.3.1 Théorème d'Euclide

**Théorème 3.8.** *L'ensemble des nombres premiers est infini.*

### 3.3.2 Indicatrice d'Euler

**Définition 3.5.**
*L'indicatrice d'Euler est la fonction $\varphi$, définie par :*

$$\begin{aligned}\varphi \ : \ & \mathbb{N}^* \to \mathbb{N}^* \\ & n \longmapsto card(\{m \in \mathbb{N}^*;\ m \leq n \text{ et } m \text{ premier avec } n\})\end{aligned}$$

**Propriété 3.3.**
*Pour tout entier $n$ non nul $\varphi(n)$ est égal :*

- *Au nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*
- *Au nombre de générateurs d'un groupe cyclique d'ordre $n$.*

**Propriété 3.4.**

1. *Si $m$ et $n$ deux entiers premiers entre eux alors :$\varphi(mn) = \varphi(m)\varphi(n)$*
2. *Si $p$ est un nombre premier et $k \in \mathbb{N}^*$ alors $\varphi(p^k) = (p-1)p^{k-1}$*
3. *La valeur de l'indicatrice d'Euler s'obtient à partir de la décomposition en facteurs premiers de $n$.*
4. *Tout nombre est la somme des indicatrices de ses diviseurs : $n = \sum_{k/n} \varphi(k)$ pour tout les nombres $k$ qui divisent $n$.*

**Démonstration 26.**

1. *Soient $a \in [\![1; mn]\!]$ et $q, r$ désignent respectivement le quotient et le reste de la division euclidienne de $a$ par $m$, alors on a la relation*

   $$a = mq + r \text{ avec } 0 \leq r < m$$

   *Lorsque $a$ parcourt l'ensemble $\{1, 2, \ldots, mn\}$ alors le couple $(q, r)$ parcourt tous les couples $(x, y)$ avec $0 \leq x < n$ et $0 \leq y < m$.*
   *Supposons $a$ premier avec $mn$ (ce qui est équivalent au fait que $a$ est premier avec $m$ et avec $n$), alors*

   $$r \text{ est premier avec } m$$

   *(car sinon $a$ et $m$ auraient un facteur commun).*
   *Par suite,*

   $$r \text{ ne peut prendre que } \varphi(m) \text{ valeurs}$$

   *De plus, $r$ étant fixé, la suite des entiers*

   $$mq + r \text{ avec } q \in [\![0; n-1]\!]$$

   *ne possède que des restes différents modulo $n$*
   *Par conséquent il n'y a que $\varphi(n)$ valeurs possibles pour $q$ si $a$ est premier avec $n$.*
   *En conclusion, il ya pas $\varphi(n)\varphi(m)$ choix possible pour le couple $(q; r)$ pour que $a$ soit premier avec $mn$, et ainsi :*

   $$\varphi(mn) = \varphi(n)\varphi(m)$$

2. *Si $p$ est un nombre premier et $k \in \mathbb{N}^*$, alors le nombre d'entiers inférieurs à $p^k$ et non premier avec lui sont exactement les multiples de $p$ inférieurs à lui même, il y en a exactement $p^{k-1}$. Par conséquent :*

$$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$$

3. *Soit $n$ un entier naturel non nul, alors $n$ se décompose en produit de facteurs premiers comme suit :*

$$n = p_1^{k_1} \times p_2^{k_2} \times ; \ldots ; p_m^{k_m}$$

*D'après les questions précédentes on déduit que :*

$$\varphi(n) = \varphi(p_1^{k_1}) \times \varphi(p_2^{k_2}) \times \ldots \varphi(p_m^{k_m}) = n(1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times \ldots \times (1 - \frac{1}{p_m})$$

4. *On fait un raisonnement par récurrence.*
*Pour $n = 1$ le résultat est vrai.*
*Soit $n = p^a q$ avec $p$ un nombre premier et $q$ est premiers avec $q$($q$ peut être égal à 1).*
*Supposons que le résultat est vrai pour $q$. Tout nombre $k$ qui divise $n$ est de la forme $p^j m$ avec $j \in [\![0; a]\!]$ et $m/q$. Donc, on peut écrire :*

$$\sum_{j=0}^{a} \sum_{m|q} \varphi(p^j m) = \sum_{j=0}^{a} \sum_{m|q} \varphi(p^j)\varphi(m) = \sum_{j=0}^{a} \sum_{m|q} \phi(m) = \left(1 + \sum_{j=1}^{a} p^{j-1}(p-1)\right) q = p^a q = n$$

*Donc, par hypothèse recurrence :*

$$\sum_{k \backslash n} \varphi(k) = n$$

### 3.3.3 Petit théorème de Fermat

**Théorème 3.9.** *Si $p$ est un nombre premier, alors pour tout entier $n$ on a :*

$$n^p \equiv n \ [p]$$

**Démonstration 27.**
***première étape***
*On montre que :*

$$Si\ p\ est\ premier\ \Leftrightarrow p \setminus C_p^k\ Pour\ tout\ k \in [\![1; p-1]\!]$$

*Soient $p$ un nombre premier, et $k \in [\![1; p-1]\!]$ un entier fixé, alors on a :*

$$kC_p^k = pC_{p-1}^{k-1}\ d'où\ p \setminus kC_p^k$$

*or $p$ et $k$ sont premiers entre eux car $p$ est premier et $k \in [\![1; p-1]\!]$ donc par le théorème de Gauss on a $p \setminus C_p^k$. Réciproquement, on va raisonner par contraposition, supposons que $p \geq 2$ n'est pas premier. Soit $q$ un diviseur premier de $p$, alors on a la relation :*

$$q! \times C_p^q = p \times (p-1) \times \ldots \times (p-q+1)$$

*Si $r$ est l'exposant de $q$ dans la décomposition en facteurs premiers de $p$, l'entier $q$ étant premier avec chaque terme du membre de droite de l'expression ci-dessus à l'exception de $p$, alors $r$ l'exposant de $q$ dans la décomposition en facteurs premiers de $p(p-1)\ldots(p-q+1)$.*

*De même, cet exposant vaut 1 dans la décomposition en facteurs premiers de* $q!$
*Ainsi, si :*

$$p \setminus C_p^q \text{ alors } q^{r+1} \setminus q! \times C_p^q$$

*impossible.*
*Donc,* $p \nmid C_p^q$*, et on a le résultat voulu par contraposition.*

***deuxième étape***
*Si* $n = 0$ *le resultat est clairement vrai. Supposons donc le résulat vrai au rang* $n \in \mathbb{N}$ *et montrons le au rang* $n+1$*.*
*On a :*

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} n^k C_p^k + 1 \equiv n^p + 1 \ [p] \ (d'après \ la \ première \ étape)$$

$$(n+1)^p \equiv n+1 \ [p] \ (par \ hypothèse \ de \ récurrence)$$

### 3.3.4 Exercices d'application

**Exercice 1 :**

Soit $n \in \mathbb{N}^*$

1. Montrer que $\forall n \geq 5 \;\; n^4 - 20n^2 + 4$ n'est pas premier.
2. Pour $n \geq 7$ calculer (selon les valeurs de n) le PGCD de $n^3 - 6n^2 + 1$ et $n^2 - 6n - 1$.

**Exercice 2**

1. Soient $d, a_0$ (respectivement) le quotient et le reste de la division euclidienne de $n$ par 10. Donner une condition nécessaire et suffisante pour que $n$ soit divisible par 13 ou par 17 ?
2. Sans utiliser le calculateur, monter si le nombre 1633123612311854 est divisible par 13.
3. Calculer $\varphi(255255)$, où $\varphi$ désigne l'indicateur d'Euler.

**Exercice 3**

1. Résoudre dans $\mathbb{N}$ l'équation suivante :
$$31x - 13y = 1$$
2. Application : au bord d'une piscine pleine d'eau, on dispose d'une cuve de 31 litres munie à sa base d'un robinet de vidange, et d'un seau de 13 litres.
Expliquer comment operé pour obtenir exactement 1 litre dans le seau.

**Exercice 4 : Lemme des restes chinois**

1. Soient $m$ et $n$ deux entiers naturels non nuls premiers entre eux, et $a$,$b$ deux entiers donnés. Montrer que le système de congruence :
$$\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$$
admet toujours au moins une solution $x \in \mathbb{Z}$.
2. Soit $x_0 \in \mathbb{Z}$ une solution particulière du système(S), déterminer toutes les solutions de (S) en fonction de $x_0$.

**Exercice 5**

1. Calculer, en utilisant le théorème de Fermat, le reste de la division euclidienne de $3^{30}$ par 341.
2. Calculer, sans utiliser le calculateur, le reste de division euclidienne de $3^{340}$ par 341.
3. Nous avons des choses dont nous ne connaissons pas le nombre :
   - Si nous les partagons par paquets de 3, le reste est 1
   - Si nous les partagons par paquets de 5, le reste est 4
   - Si nous les partagons par paquets de 7, le reste est 3

Combien y a t'il de choses sachant que ce nombre est inferieur à 100 ?

**Exercice 6 : équations diophantiennes quadratique**

On se propose de chercher toutes les solutions entières de l'équation diophantienne.

$$x^2 + axy + y^2 = z^2 \qquad (1)$$

*où* $a \in \mathbb{Z}$ est un entier donné.

1. Montrer que toutes les solutions entières de l'équation (1) sont données par :

$$\begin{cases} x = k(an^2 - 2mn) \\ y = k(m^2 - n^2) \\ z = k(amn - m^2 - n^2) \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(an^2 - 2mn) \\ z = k(amn - m^2 - n^2) \end{cases} \qquad (2)$$

   *où* $k, m, n \in \mathbb{Z}$.

2. En déduire alors :

   (a) toutes les solutions entièrs $(x, y, z, t) \in \mathbb{Z}^4$ de :

$$x^2 + xyt + y^2 = z^2$$

   (b) Toutes les solutions entières $(x, y, z) \in \mathbb{Z}^3$ de :

$$x^2 + axy + by^2 = z^2 \qquad (a, b \in \mathbb{Z}^2)$$

   (c) Toutes les solutions entières $(x, y, z, u, v) \in \mathbb{Z}^5$ de :

$$x^2 + uxy + vy^2 = z^2$$

   (d) Toutes les solutions entières $(x, y, z) \in \mathbb{N}^3$ de :

$$x^2 + axy + y^2 = z^2 \qquad (a \in \mathbb{Z})$$

### 3.3.5 Solution d'exercices

**exercice 1 :**

1. $n^4 - 20n^2 + 4 = (n^2-2)^2 - (4n)^2 = (n^2 - 4n - 2)(n^2 + 4n - 2)$

$$n \geq 5 \Rightarrow \begin{cases} n-4 \geq 1 \\ n+4 \geq 1 \end{cases} \Rightarrow \begin{cases} n(n-4) \geq 5 \\ n(n+4) \geq 5 \end{cases} \Rightarrow \begin{cases} n^2-4n-2 \geq 3 \\ n^2+4n-2 \geq 3 \end{cases}$$

$\Rightarrow n^2 - 20n + 4$ n'est pas premier.

2. $n^3 - 6n + 1 = (n^2 - 6n - 1)(n + n + 1)$, ainsi :

$$\begin{aligned} n^2 - 6n - 1 &= (n+1)(n-7) + 6 \\ \Rightarrow pgcd(n^3 - 6n + 1; n^2 - 6n - 1) &= pgcd(n^2 - 6n - 1; n+1) \\ &= pgcd(n+1; 6) = d_n \end{aligned}$$

où :

$$d_n = \begin{cases} 1 & si\ n \equiv 0, 4\ mod\ 6 \\ 2 & si\ n \equiv 1, 3\ \ mod\ 6 \\ 3 & si\ n \equiv 2\ mod\ 6 \\ 6 & si\ n \equiv 5\ mod\ 6 \end{cases}$$

**Exercice 2 :**

1. $n = 10d + a_0$

$$\begin{aligned} 13/n\ ssi\ 13/10(d + 4a_0) - 39a_0 \\ ssi\ 13/d + 4a_0 \\ 17/n\ ssi\ 17/10(d - 5a_0) + 51a_0 \\ ssi\ 17/d - 5a_0 \end{aligned}$$

*b) Comme* $10^3 \equiv (-3)^3 \equiv -27 \equiv -1\ \ = mod\ 13$.

$$\begin{aligned} n &\equiv ((854 - 311) + (612 - 123) + (633 - 1))\ mod\ 13 \\ &\equiv (543 + 489 + 632)\ mod\ 13. \\ 13/n &\Leftrightarrow\ 13/1664 \\ &\Leftrightarrow\ 13/(166 + 16) \\ &\Leftrightarrow\ 13/182 \\ &\Leftrightarrow\ 13/(18 + 8) \end{aligned}$$

Comme $13/26$, alors $13/n$.

2. Factorisons d'abord :

$$n = 255255 = 255(1001) = 51.5.(1001)$$

Comme :

$$7/1001 \Leftrightarrow 7/(100-2) \Leftrightarrow 7/98$$

alors :

$$1001 = 7.143$$

3. D'où $n = 3.5.7.11.13.17$, donc :

$$\varphi(n) = 2.4.6.10.12.16 = 144.64.10 = 92160$$

**Exercice 3 :**

1. $pgcd(31;13) = 1$, cherchons d'abord :

$$(u'_0; v'_0) \ / \ 31u'_0 + 13v'_0 = 1$$
$$n = 5; (u'_0, v'_0) = (-5; 12)$$

c-à-d :

$$31(-5) + 13(12) = 1 \ (\star)$$

par suite on a :

$$31(-5) - 13(-12) = 1$$

d'où $(x_0; y_0) = (-5; -12)$ est une solution particulière d'où :

$$S = \{-5 + 13k, -12 + 31k, k \in \mathbb{Z}\} \cap \mathbb{N}$$
$$S = \{(-5 + 13k, -12 + 31k), k \in \mathbb{N}^*\}$$
$$S = \{(8 + 13k, 19 + 31k), k \in \mathbb{N}\}$$

2. $b$) D'après $\star$ on a : $12(13) - 5(31) = 1$ c-à-d 12 seaux-5 cuves=1 litre.
En pratique, on ferme le robinet de vidange, puis on remplit la cuve avec le seau,ensuite on ouvre le robinet de vidange.
Après 5 vidange, il nous reste qu'un litre dans le seau.

**Exercice 4**

1. Comme $m$ et $n$ sont premiers entre eux alors il existe, d'après le lemme de **Bézout** deux entiers $u$ et $v$ tel que :

$$mu + nv = 1$$

Donc, il s'ensuit en particulier que

$$mu \equiv 1[n] \ et \ bmu \equiv b[n]$$

De même on a aussi :

$$nv \equiv 1[m] \ et \ anv \equiv a[m]$$

Comme on cherche un nombre équivant a $b$ modulo $n$ (resp modulo $[m]$), alors on déduit qu'il est de la forme :

$$bmu + ny \ (resp \ anv + mx)$$

Finalement, le nombre $x = bmu + anv$ est de chacune de ces formes et vérifie le système (S).

2. Soit $x_0$ une solution particulière de (S). Si $x_1$ est une autre solution de (S) alors :

$$x_0 - x_1 \equiv 0[m] \;\; et \;\; x_0 - x_1 \equiv 0[n]$$

Donc, $x_0 - x_1$ est un multiple de $m$ et de $n$, par suite il est multiple de leur ppcm qui est égal à $mn$ (car premiers entre eux).
Réciproquement, si $x_0$ est une solution particulière de (S) alors :
$x_0 + kmn$ en est une autre (avec $k \in \mathbb{Z}$).
En conclusion, l'ensemble des solutions est donné par :

$$\{x_0 + kmn \; ; \; k \in \mathbb{Z}\}$$

**Exercice 5 :**

1. $341 = 11.31$

$$Fermat \Rightarrow \begin{cases} 3^{10} \equiv 1 \; mod \; 11 \\ 3^{30} \equiv 1 \; mod \; 31 \end{cases} \quad \begin{cases} 11/3^{30} - 1 \\ 31/3^{30} - 1 \end{cases} \Rightarrow \begin{cases} 11.31/3^{30} - 1 \\ pgcd(11, 31) = 1 \end{cases} \Rightarrow \left\{ 3^{30} \equiv 1 \; mod \; 341. \right.$$

$\rightarrow$ Le reste de la division euclidienne de $3^{30}$ par 341 est 1.

2. $3^{340} \equiv 3^{30.11} 3^{10} \equiv 3^{10}$ mod 341 d'après "a". Ainsi :

$$\begin{aligned} 3^{340} &\equiv 3^4.3^2.3^4 \; mod \; 341 \\ &\equiv (81.9).81 \; mod \; 341 \\ &\equiv 729.81 \; mod \; 341 \\ &\equiv 47.81 \; mod \; 341 \; (car \; 729 = 682 + 47) \\ &\equiv 380.7 \; mod \; 341 \\ &\equiv 397 \; mod \; 341 \; (car \; 3410 \equiv 0 \; mod \; 341) \\ &\equiv 56 \; mod \; 341 \end{aligned}$$

$\Longrightarrow$ *le reste est* 56

3. Cela revient à resoudre, dans $\mathbb{Z}$, le (s.c) suivant :

$$\begin{cases} x = 1 \; mod \; 3 \\ x = 4 \; mod \; 5 \\ x = 3 \; mod \; 7 \end{cases}$$

Utilisons le théorème de reste chinois :
Ici $n_1 = 3, n_2 = 5, n_3 = 7, a_1 = 1, a_2 = 4, a_3 = 3, N_1 = 35, N_2 = 21 \; et \; N_3 = 15$.
Cherchons d'abord $u_1, u_2 \; et \; u_3$ (qui sont les inverses respectivement de $N_1$ modulo $n_1$,$N_2$ modulo $n_2$ et $N_3$ modulo $n_3$) :

$$\begin{aligned} 35(-1) + 3(12) = 1 \leftarrow u_1 = 2(puisque \; -1 \equiv 2 \; mod \; 3) \\ 21(1) + 5(-4) = 1 \leftarrow u_2 = 1(inverse \; de \; 21 \; modulo \; 5) \\ 15(1) + 7(-2) = 1 \leftarrow u_3 = 1(inverse \; de \; 15 \; modulo \; 7) \end{aligned}$$

$c = 2.35.1 + 1.21.4 + 1.15.3 = 70 + 84 + 45 = 199 = 105 + 94$ où $105 = 3.5.7 = N \leftarrow x_0 = 94$
$S = \{94 + 105k, k \in \mathbb{Z}\}$. Donc la seule solution compris entre 0 et 100 est donc 94.
Par conséquent il y a 94 choses.

**Exercice 6**

1. Tout d'abord, il est facile de vérifier que les triplets $(x, y, z)$ donnés par la relation (2) sont bien solutions de l'équation (1). Il suffit juste de remplacer les valeurs de $x, y$ *et* $z$ pour avoir l'égalité.
   Réciproquement, l'équation (1) est équivalente à :

$$x(x + ay) = (z - y)(z + y)$$

   Si $y = z$ ie $x = 0$ ou $x + ay = 0$, alors le résultat est clair dans ce cas là.
   Sinon, l'équation ci-dessus est équivalente à :

$$\frac{x}{z-y} = \frac{z+y}{x+ay} = \frac{n}{m} \qquad (m, n) \in \mathbb{Z}_*^2$$

   Par conséquent, on obtient le système d'équations :

$$\begin{cases} mx + ny - nz = 0 \\ nx + (n - am)y - mz = 0 \end{cases}$$

   Les solutions de ce système sont données par :

$$x = \frac{an^2 - 2mn}{amn - m^2 - n^2} \quad ; \quad y = \frac{m^2 - n^2}{amn - m^2 - n^2}$$

   On choisit

$$z = k(amn - m^2 - n^2)$$

   et alors les solutions sont données par :

$$\begin{cases} x = k(an^2 - 2mn) \\ y = k(m^2 - n^2) \\ z = k(amn - m^2 - n^2) \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(an^2 - 2mn) \\ z = k(amn - m^2 - n^2) \end{cases}$$

2. (a) La solution générale est $(x, y, z, t)$ avec $t = a \in \mathbb{Z}$ et $x, y, t$ donnés par la relation (2)
   (b) On montre comme ci-dessus que les solutions sont données par :

$$\begin{cases} x = k(m^2 - bn^2) \\ y = k(an^2 - 2mn) \\ z = k(amn - m^2 - bn^2) \end{cases}$$

   *où* $k, m, n \in \mathbb{Z}$
   (c) Les solutions de cette équation sont les $(x, y, z, u, v)$ avec $u = a \in \mathbb{Z}$ , $v = b \in \mathbb{Z}$ et $x, y, z$ sont donnés par la relation (3)
   (d) Les solutions entières positives sont données par :

$$\begin{cases} x = k(2mn + 2an^2) \\ y = k(m^2 - n^2) \\ z = k\lvert m^2 + amn + n^2 \rvert \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(2mn + an^2) \\ z = k\lvert m^2 + amn + n^2 \rvert \end{cases}$$

   *où* $k, m, n \in \mathbb{N}^*$ , $2m + an > 0$ , $m > n$

# Bibliographie

[1] Rachid Acharghaoui, ***Logique et Arithmétique***, Filière : SMAI, Polycopié, Univérsité Ibn Tofail.

[2] Mohammed Aassila, ***400 exercices corrigés d'algèbre avec rappels de cours Prépa Sup***, ELLIPSES (17 septembre 2013)

[3] Stéphane BALAC-Frédéric STURM, ***Algèbre et analyse Cours de mathématiques de première année avec exercices corrigés deuxième édition revue et augmentée***, 2008 , Université de Rennes 1, INSA de Lyon